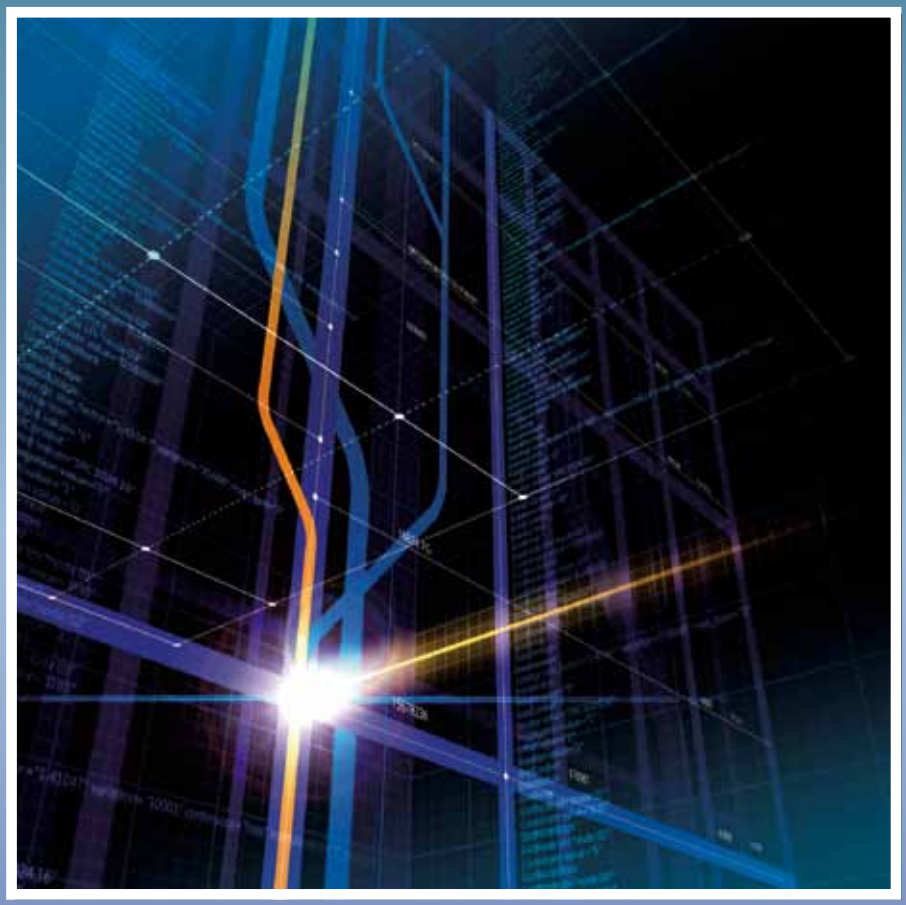
Cyber Warfare:
Concepts and Strategic Trends

Shmuel Even and David Siman-Tov



Memorandum 117

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

Cyber Warfare:
Concepts and Strategic Trends

Shmuel Even and David Siman-Tov

Institute for National Security Studies

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

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

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

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

Shmuel Even and David Siman-Tov

Cyber Warfare:
Concepts and Strategic Trends

Memorandum No. 117 May 2012

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

שמואל אבן ודוד סימן־טוב

לוחמה קיברנטית:
מושגים ומגמות אסטרטגיות

Editor: Judith Rosen
Graphic design: Michal Semo-Kovetz
Printing: Elinir

Institute for National Security Studies
40 Haim Levanon Street
POB 39950
Ramat Aviv
Tel Aviv 61398

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

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

May 2012

ISBN: 978-965-7425-35-0

Contents

Preface

Cyberspace is a new domain of warfare that in recent years has joined the traditional arenas of land, sea, air, and space. The study that follows describes the unique characteristics of this new domain of warfare, offers fresh interpretations of familiar concepts, and surveys landmark events and organizations in the field of cyberspace in Israel and abroad.

Modern nations and advanced militaries around the world are intensifying their activities in cyberspace, which simultaneously constitutes a source of power and a soft underbelly. The infrastructures critical for the functioning of a state (electricity, communications, water, transportation, finance, and so on) all rely on this domain. Military command and control networks depend on cyberspace, as do all the most advanced technologies of the modern battlefield, such as intelligence gathering, processing and fusion systems, satellite use on the battlefield, use of autonomous fighting tools, real time integration of sensors to identify targets with fire systems, and more.

As an arena of warfare, cyberspace presents some unique features, including the ability to operate quickly, in thousandths of seconds, against enemies located far away, without risking the lives of combat personnel. The unique features of the domain also make it attractive for confrontation in the intervals between conventional wars. One may distinguish between confrontations in cyberspace (such as the 2007 attack on Estonia, attributed to Russia) and wars in which attacks in cyberspace are but one component in a war alongside other forces (such as Russia's attack on Georgia in 2008). Furthermore, one may distinguish between attacks taking place in cyberspace (attacks on computerized systems) and the use of cyberspace as a means to damage the functionality of machines operating in the physical domain, e.g., the 2009 cyberspace attack on Iran's nuclear program. This event (the Stuxnet virus attack), which demonstrated the great potential impact of cyberspace weapons, was formative in the development of cyberspace as grounds for warfare.

It appears that from now on, cyberwar will likely play a part in every modern war. Indeed, both cyberspace attacks that have occurred and processes undertaken by states to prepare themselves in this domain indicate that the cyberspace arms race has already started. As part of this race, a number of states (the US, Great Britain, France, Germany, China, and others) have in recent years established offices and headquarters dedicated to cyberspace as a domain of warfare, and security strategies for cyberspace have been formulated. At the same time, states are also faced with considerations regarding the constraints of cyber attacks and the risk of exposure to counterattacks, especially because defenses are still not sufficiently strong. In addition, non-state elements such as terrorist organizations are liable to use cyberspace to launch attacks, once they achieve the capability of causing severe damage.

In tandem, there is growing international recognition that it is necessary to defend cyberspace and regulate its activities – similar to regulation in other realms. This type of regulation can be achieved through inter-state cooperation, adaptation of international law to cyberspace, and formulation of a compelling international treaty. Progress thus far has been slow, certainly not in pace with developments in cyberspace.

In the Israeli context, information technologies and cyberspace play a decisive role in Israel's qualitative superiority in terms of its economy and security. Cyberspace is crucial to Israel's society, the bond between the government and the population, and Israel's connections with the world at large. Even more so, it plays a critical role in Israel's national security, especially given the developing cyberspace threats, Israel's information technology advantage, and the potential cyberspace implications for the modern battlefield. All of these dimensions oblige Israel to accelerate its efforts to improve defense of its cyberspace and contribute of its capabilities to the defense of cyberspace on a global scale.

This research was conducted in the framework of the INSS Program on Cyber Warfare, headed by Prof. Isaac Ben-Israel and Dr. Gabi Siboni and supported by the Philadelphia-based Joseph and Jeanette Neubauer Foundation. The authors would like to extend their thanks to Dr. Amos Granit, Head of the Institute for Intelligence Research in Military Intelligence, for his constructive comments, and to Patrizia Isabelle Duda for her contribution to the memorandum.

This study is published with the assistance of the gift of the late Esther Engelberg.

Chapter 1

Cyberspace and the Security Field: A Conceptual Framework

The term "cyberspace" defines a phenomenon that emerged with the invention of the telegraph in 1844, which involves taking advantage of the electromagnetic field for human needs by means of technology. An essential turning point in the development of cyberspace was the invention of the numerical computer in 1949. Other milestones include: the linking of communications networks with computers and machines, which began in the 1970s; mass use of the internet and personal computers since the mid-1990s; and in the past decade, the comprehensive integration between computer systems and various communications systems and machines (such as in industry, transportation, and other fields), the mass use of handheld cellular devices, the flourishing of social networks on the internet, and more. All of these have profoundly influenced society and the economy.

Information technologies and cyberspace are rapidly changing the nature of the modern battlefield as well. One example is the advanced technology found on the battlefield, including intelligence systems, systems for information sharing and information fusion, the use of satellites on the battlefield, autonomous tools, real time integration of target seeking sensors with fire systems, and more. The development of cyberspace has also allowed extensive civilian coverage of the combat arena, partly by means of mobile cellular devices that provide anyone present in the arena with the ability to document information, or alternatively, manipulate it. This information is transmitted instantly to internet networks, which in turn generates discussions in the social networks and affects public opinion. Thus arenas of war have become a space in which the public plays a central role

and exerts – more so than in the past – its influence on the political stances of governments and international institutions, at times on the basis of nebulous information. This phenomenon has far reaching implications for everything having to do with the use of military force. It limits the ability to apply force but can also help enlist public opinion in favor of the use of force.

Definitions

Cyberspace has several definitions, many of which feature several shared layers. According to the International Telecommunications Union (ITU) of the United Nations, cyberspace is "the physical and non-physical terrain created by and/or composed of some or all of the following: computers, computer systems, networks and their computer programs, computer data, content data, traffic data, and users."[1] This definition implies that cyberspace entails three interdependent layers (table 1):

a. The human layer: the users of computerization (communications and computers).
b. The logical layer: the software and bits. These move at the speed of light and represent information, instructions, cyberspace assets (such as valuable software, electronic funds), malware (such as Trojan horses), and more.
c. The physical layer: the network physical components, including hardware, mobile infrastructures, and stationary infrastructures, found on land, at sea, in the air, and in space (henceforth, "the physical spheres").

While other definitions of cyberspace recognize the three layers (human, logical, and physical), each distinguishes the term "cyberspace" using some of the layers only.

In US military documents, cyberspace is defined in the context of the second (logical) and third (physical) layers as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[2] Furthermore, cyberspace is the fifth domain (in addition to land, sea, air, and space), with interfaces between the domains: cyberspace exists physically in each of the other domains, connects them, and strengthens capabilities in them, while their activities are expressed in the domain of cyberspace.

Table 1. The Three Layers of Cyberspace

Layer	Type of activity and its purpose	Contents (examples)	Developing trends (examples)
1. The human layer			
The user	Human use of computerization products	Reading, trading, investing, finding information, exchanging information, maintaining contact with friends, contact between citizens and government offices, crime, cyberwar	An increase in the phenomenon of user communities (WEB2) and the use of mobile and integrative devices (smart phones); the start of sophisticated internet use (WEB3)
2. The logical layer	Software activity		
Graphic user interface (GUI)	Translating information from user language to computer language (digital information) and back	Pages of text, pictures, videos, audio, buttons	Increase in types and levels of applications presented at the interface; rise in graphic presentation; transition to 3D
Applications software	Processing information from user interfaces, network management software	Instructions and flow charts in programming language (algorithms)	More applications; more and more layers of software between the hardware and user interface
Operating systems	Running software and translation from computer language to machine language	Information in programming language relevant to the layer	
3. The physical layer			
Hardware	Electromagnetic physical infrastructure doing machine operations	Chips, electronic cards, etc; electrical impulses	Growth in volume of information about electronic components, miniaturization, mobility, flash memory

The Three Layers of Cyberspace – cont'd

Layer	Type of activity and its purpose	Contents (examples)	Developing trends (examples)
Communications and energy systems (electromagnetic infrastructure)	Providing conditions for existence and activity of computerization in electromagnetic field	Infrastructure and maintenance; laying cables, computer tables, etc; RF signals, light and electricity waves	Growth in variety and spread of communications systems: cellular, Bluetooth, router, satellite, ocean cable. Improved energy utilization and miniaturization
Hardware and software carriers	Provide additional conditions to maintain cyberspace on land, at sea, in the air, and in space.		People carrying smart computers and phones; computer-embedded installations, systems, and tools; equipment with integrated processors and controllers; and devices with input options (scanners), sensors, and effectors. This is where the connection between cyberspace and the physical realms occurs.

In a document entitled, "Cyber Security Strategy of the United Kingdom," the UK Cabinet Office defines cyberspace as follows: "Cyber space encompasses all forms of networked, digital activities; this includes the content of and actions conducted through digital networks."[3] This definition places the logical layer at its center.

In a document entitled "The New Cyber Security Strategy for Germany" ("Nationale Cyber-Sicherheitsstrategie"), the German Federal Ministry of the Interior defines cyberspace with a relatively narrow focus: "Cyberspace is the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace."[4]

Unlike definitions that view cyberspace as a fifth dimension, there is an approach that claims that cyberspace is one of seven domains, alongside air, space, sea, land, the electromagnetic domain, and the human domain. Departing from previous definitions, this approach distinguishes between cyberspace and the electromagnetic domain and counts the human layer as a dimension of its own.[5] Cyberspace is an artificial domain realized by means of the electromagnetic domain that interfaces with physical domains by means of sensors and effectors. As such, cyberspace serves to empower the functionality of civilian and military systems operating in all domains while it also exposes them to cyberspace attacks.[6]

The common denominator of all the definitions is the logical layer; the differences in definition reflect the particular emphases of various states and organizations as they attempt to confront the challenges posed by cyberspace. The differences in definition, however, do not reflect essentially different understandings of cyberspace, as all recognize the existence of the three layers appearing in the UN definition.

Characteristics of Cyberspace as a Domain of Warfare

For each of the layers appearing in the UN definition of cyberspace, there are different security-related activities pertaining to the domain, for example:

a. Actions in cyberspace aimed at the human layer designed to change user conduct, such as transmitting informational messages (open or hidden) through cyberspace to the enemy.
b. Logical penetration (by means of software) for purposes such as espionage, attacks on enemy computers in order to withhold cyberspace benefits from the enemy, and attacks on machines and installations in the physical domains controlled from cyberspace, e.g., disrupting thermal control mechanisms that could lead to the explosion of a security plant (an effect in the land domain) or disrupting an altimeter that could lead to damage of aircraft (an effect in the air domain). In such cases, the enemy's cyberspace becomes a tool helping the attacker and may therefore prevent damage to the enemy's computerization systems.
c. In the physical layer, damage to hardware that serves as the foundation for the logical layer, as well as actions outside cyberspace aimed against infrastructures on which the domain relies, e.g., firepower and electronic

warfare to damage or paralyze communications components and energy systems on which cyberspace depends.

Some of the characteristics of the new domain of warfare include:

The ability to act at nearly the speed of light, without traditional geographical limitations. This feature allows attackers the opportunity to execute long distance attacks in fractions of seconds without having to contend with the enemy in a physical arena. At the same time, cyberspace depends on the physical domain and the network infrastructures diffused in the physical space. On the defensive side, the possibility of a quick attack requires a foundation of dynamic defensive systems reacting automatically to attacks in real time and independent of human calculations.

The ability to act in secret. Cyber attacks that have already occurred and information about strategies for action in cyberspace indicate that the attacker has the ability to operate in cyberspace anonymously – without leaving a signature (identifying marks) – and hide behind others such as private hackers, criminal elements, or foreign agencies and nations. In other words, the use of cyberspace allows the attacker to minimize exposure, incrimination, and risk of counterattack, as evidenced by the fact it has been impossible to implicate the suspected nation in any of the cyber attacks carried out to date. In warfare in a kinetic battlefield it is usually clear who started, who attacked, and what space was conquered; none of this applies in cyberwar. This fact has contradictory implications: on the one hand, this may serve to limit counterattacks (there isn't anyone to respond to), yet there is also the potential for uncontrolled escalation. For example, should there be attacks causing fatalities and heavy damage to property, there will be political pressure to react against suspected elements even in the absence of solid evidence about the identity of the attacker.

Cyber weapons can also be used as non-lethal weapons. The ability to cause heavy damage to the functioning of a state without destroying its physical infrastructures or killing people is considered an advantage of cyber weapons over strategic kinetic attacks (firepower). At the same time, cyber attacks can also cause a great deal of destruction and loss of human life by means of damaging systems located in physical domains but connected to cyberspace.

Cyberspace makes accessible targets not susceptible to attack by fire, such as:

a. Installations and systems (communications, command and control, etc.) located in areas difficult to access in a kinetic attack (because of distance, strong kinetic defenses, concentrations of population, and so on).
b. Banking and finance: Today these are considered critical national infrastructures vulnerable to attack in cyberspace, both because of the nation's great dependence on financial systems and because of these systems' dependence on cyberspace. Damage to the financial system is liable to keep salaries from being deposited in banks, limit foreign trade, and even cause the economy to stop functioning.
c. Logistics and transportation systems, which today are computer-enabled.
d. National databases, i.e., in government ministries, the courts, universities, and so on.

Low risk to human life. Attacks in cyberspace entail little risk to the life of the attacker compared to military kinetic attacks in which risk to troops is one of the considerations likely to prevent an attack. This allows more audacity in the promotion of offensive ideas. For the party defending against attack, the limited risk to human life allows a fairly large scope of activity and even the ability to operate automatic defense mechanisms, without dependence on human calculations and, unlike kinetic defense systems, without risk to individuals on either the attacking or the attacked side.

Selectivity. This feature is somewhat equivocal. In certain attack scenarios, it is possible to attack specific targets within a certain domain without damaging additional entities. In other scenarios, however, it is difficult to control the scope of the attack and damage may spread beyond what was planned.

Virality. This feature touches on the tendency of viruses to replicate themselves unchecked and their ability to move through the web to different locations. This is a difficult challenge for an attacked party, which must prevent the virus from spreading. For the attacker this is an advantage in certain scenarios of widespread attack, as many additional effects may be created by means of a limited effort. However, this characteristic is liable to present a difficulty to the attacker who is interested in a focused and selective attack and tight control of the attack results.

Standardization of cyberspace. The cyber domain is based primarily on infrastructures made by global companies (e.g., Microsoft, Cisco, Check Point) that are located in every country and linked together. While the

universal nature of the domain and the use of the same equipment (for example, Unix and Windows operating systems) serve those constructing cyberspace, these features also entail a great deal of risk to an attacked party. For example, hacking of information security software or a technological database belonging to a global cyberspace company is liable to endanger every site where it is used. In March 2011, RSA, the information security company owned by the giant storage company EMC, announced it sustained damage by a sophisticated attack by hackers who managed to steal information on a secure ID apparatus serving to verify employee identity in organizations and governments around the world.[7] Such incidents endanger the effectiveness of security products shared by many corporations and governments.

Connectivity between cyberspace and devices operating in other domains. Using sensors it is possible to convert geographical, thermal, mechanical, and other data from physical domains into bits, and vice versa, and using effectors it is possible to convert directions transmitted over the bit web to actions in those domains. This connectivity allows a cyberspace attacker to generate effects in physical domains by attacking systems connected to cyberspace, such as computer embedded systems.

Reversibility – the ability to go back in time. From the point of view of the attacked party, this feature means a fast recovery time from a cyberspace attack by reversing the computerization products backwards (resetting the time) with the help of backup systems. The more comprehensive and continuous the backup systems are, the more the return to the precise original configurations becomes possible. Restoration after a cyberspace attack is usually quick and cheap relative to physical destruction caused by massive fire attacks. Nonetheless, certain cyberspace attacks are also liable to cause extensive physical damage that is less easily reversed. From the attacker's perspective, the advantage of this feature is that it allows the infliction of limited and temporary damage to an infrastructure under attack, e.g., a civilian infrastructure. The drawback to the attacker lies in the targeted party's ability to regroup and block tracks that were attacked and defend against tools used in prior attacks (making cyberspace weapons virtually disposable); this in turn will make it difficult for the attacker to generate cumulative damage and maintain attack continuity and strength. This is a major challenge to attackers who desire to reach strategic goals using extended and extensive cyberspace attacks. Because of this difficulty, some

researchers believe that the potential of damage to the enemy or gain to the attacker attributed to cyberspace attacks is significantly lower than that estimated by many institution and experts.[8]

High human ability to control cyberspace. Because cyberspace is an artificial, man-made domain, defenders should be able to control the sphere they have constructed. They should be able to anticipate the conditions in the domain, as opposed to the difficulty in anticipating conditions in other domains (e.g., weather). They can shut the domain down or limit its use: examples of attempts to limit the use of cyberspace may be found in China, Arab states, and Iran. The domain also allows both sides (attacker and attacked) to train with great ease and undertake simulations. In addition, it is easier for those attacked to rebuild an organized, ordered network quickly than a less organized network. Nonetheless, events unanticipated by the builders of the domain do occur in cyberspace, products of interactions between computers or the intensification of human errors (e.g., errors in providing instructions to the capital market). The features of the domain intensify the ability of insiders to act maliciously by means of cyberspace.

Integrated civilian-military domain. In many cases, military communications infrastructures are linked to civilian infrastructures. Hence, defending civilian infrastructures is also critical for military purposes. At the same time, militaries have cyberspace capabilities that may help defend civilian infrastructures. In democratic nations, this integration is a legal challenge for a threatened or attacked party in light of advanced legislation in the field of individual rights, which makes it difficult, for example, to gather information and use military units in civilian cyberspace.

Connectivity and use of computerization resources of other elements. Global communications networks allow an attacker to cross borders and move quickly to connected targets and even use the enemy's own computerization resources to attack its systems. At the same time, connectivity allows the attacked party to make use of resources among friendly nations to identify attacks and foil them before they arrive at its own doorstep.

Mutual dependence between cyberspace and physical domains. Cyberspace has two-way interdependence with physical domains. On the one hand, it enhances activity in those domains. On the other hand, it is possible to damage targets in those domains through cyberspace. In other

words, kinetic damage to physical infrastructures such as communications installations and power stations is liable to enhance cyberwar.

Ability to mass produce cyber weapons quickly and cheaply. From the moment a cyber weapon such as a worm or defense software is created, there is nothing stopping its mass replication, effortlessly and at low cost. This characteristic, which departs entirely from kinetic weapons, serves both the attacking and attacked parties.

Use of remote resources. Cyberspace allows users to reach human and computer resources in ways unfeasible in physical domains. Unlike the traditional battlefield in which soldiers are present in battle, soldiers and computer resources operating in cyberspace can be deployed in different locations and mobilized quickly by means of information technologies. This greatly improves the capabilities of using reserves in cyberspace.

Technological and operational depreciation. Technological developments and weaknesses in existing structures force frequent changes in defensive tools. Similarly, regular upgrade and development of defensive capabilities and the repair of breaches obligate users to improve the tools for attack. This is a major drawback for the attacker because it must replace large amounts of means once they are obsolete.

Low entrance threshold. Cyberspace imposes few limitations on the construction of major cyber offensive capabilities, unlike the construction of armed forces based on kinetic forces. This is due to:

a. Technology. Technological means on the free market are highly available. Attackers can even buy defensive systems used by the enemy and invest in developing attack capabilities to the point of attaining technical superiority.
b. Offensive knowledge. A considerable amount of knowledge is also available on the free market, e.g., hackers and businesses provide attack services in cyberspace, mainly to test and drill defensive structures of companies and organizations.
c. The capital needed to develop offensive capabilities is low compared to the capital needed to establish a modern conventional army.

In short, nations can establish cyberspace forces with advanced offensive capabilities at far lower costs than those required in constructing advanced kinetic forces. Organizations and groups can also acquire and operate cyber weapons, and all can hire civilians and private companies to work on their

behalf. As Deputy Secretary of Defense William Lynn said, "a couple dozen talented programmers wearing flip-flops and drinking Red Bull can do a lot of damage."[9] At the same time, it is necessary to distinguish between offensive capabilities that are liable to cause local and/or temporary damages, severe as they may be, and capabilities to undertake a widespread, extended cyberspace offensive against the enemy's strategic targets that are endowed with advanced defensive capabilities. The latter type of attack presumably requires capabilities reserved thus far for nations with high technological abilities. From the perspective of the attacked party, cyberspace defenses are available on the open market, but comprehensive cyberspace defense requires responses to a wide array of threat types and entities that are already well protected and therefore entail high costs.

Cyberspace: Traditional Security Concepts in a New Light

Security differences between cyberspace and physical domains demand the reexamination of traditional strategic concepts and their infusion with new meaning. US military documents have adopted new operational terms when talking about cyberspace warfare. Nonetheless, it seems that the primary terms for the traditional battlefield also serve the cyberspace war domain: deterrence, defense, attack, arms race, and so on. Perhaps these terms will serve the new domain for many years to come as they adjust to the new domain; conversely, this may be a transitional lexicon that will be succeeded with new terms and concepts coined within the security establishment.

The Strategic Environment

The cyberspace strategic environment[10] differs from the traditional strategic environment where – at least in Israel – it is customary to note geographical reference circles (threats). The connection between cyberspace and geography has to do with the geographical spread of computer and network infrastructures, so that the concept of geography is somewhat different in the cyberspace context. The attitude toward time in cyberspace also differs because of the speed with which bits move in the electromagnetic sphere. Cyberspace is thus liable to enhance capabilities of previous enemies, while new and different enemies that had found it difficult to engage in conventional battles, whether because of distance or geographical separation (nations without common borders), might join them. Similarly, cyberspace

creates different security opportunities and allows actors to tap allies in new ways on the basis of capabilities and presence. Consequently, and due to the priority different nations can give to development of cyberspace capabilities, new balances of power between nations or non-state organizations (terrorist groups, nationalist or anarchist hacker groups) may emerge. As a result, cyberspace creates a unique strategic environment and in general expands it.

In terms of security activities against enemies in cyberspace, it is customary to distinguish among three areas:

a. Penetrating enemy computerization systems for the purposes of espionage. This is not considered cyberwar.
b. Soft cyber warfare, i.e., activities in cyberspace designed to disrupt the enemy's functioning, such as psychological warfare, but not to cause destruction directly.
c. Cyberwar[11] – activities in cyberspace, including attacks intended to cause direct damage or destruction to the enemy, such as damage to computerized systems or targets in physical domains, by means of attacking machines controlled through cyberspace or operating them in a manner that causes damage.

In the nations of the world, the organizations charged with these sorts of activities are security services – militaries and intelligence gathering organizations. At the same time, defending cyberspace also involves many organizations within the civilian sector, including government ministries and offices (e.g., the US Department of Homeland Security) as well as private companies (security, technology, and communications companies). Creating a joint, synchronized system among all those participating in defense and allowing feedback between attackers and attacked is the central challenge for those charged with shaping cyberspace strategy at the national level.

Espionage

Espionage, an invasive (not offensive) activity prevalent in security institutions, is designed primarily to gather intelligence in a clandestine manner. The activity is not intended to damage or disrupt the enemy's systems, nor is it meant to affect the enemy directly (as long as the enemy remains unaware of the fact that its secrets have been uncovered). Using cyberspace for intelligence gathering has a long history, dating back to when

computers and software were first introduced into various communications systems. In this field, one may distinguish among three types of activity:

a. Intelligence gathering – military, state/political, technological, economic, and social – about the enemy's capabilities and intentions in peacetime and in war, in order to form situation assessments, formulate strategies, make decisions, and construct military and fighting forces.
b. Technological and economic intelligence gathering – including theft of technological and business secrets.
c. Gathering enemy cyberspace assets, such as stealing software and databases, for the purpose of using them without permission. This goes beyond knowledge theft and is closer to using looted weapons or stealing assets, and may therefore be viewed as soft cyberwar. Nonetheless, even cyber asset theft can be effected through duplication and without removing any assets from the enemy's domain.

In a world where economic and technological power may have far reaching implications for strategic balances of power, gathering and sorting cyber, technological, and economic information and assets carries much significance for the national security of both sides. Such information and assets are likely to improve the ability of the nation doing the gathering to compete on the global market and close gaps in defense R&D. By the same token, an invaded/penetrated nation is liable to lose its strategic advantages. This is an area in which gathering goes beyond the traditional need to gather information in order to know the enemy and understand the enemy's capabilities and intentions.

The *New York Times* noted an event that may be viewed as the first in cyberspace espionage: in the 1970s, Russia managed to connect to ARPANET (the US Advanced Research Projects Agency Network, the precursor of the internet). It was revealed that within the framework of a military project financed by the United States at the Center for Mathematical Studies in Geneva, the communications network modem had been connected to Moscow and was supplying the Russians with accessibility to the United States via the network.[12] Another example of a serious event of cyberspace espionage was described by Deputy Secretary of Defense Lynn: "We learned the hard way in 2008 when a foreign intelligence agency used a thumb drive to penetrate our classified computer systems – something we thought was impossible. It was our worst fear: a rogue program operating silently on our

system, poised to deliver operational plans into the hands of an enemy."[13] It may be that this description refers to an intrusion attributed to China, when the plans for Lockheed Martin's future F-35 Lighting II fighter jet were stolen, including the plans for the electronic systems of the most advanced aircraft in the world, whose development had cost $300 billion.[14]

Lynn views the intrusion of networks and the theft of secrets in cyberspace as the most common threat to date. He characterizes this threat against the United States (true also for other developed nations) as follows:

> To date, the most prevalent cyber threat has been exploitation of our networks. By that, I mean the theft of information and data from both government and commercial networks. On the government side, foreign intelligence services have exfiltrated military plans and weapons systems designs. Commercially valuable source code and intellectual property has likewise been stolen from business and universities. The recent intrusions in the oil and gas sector and at NASDAQ join those that occurred at Google as further, troubling instances of a widespread and serious phenomenon. This kind of cyber exploitation does not have the dramatic impact of a conventional military attack. But over the long term it has a deeply corrosive effect. It blunts our edge in military technology and saps our competitiveness in the global economy.[15]

Soft Cyber Warfare: Informational Message Warfare

Informational message warfare is a type of soft warfare based on information manipulation. It is a central component in the fields of psychological warfare, fraud, propaganda, and disclosure of secret information. Its purpose is to affect the opinions and conduct of the enemy and its supporters in a way that is consistent with the goals of the initiator and without using kinetic force (firepower). The flip side of the same coin is public diplomacy, whose purpose is to supply information and present the rationale of an action to the domestic audience and friends, a move critical in gaining legitimacy for the use of force. Since the transition of the mass media to the internet in the 1990s, there has been a steady rise in the use made of cyberspace for informational message warfare and public diplomacy.

The main difference between information warfare in cyberspace and cyberspace attacks is the layer under direct attack. Hence also the difference in the way the information is organized: informational message warfare usually uses information that is structured and presented in a way that is understood by the normal user (messages are information intelligible to

human beings), unlike cyberspace attacks that are carried out in the logical or physical layer in language understood only by software and electronics engineers.

The United States recognizes the great potency of informational message warfare; in Iraq, for example, it conducted online psychological warfare against al-Qaeda. At present, the Americans are working to expand this tactic to the context of fighting hostile Islamic elements in Pakistan, Afghanistan, Iran, and the Middle East. The Americans have also embarked on an effort to change their negative image in the Islamic world, as evidenced by testimony submitted before the United States Congress in March 2011 by General David Petraeus, Commander of the US Forces in Afghanistan (July 2010-July 2011). In his testimony, General Petraeus reported on the effort to increase espionage activities on social networks in order to fight radical ideologies and anti-US as well as anti-Western propaganda. As part of this effort, software is being developed that will allow stealth intervention in social networks. For example, an American company based in California won a tender issued by the US military to develop online management services that would allow one operator to manage ten fictitious identities on the internet simultaneously. All identities would be furnished with a detailed background history and use different servers around the world in order to create the impression those responders were located in different places. The software would allow intervention by impostor talkbackers and bloggers in discussions in Arabic and Farsi and other languages spoken in Pakistan and Afghanistan.[16]

The US Air Force is equipped with C-130 Hercules airplanes charged with carrying out psychological warfare missions, such as penetrating TV and radio broadcasts in enemy states and broadcasting messages against the regime and other messages meant for the local populations. The planes also serve as relay stations that allow the establishment of cell phone networks that can provide the population with cell phone and wireless internet services and allow for communication with the population should the regime attempt to cut off connectivity. In other words, this can take control of the electromagnetic field and cyberspace out of the hands of the regime and place it in the hands of an intervening party.[17]

An example of the power of informational message warfare is the cyberspace component in the 2011 Middle East uprisings. Young people

using informational messages and cyberspace functionality succeeded in generating regime change in Egypt and Tunisia. Here cyberspace is a supporting and influential mediator, though in these cases the enemies of the authoritarian regimes are their own citizens rather than external entities. Another field of informational message warfare is the exposure of enemy secrets in order to cause damage. Such exposure can entail planned activities, illegal activities, embarrassing statements by leaders, and so on. In this field, one may note the activity of political individuals and organizations against state establishments.

Soft Cyber Warfare: Sanctions

Sanctions constitute soft, non-clandestine warfare designed to punish the party violating the rules (from the point of view of whoever is imposing the sanctions) in order to cause the violator to change its conduct and deter it from doing so again, or to weaken it should it seek to use other levers of power. There are many types of sanctions against a violating party, from denial of cooperation and other rights, through ostracism, to a blockade on borders (such as the blockade by the coalition headed by the United States against Iraq during Saddam Hussein's regime). Cyberspace is an attractive domain for sanctions because technically it is relatively easy to enact operations that have a significant impact, such as preventing communications with foreign nations. At the same time, instituting effective cyberspace sanctions obligates the formation of a coalition of relevant nations.

Cyberspace sanctions can be imposed as part of a package of sanctions in place against a rogue nation or as part of a general formulation of rules governing cyberspace. General (ret.) Michael Hayden recalls that in the past the American administration considered possible actions against nations from which cyberspace attacks against the US originated, such as different forms of cyberspace ostracism or a response that would threaten or damage internet traffic in the country that was the source of the attack.[18]

Cyberwar

Cyberspace belligerency is an act of warfare against an enemy in the domain of cyberspace designed to cause harm to the enemy in order to damage its functioning and cause it to act according to a script dictated by the attacker. By itself, a cyberspace attack cannot wrest a decision or produce strategic

achievements, such as occupying land by ground forces, but it is capable of striking critical enemy targets and capabilities. In his testimony before Congress in April 2010, the Commander of the US Cyber Command listed the types of targets susceptible to cyberspace attack: aerial defense systems, military weapons and command and control systems, civilian infrastructures such as the electric grid, the financial system, and systems of transportation and communications.

A cyberspace attack is thus likely to be a component in every modern war in the future, alongside other force components. The unique features of cyberspace also make it attractive for the periods that separate conventional wars. Cyberspace attacks may serve the following functions:

a. A means of leveling pressure on the enemy to change its policies (e.g., the attack against Estonia attributed to Russia) between conventional wars.
b. Foiling security risks in the making, such as the development of non-conventional weapons.
c. Constructing attack capabilities as part of the balance of deterrence.
d. A counter-response – cyberspace attack against attackers or against nations that are the source of cyberspace attacks

Although the subject of attacks in cyberspace is not regulated by international law, offensive cyberspace activity could be considered an act of war, as opposed to cyberspace espionage, which does not involve immediate concrete damage and is not considered as such.[19]

Cyberspace attacks usually occur in the logical layer, but there is also offensive activity that makes use of the hardware component. One may distinguish between two types of attack: one is an attack in cyberspace designed to disrupt or damage the enemy's cyberspace (computers, networks, databases, etc.) in a way that prevents the enemy from taking advantage of the cyberspace domain for its own benefit (e.g., the attacks attributed to Russia against Estonia and Georgia); the other is using cyberspace to attack devices connected to it (infrastructure installations, means of warfare, etc.) such as the Stuxnet attack in Iran.

Senior American officials stress that currently, cyberspace attackers are in a better position than targeted parties. According to Lynn, the attackers' advantage stems from the fact that the internet was fundamentally designed to be open and is built to ensure the flow of information and entry of new technologies, whereas network security was seen as being of secondary

importance. These structural issues, which have contributed to the internet's development, have endowed attackers with an inherent advantage. This can be demonstrated by comparing anti-virus software to malware. A sophisticated anti-virus system (February 2011) has some 10 million lines of code compared to 1 million just a year ago. Nonetheless, malware with 125 million lines of code (its length as of one year ago) is capable of penetrating anti-virus software. Lynn distinguishes between cyberspace attacks whose purpose is a disruption limited in time and scope, such as hacker attacks or shutting down a website by using relatively simple attack means, and cyberspace attacks whose purpose is to damage and destroy the enemy's cyberspace infrastructure. While such attacks have yet to make extensive appearances, they carry destructive potential within them.[20]

Although the cyberspace threat pales against the existential threat that loomed over the world during the nuclear age, Lynn claims there are certain parallels between them. Cyber attacks offer a means for potential adversaries to overcome overwhelming US edges in conventional military power and to do so in ways that are instantaneous and exceedingly hard to trace. Such attacks may not cause the mass casualties of a nuclear strike, but they could potentially paralyze US society. In the long run, hackers' systematic intrusion into US universities and businesses could rob the United States of its intellectual property and competitive edge in the global economy.[21]

In the range of logical attacks, intrusions making use of malware differ from methods that are not penetrative by nature, such as DDoS (distributed denial-of-service) attacks. Malware of various types is typically inserted secretly into the enemy's computers, relying on the weaknesses of the defense system. The intrusion may be from without, through global, universal networks, or from within, through a secret agent in the organization, or a combination – penetration of a local network via agents. In this family of malware there are software types such as worms and Trojan horses that allow the intruder to undertake a variety of information gathering or attack activities, such as: intelligence gathering stored in the enemy's computers (spyware), disruption of enemy computers, file erasure, control of files, and through them control of other networked computers and devices. Malware tends to spread to additional computers, sometimes in the service of the operator but sometimes randomly. Certain malware types can lie dormant in enemy computers until activated.

DDoS attacks are meant to disrupt enemy cyberspace. In attacks of this kind, websites under attack are flooded by a large number of simultaneous hits, to the point they can no longer bear the load, and crash. Such attacks use technical isolation (use of servers not identified with the attacking establishment) and HUMINT (hackers) in order to avoid incrimination. According to Lynn, DDoS attacks, meant to disrupt information systems, have up to now been relatively unsophisticated in nature, short in duration, and narrow in scope. In the future, however, more capable adversaries could potentially immobilize networks on an even wider scale for longer periods of time. Lynn notes that this type of attack was launched in 2007 against Estonia and in 2008 against Georgia, and the hacker group "Anonymous" targeted eBay and PayPal with similar attacks.[22] According to Lynn, the technical effect of such attacks is reversible, though the resulting economic damage and loss of confidence in the system may not be. Similarly, Hayden has noted that the use of DDoS attacks was one of the options examined by the American administration in its attempt to act against nations that are the source of attacks against the United States, because attacks of this kind fall within Geneva Convention limits.[23]

Offensive use of hardware is yet another way to penetrate enemy cyberspace. Lynn has stressed that the threat to the attacked party stems not only from software but also from hardware, which can be loaded with secret components that serve whoever installed them; identifying these is a much harder proposition. According to Lynn, computer companies, including Microsoft, have started to check and monitor this type of threat and suggest that governments take similar precautions.[24]

In their article "Cyber-Weapons," Thomas Rid and Peter McBurney define weapons as "a tool that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living things."[25] However, they point to the divergence inherent in the concept of cyber weapons. In their view then, cyber weapons are a subset of weapons, or in general terms, a "computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings."

Table 2 charts different types of cyberspace attacks. Table 3 summarizes different levels of cyber aggression.

Table 2. Type of Attack in Cyberspace

Attack	Characteristics
1. Disrupting the enemy's computerization	Attacks that do not change computerization configuration but create an artificial overload on the system, causing functional paralysis and disruption for a certain period of time, e.g., DDoS attacks
2. Damaging the enemy's computerization	Attacks that damage and destroy computerization, changing computerization configuration or databases, and prevent the enemy from using cyberspace to its own advantage
3. Using enemy cyberspace to damage devices connected to cyberspace or using them to cause damage and destruction	Attacks that are not necessarily meant to change computerization configuration because they rely on cyberspace to attack computer-embedded systems (critical infrastructures, weapons systems)

Table 3. Security Activities in Cyberspace against Enemies

Actions	Targets and features	Examples of limited damage	Examples of extensive damage
1. Espionage			
a. Information gathering	a. Attaining information for the sake of making decisions and carrying them out and attaining superiority in information about the enemy (not cyberwar). b. Features: secret activity, especially in the logical layer. Not designed to affect computer configuration, databases, or users. c. Not considered an act of war.	Revealing specific tactical or operational secrets to the enemy.	Revealing strategic secrets (loss of element of surprise in war). Attaining superiority of intelligence over the enemy.
b. Gathering (theft) of intellectual property and cyberspace assets	a. Gathering activity to attain technological, military, or business superiority (soft cyberwar). b. Features: similar to information gathering.	Loss of intellectual property and certain cyberspace assets.	Loss of technological, military, or business advantage; severe damage to competitive edge.

Actions	Targets and features	Examples of limited damage	Examples of extensive damage
2. Informational message warfare (psychological warfare, propaganda, revealing secrets)			
	a. Using open or hidden informational messages designed to cause a change in conduct of enemy or elements affecting the enemy (soft cyberwar). b. Features: manipulating information vis-à-vis the user layer in cyberspace. Not meant to damage functionality of enemy's computer systems.	Revealing secrets causing short term damage to operational plans. Damage limited to public diplomacy.	Falling victim to strategic fraud, changing the nature of the war. Severe damage to legitimacy of state or regime.
3. Cyberspace sanctions			
	a. Cyberspace ostracism of enemy designed to cause a change in its conduct (soft cyberwar). b. Features: cessation of contacts in services and trade in computers and communications.	Disruptions to cyberspace activity.	Extensive and extended paralysis of cyberspace.
4. **Cyberspace warfare** (cyberwar)			
a. Cyber attacks within cyberspace	a. Attacking enemy computer systems in order to damage enemy's functionality (cyberwar). b. Features: dynamic action, in particular at the logical layer. Hardware activity also possible. c. Could be considered an act of war.	Damage limited to databases and temporary disruption of cyberspace.	Extensive and extended paralysis of cyberspace, extensive loss of critical databases.
b. Cyber attack of devices connected to cyberspace	As above, except that the attack goes beyond cyberspace and directly affects the functioning of devices and systems that are outside the domain.	Damage to the functioning of a few isolated industrial plants. Rapid recovery.	Severe damage to infrastructures, military capabilities. Much damage to property, even loss of life.

Deterrence

The weakness of the traditional concept of deterrence vis-à-vis cyberspace is clear, since the perpetrator of the attack is not always known and the attacker may be making use of third party infrastructures. Furthermore, attaining deterrence obligates one to present classified capabilities whose exposure would render their relevance null and void. In addition, the short history of cyberspace attacks has not yet clarified the "price tag." In his testimony before Congress, Lieutenant General Keith Alexander, Commander of the US Cyber Command, said: "Cyber warfare has unique and important differences from classic deterrence theory and escalation control."[26] Among the ways to create deterrence in cyberspace are warnings to aggressive nations[27] and limited attacks against enemies in order to demonstrate capabilities, even at the cost of exposing certain capabilities. Despite the difficulties in presenting deterrence, balances of deterrence between nations are possible in cyberspace.

Defense

The development of cyberspace as a domain critical to national function gives rise to the need to defend the domain and prevent harm to targets outside cyberspace by cyberspace means. The more a nation uses cyberspace for its own benefit, the more it is vulnerable to damage and exposes its infrastructures to damage. This is true also of defense establishments. The more that armed forces and defense organizations rely on cyberspace, the more their dependence on cyberspace for their very functioning grows, as does their exposure to cyberspace damage and to related systems. Cyberspace vulnerability also stems from cyberspace's reliance on the electromagnetic field and its infrastructures. Defense in cyberspace must cope with a wide range of intrusions, from entries designed to gather intelligence to cyberspace attacks. A defense structure must contend with a range of enemies, including nations, terrorist organizations, malicious insiders, criminals, and hacker groups motivated by ideologies or other rationales – and in addition, contend with accidents.[28]

Despite the well-known adage about cyberspace being "a domain without borders," one may distinguish between global cyberspace and state-limited cyberspace. The latter means computers, mechanical systems and networks, software, computerized information, contents, and traffic data and control

in use by a nation, and the users of all of the above (see the UN definition early in this chapter).

Defense in cyberspace is a new kind of challenge, in part because of the enemy's capability to attack with the speed of light. Moreover, a small breach of one weak link – whether human or technological – is enough to cause a defense already in place to fail. Indeed, cyberspace enhances a hostile element's ability to take advantage of breaches in the defensive systems, while security systems are often powerless against malicious acts by insiders who have permission to operate in the system. In addition lies the difficulty in identifying the attacker. General Alexander has explained that when detecting a cyberspace intrusion, one cannot determine the purpose of the activity and therefore at the initial stage the distinction between espionage and an attempted attack in the domain may be difficult. The distinction between espionage and attack is important when considering a countermove, because nations go to war after being attacked but do not respond to espionage the same way, since espionage has traditionally not been considered an act of war.[29]

According to a 2010 US army document,[30] cyber defense comprises actions that combine computer network defense and critical infrastructure protection in a broad framework from which it is also possible to react to an attack or launch a preemptive attack. As part of cyberspace defense, there are measures to prevent and reduce risk and damage to critical computer communications infrastructures, including: redundancy (redundant capabilities and backups), isolation of certain information systems, separation between systems, deployment of conventional information security structures at several layers, physical protection of information systems, rigid and changing information security procedures, and heightened user culture.

A (partial) response to the challenge of cyberspace attack speed may be found in the concept of dynamic cyber defense, one of the prominent features of a comprehensive defense strategy in cyberspace formulated by the Pentagon. This concept is based on advanced intelligence capabilities to identify activity on the web, mechanized defense systems to identify attacks and generate automatic response without human intervention, and offensive capabilities for the purpose of foiling enemy activities.[31]

Thus, it is clear that the concept of information security (whose purpose is to guard information from theft, destruction, and glitches) does not begin

to cover cyberspace defense and the protection of systems linked to it, such as critical infrastructures and weapon systems. In reality, the most destructive actions – use of the domain in order to damage such systems – can be effected without damaging computer configurations in any way.

Early Intelligence Warning

The concept of early warning does not require much adjustment for cyberspace in terms of analysis of strategic intentions and the methods of action and tools available to the enemy. However, the challenge is different with regard to operational and tactical warnings where it is necessary to relate to the details of the attack and its timing. Preparations for attack in cyberspace may occur in utmost secrecy, unlike widespread preparations needed to organize conventional troops for war, which are easily leaked. It is often hard to know in real time that a cyber attack has begun before its results are felt; it may also be that the results are never felt (and will be dismissed as a glitch in the system). A different question is the purpose of the warning in a reality in which an attack occurs with the speed of light and what operational defensive moves it could possible serve. The need of the US military to base itself on dynamic cyber defense, which reacts automatically as soon as an attack is identified, is indicative of situations in which it is impossible to rely on traditional tactical warnings (such as warnings supplied by observation posts to field unit commanders about the advance of enemy forces).

Joining of Forces

Synergy and joined forces of various types in war allow one to attain a systemic effect in which the whole is bigger than its parts. The nature of cyberspace bears this idea out to a great extent. A cyber attack may be incorporated with kinetic fighting, electronic warfare, and informational message warfare. In some cases cyber warfare may be the primary trend (main effort), whose other force components serve in a supporting role, while at other times cyber warfare can be used to assist other force components.

Inter- and Intra-national Cooperation

Cooperation is central to cyberspace defense, as the domain crosses borders, sectors, and organizations. Intra-national cooperation in cyberspace is unique

in defense. Unlike the field of offense, whose responsibility lies with the nation's security forces, the establishment of an effective national defense system requires concentrated cooperation between the civilian sector (private and public) and the military, since it is very hard to separate civilian from military cyberspace infrastructures, and a significant portion of cyberspace capabilities of a nation lies in private hands. Therefore, multidimensional cooperation is necessary: on one axis, cooperation and synchronization within the public sector, between the civilian and the military; and on the other axis, cooperation between the public and private sectors (leading technology, communications, security, critical infrastructure, and other companies). In addition, cooperation with foreign nations is an important component, given the universal nature of cyberspace. For example: by means of joint monitoring of networks and intelligence cooperation it is possible to improve early warning, traceability, and response.

Chapter 2

Cyberspace Attacks and Restraints

This understanding of cyberspace as a domain of warfare provides good background for a brief historical survey of state-attributed cyber attacks. This category does not include intrusions for the sake of espionage, psychological warfare, or criminal activity, and thus the list of cyber attacks attributed to nations is quite short. Although Western nations seem to be anticipating massive cyber terrorism, to date there is no evidence of any significant cyber attack perpetrated by a terrorist organization.

Assessments that have appeared in various publications purporting to identify states behind certain attacks have not relied on solid evidence, rather on experts' conjectures based on an analysis of motives, scope, sophistication, and other attack elements. Thus far no nation or terrorist organization has ever assumed responsibility for a cyber attack.

Prominent Cyber Attacks

The first cyber attack is said to have occurred when the CIA planted malware in an American-made computerized control system, which was then stolen by the Russians and transported to the USSR via Canada. The Soviets installed the control system on the trans-Siberian gas pipeline in July 1982; shortly afterwards, it exploded because the CIA had tampered with the software so that it would, according to the memoirs of Thomas Reed, "go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds," producing "the most monumental non-nuclear explosion and fire ever seen from space." According to Reed, the purpose of the operation was to stop Soviet technology and intellectual property thefts. This event may be viewed as the opening salvo of cyberspace warfare.[32]

The first significant attacks on the modern network have been attributed to Russia. In 2007, many Estonian government websites were attacked and disabled for two days in an attack that made use of the DDoS method. For Estonia, one of the most advanced nations in the world in terms of computer and internet use, this was a serious blow to governability. The widespread use of computers was revealed as a weakness in light of the extensive attack that took place entirely in cyberspace.[33] The Russian-attributed cyber attack was purportedly motivated by the Estonian government's decision to move a monument, erected in memory of World War II Red Army soldiers, from the capital, Tallinn, to the suburbs. As a result of the attack, NATO signed an agreement of cooperation with Estonia, a NATO member, designed to help it if attacked in the future.[34] The attack heightened US awareness of cyberspace threats from enemy nations and made cyberwar a part of global consciousness. Indeed, many essays and articles cite the attack against Estonia as a turning point.

In 2008, Georgia came under cyber attack in an event also attributed to Russia. This attack too made use of the DDoS method, damaging many public servers and shutting down government websites. Unlike the attack against Estonia, however, the attack on Georgia was not a stand-alone event: rather, it preceded the invasion of the country by Russian ground troops. It seems that the cyber attack was meant to damage communication between the regime and the citizenry. The US Cyber Consequences Unit (US-CCU) traced this attack to civilians in Russia, Ukraine, and Latvia. It alleged that the attackers, who had been recruited with the aid of social networks, had advance notice of Russian military intentions and received support from Russian organized crime. Their targets included government and news media websites, financial institutions, and business associations, as well as educational institutions.[35] The attack is an example of cyberwar serving as ancillary to an overall military effort.

Other examples of attacks involving DDoS or intrusion of websites:

a. Attacks attributed to North Korea: In July 2009 American websites, including governmental sites (such as NASA, FBI, and CIA), and civilian sites (banking, media, and commercial) came under attack. At the same time, sites in South Korea were also targeted. The attacker was never identified, but the suspicion is that North Korea was reacting to sanctions enacted against it at the time.

b. In November 2010 there were two-sided battles in cyberspace between Indian and Pakistani hackers, leading to mutual attacks on government websites of both nations. In this skirmish, 270 websites in India were attacked in retaliation for the attack on 40 websites in Pakistan.
c. Israel has been targeted for attack by Hizbollah, Saudi, Turkish, North African, Palestinian, and other hackers on official and commercial websites (e.g., the Bank of Israel, Tel Aviv Stock Exchange, commercial banks, news media, the Tel Aviv Municipality, El Al, and more). The frequency of attack has increased during security emergencies, such as the Second Lebanon War, Operation Cast Lead, and the flotilla to Gaza, as well as during the so-called Arab-Israeli cyberwar that started in early 2012 with the release of thousands of Israeli credit card details by a pro-Palestinian hacking group.[36] Although the damage caused by these attacks was minor, Deputy Foreign Minister Danny Ayalon called them "a breach of sovereignty comparable to a terrorist operation."[37] Later, pro-Israeli hackers, including a group called "IDF Team" and a hacker named "Hannibal," brought down Iran's Press TV website and two websites belonging to the Islamic Republic's Ministry of Health and Medical Education,[38] as well as websites of the Saudi Arabia and Abu Dhabi stock markets and the SEC website of the Saudi government.[39]
d. In January 2012 anti-Israeli hackers attacked Azerbaijan's government websites, leaving threats and anti-Israeli messages. AFP reported that the Interior Ministry's homepage was replaced with a devil's image looming over a photograph of President Shimon Peres shaking hands with his Azerbaijani counterpart, Ilham Aliyev.[40]
e. In February 2012 Israel's Bank Hapoalim reported an attempt to plant a worm designed to obtain user information in the bank's personal computers. The cyber attack was launched through a PowerPoint file that was sent to some employees. Traced to servers in Iran with Canadian IP addresses, it was identified and blocked in real time by the bank's data security team.[41]

The Stuxnet attack in Iran marked a new era in cyberwar. In September 2010 it was revealed that Iranian nuclear installations had been attacked and damaged by the Stuxnet worm that was inserted during the summer of 2009. Symantec, the global security company, which has published a comprehensive report on the attack, estimated that the worm had been

adapted to damage specific frequency converters installed on Iran's uranium enriching centrifuges.[42]

Iranian President Ahmadinejad, admitting that the attack had occurred, tried to downplay its importance: "They managed to damage a limited number of centrifuges using software they installed on certain parts. Fortunately, our experts took care of it and today they can no longer pull it off again."[43] Once the attack became public knowledge, Siemens put out a kit to discover and remove the worm,[44] and the Iranians put a team together to remove it. In this case, too, there is no evidence linking anyone in particular to the attack. Given the targets and the high level of sophistication, various media publications – as well as Iran – pointed the finger at Israel and the United States.[45]

The event received extensive media coverage[46] and generated a global discussion about cyberwar. The community concerned with cyberspace protection viewed the Stuxnet attack as a formative event, and the consensus is that the attack may have signaled a leap in terms of protection and development of cyber weapons. Some of the primary strategic analyses of the event are:

a. The Stuxnet attack differed from previous attacks because it was a far more sophisticated tool focused on a particular target, unlike prior attacks – attributed primarily to Russia – which made use of relatively primitive tools and a broad front.
b. The attack was the first event in the cyberwar era in which a cyber attack spilled over into the physical domain connected to cyberspace. That is, the attack embodies the notion of attacking systems outside the cyber domain by means of cyberspace.
c. The uniqueness attributed to this cyber attack is that Stuxnet was inserted into a common computer – Stuxnet is a Windows-based computer worm – in order to attack a specific professional system of controlling industrial equipment also found in systems such as the power grid, manufacturing equipment in industrial plants, gas pipelines, dams, and power stations. Prior to this event, cyber attacks focused only on internet websites, corporate networks, and military networks. In other words, the event demonstrated the potentially enormous damage a widespread cyber attack could have on these sophisticated tools.

d. The specific virus or a weapon of its type is liable to fall into the hands of elements that would make additional use of it, such as terrorist or criminal organizations.

In December 2011 Iran reported that its cyber warfare unit had successfully brought down an American unmanned aerial vehicle (UAV) - USAF RQ-170 Sentinel drone. Islamic Revolutionary Guards Corps (IRGC) Aerospace Forces Brigadier General Amir Ali Hajizadeh stated:

> Recently, our collected intelligence and electronic monitoring revealed [the] aircraft intended to infiltrate our country's airspace for spying missions. After it entered the eastern part of the country, [the] aircraft was downed with minimum damage…The wing-to-wing width of the RQ-170 Sentinel drone is around 26 meters with a length of 4.5 meters and height of 1.84 meters. [It is] equipped with highly advanced surveillance, data gathering, electronic communication and radar systems. This kind of plane has been designed to evade radar systems and from the view point of technology it is amongst the most recent types of advanced aircraft [deployed] by the US.[47]

To the request submitted by US President Barack Obama to return the drone, Iran's President Mahmoud Ahmadinejad responded on Venezuelan state television that "the Americans have perhaps decided to give us this spy plane. We now have control of this plane." Iranian authorities claim that the drone has been nearly fully decoded and its technology will be adapted into Iran's own arsenal.

Enhanced Cyberwar Awareness

Despite the short history of cyberwar, it appears there is a profound awareness both of the growing risks and the opportunities it invites. This consciousness has been shaped by elements other than security-related factors. For example:

a. *Cyber crime* provides good reason to defend information systems regardless of the need to defend against enemy states. Common cyber crimes include theft of money, fraud, money laundering, theft of commercial secrets, extortion, impersonation, and disruption and destruction of data in databases. In all these areas, cyberspace is fertile ground for criminal capabilities. The United States apparently views cyber crime as a threat to national security (in the broader sense of the term) because this type of crime threatens the growing commercial

and corporate cyberspace activity, it has already caused considerable damage, and companies are hard pressed to overcome it. There are some assessments that global cyber crime already exceeds the scope of the criminal drug trade.[48] Foiling cyber crime also preoccupies intelligence organizations such as the FBI.

b. *Accidents and glitches in cyberspace* demonstrate the potential damage of planned attacks. On May 6, 2010, a trust fund using a computerized commercial algorithm executed one sales order of futures worth $4.1 billion. The order sparked a chain of events resulting in the steepest drop ever experienced by the NYSE (the Dow Jones plunged by more than 9 percent in a matter of minutes).[49] This is indicative of the capital market's sensitivity to software-based activities. Similarly, glitches and damages stemming from computerized system shutdowns are fairly common and illustrate the growing dependence of both the market and the public on cyberspace. In Israel, Bank Hapoalim's software glitch in November 2008 halted the bank's operations, and a software malfunction in Cellcom's communications system in December 2010 caused the network to crash throughout Israel.
c. *Extensive public and media discourse* (e.g., articles in the media, academic conferences, and professional essays) stress the population's growing dependence on cyberspace in every aspect of life and the implications of damage to the domain. There are experts who downplay the risks of cyberwars, but they are in the minority.
d. *Culture*: Movies, computer games, and futuristic books all illustrate the potential of cyberspace as a domain of warfare (e.g., the 2007 movie *Live Free or Die Hard*). In light of rapid technological advances, some of the futuristic scenarios in movies of just a few years ago seem totally plausible today.

Factors Limiting the Use of Cyber Weapons

In light of the immensely powerful threat, how does one explain the low number of actual cyber attacks that states have carried out thus far? First, not every nation has sufficient capabilities to attain significant results; although not enough by themselves, these capabilities are a prerequisite. As for states that do have the capabilities, it seems that launching a cyber attack entails some difficult dilemmas: on the one hand, there is uncertainty about the gains

of an attack, while on the other hand, there are significant risks. Moreover, using cyber force is also a matter of political motive and circumstance.

Uncertainty exists regarding what can be achieved from a cyber attack, in part because of a lack of knowledge and experience given the short history of cyberspace warfare. Specifically, certain actions may have limited effectiveness while others may go beyond the intended scope, such as causing undesirable damage to civilian apparatus. According to Michael Hayden, damage from cyberspace attacks is more difficult to forecast than damage caused by physical attacks: this is not a video game and something will happen to someone in the real world.[50]

In addition, it is difficult to translate a cyber attack into political gain. There is, for example, no conquest of land or other targets that can be used as the basis for negotiations at the end of the war, as is the case in a physical war. Furthermore, it is difficult to ensure continuity of attack in cyberspace. In many cases, the enemy can block the breach and rebuild its systems relatively quickly compared to restoration following a kinetic attack. Therefore it is hard to create the effect of cumulative damage that would provide political pressure, as would, for example, a series of strategic aerial bombardments. Some experts view this as the biggest drawback of military-initiated cyberspace attacks, and feel that expectations of the domain are highly overrated.[51]

At the same time, there are risks to the attacker that also serve as restraining factors. The first is the risk of counterattack**.** Cyberspace attacks are liable to expose the attacking nation to counterattack, which could take place outside of cyberspace. Deputy Secretary of Defense Lynn noted:

> Thus far, nation-states have primarily deployed their capabilities to exploit adversaries' networks, rather than to disrupt or destroy them. More than 100 foreign intelligence agencies have attempted intrusions on our networks, but these intrusions are largely limited to exploitation. Although we cannot dismiss the threat of a rogue state lashing out, most nations have no more interest in conducting a destructive cyber attack against us than they do a conventional military attack. The risk for them is too great. Our military power provides a strong deterrent. So even though nation-states are the most capable actors, they are the least likely to initiate a catastrophic attack in current circumstances. We nevertheless must prepare for the likelihood that cyber attacks will be part of any future conventional

> conflict. We need cyber capabilities that will allow us to defend against the most skilled nation-state.[52]

The second risk recalls the proverb "People in glass houses shouldn't throw stones." The risks to an attacking nation are higher the more it relies on cyberspace for its own ends and the weaker its defenses are. The leading nations in cyber attack capabilities are themselves highly dependent on cyberspace and have concluded that their defenses are insufficient and that therefore they are themselves highly vulnerable. Hence, strong cyberspace defenses are likely to be a critical condition for attack, and at least for the foreseeable future nations would likely have an interest in curbing a cyberspace arms race. Nevertheless, it seems that distrust among the global players and the ambitions of some to develop offense capabilities could overcome this interest and lead to an acceleration in a cyberspace arms race.

There are also risks derived from third parties (such as neutral nations or international communications companies). The use of infrastructures of a third party to launch an attack is liable to be considered damaging to its interests. Another risk is causing damage to third party assets as the result of viral spillage. In severe cases, this could generate third party responses or responses from the international community.

In addition, risks derive from enemy alliances**.** For example, the damage Russia caused Estonia in 2007 aroused NATO's awareness of its requirement to defend a member nation. As a result, an attack of limited importance by Russia generated a cyberspace coalition arrayed against it. Similarly, there are risks related to the international community, precisely because there is still no international regulation of actions in cyberspace. Attacks that have the potential to cause loss of human life or damage to the functioning of a nation could be considered an act of war even on the basis of current international law. Given the vagueness of this issue, some may see the status quo as a window of opportunity for acting in cyberspace, which could slam shut once there is such regulation, while others are likely to expand their security spheres in order to avoid unexpected retaliation by enemies or the international community.

Two other dilemmas facing one who initiates a cyber attack concern exposure of capabilities and conflict of interests. A cyber attack, for example, is liable to expose sensitive capabilities to a nation's enemies at large (not just the one under attack), which in turn would hurry to defend them or even

use them to launch attacks of their own. Therefore many cyber weapons are considered disposable, i.e., from the moment they are revealed it is hard to rely on them for further attacks. In addition, in the intelligence services, attacks may come at the expense of information gathering, both in terms of resource allocation and in terms of the dilemma between gathering information versus attacking a target, which is the source of the information. While a cyber attack entails significant risks, the accelerated development of cyberspace as a domain for data gathering is virtually free of dilemmas for the party that is gathering. It is not intended to be exposed, does not pretend to change the enemy's systems, and is not designed to arouse a severe countermove should it nonetheless be exposed.

Cyber Terror

Cyber terror is an act of terrorism that occurs in or through cyberspace. Experts agree that cyberspace can attract cyber terror, e.g., terrorist organizations causing critical installations such as oil refineries to explode by means of viral control mechanisms.[53] Terrorist organizations such as al-Qaeda currently make extensive use of cyberspace for internal communications and propaganda, but not for cyber attacks.

In February 2011, Deputy Secretary of Defense Lynn said that the United States' biggest worry was that terrorist organizations would attain the same capabilities of cyberspace disruption and destruction currently in the hands of nations. According to Lynn, al-Qaeda has promised to launch cyber attacks, although it has not done so to date. In the future, terrorist organizations may develop cyber attack capabilities or buy them on the black market; a few dozen talented hackers are liable to cause much damage (i.e., acts of cyber terror are possible even without reaching the level of cyberspace capabilities of nations); and in any case it will be hard to track down terrorist groups operating in cyberspace.[54]

Terrorist organizations may be avoiding attacks through cyberspace for several reasons. One, they have incomplete capabilities to attain the effects that would generate significant amounts of damage.[55] Two, terrorist organizations currently prefer real, not virtual, blood-soaked suicide terrorism, which from their perspective yields much more than anonymous cyber terror.[56] Three, there can be a conflict of interests. Terrorist organizations are not necessarily interested in changing the rules of cyberspace in light of their

extensive use of the domain for their own benefit, such as managing their organizations, maintaining communications between activists, appealing to certain target audiences, and conducting informational message warfare. Four is a cost-benefit issue. While developing effective cyber weapons is less costly than building conventional armies, it is vastly more expensive than operating suicide bombers.

Of these hypotheses, the first is likely the primary reason there has not yet been any cyber terror.

International Regulation of Cyberspace Activity

Efforts have been made to formulate an international treaty to regulate permitted cyberspace activity to defend global infrastructures, but it is unclear when such a treaty may be signed or the extent to which it may be effective. The efforts are coordinated by the UN agency for information and communication technologies, the ITU. In February 2010, the head of the ITU called on nations to advance the treaty before the world heads for cyberwar.[57] According to the *Washington Post*, by mid-July 2010, the UN formulated a proposal for an agreement to deal with reducing the risk to computer networks, and it was signed by representatives from fifteen nations, including the United States, China, and Russia. Among the recommended steps: the UN would create a code of conduct for what is acceptable in cyberspace; nations would exchange information about legislation and security strategies for cyberspace; and the ability of less developed nations to protect their computer systems would be enhanced. The *Washington Post* added that in 2005 the group had failed to arrive at a shared understanding, but that this time, using a short text with shared principles, the group managed to arrive at a joint formula. According to an American government official, the agreement reflects progress in the sides' understanding of the need for an international effort to confront the risk.[58]

Nonetheless, differences of opinion between the powers about the nature of the treaty and its enforcement are making it difficult to attain more concrete progress towards a detailed, effective international treaty. For example, an American official defined the difference of opinion between the United States and Russia as follows: "They want to constrain offense. We needed to be able to criminalize these horrible 50,000 attacks we were getting a day."[59] Elsewhere it has been said that Russia wants an international

treaty to prevent the next arms race and wants to maintain limitations and supervision of cyberspace as a domain of offense, similar to ABC weapons. The United States, on the other hand, does not support the establishment of a separate international agency to limit cyberwar and feels that a better way is effective cooperation and enforcement of international law. The Americans view the enforcement of an international treaty as problematic because in cyberspace it is almost impossible to distinguish between someone attacking under the aegis of a state establishment and someone acting independently.[60] The apparent concern is that a particular framework might limit America's superior cyberspace capabilities but not restrain activity against the United States.

An Interim Balance Sheet

Cyberspace is already an attractive battlefield because of its unique features and intrinsic importance to state functions. The relatively scanty history of cyber attacks is presumably due to restraints that discourage use of this domain for attack and the lack of sufficient preparedness for cyberwar. Such preparedness requires both defensive and offensive capabilities of a very high order. In order to generate wars in the new domain, appropriate security establishments are also required for development of capabilities in the field. Indeed, in recent years, nations have been working to accelerate their preparations to act in cyberspace and are building security establishments. This activity may be evidence that nations assume that the restraints currently keeping cyber attacks in check are temporary in nature; thus, nations cannot afford to risk being unprepared for war in the new domain. In any case, constructing capabilities may itself be accelerating the development of cyberspace as a domain of military warfare.

An analogy can be made between the global development of cyberspace and the development of the aerial domain as a military battlefield. In 1908, five years after their first flight, the Wright brothers signed a contract to manufacture planes for the US military. In World War I (1914-18), new combat planes flew into the landscape of war above the heads of familiar cavalry forces. In 1917, as the United States entered the war, the US military established its Air Service, which provided defense and assistance to ground troops and had great success in aerial battles. In April 1918, Great Britain established the Royal Air Force. In World War II (1939-45), the RAF played

a central role in defending Great Britain and fought the German Luftwaffe for aerial superiority in the skies over the British Isles while also serving as the long arm of the Allies' strategic attacks in the depths of Germany. The aerial domain obtained its strategic importance during the first half of the twentieth century as it became viewed as a domain for military activities of a new kind, allowing one to reach the enemy's soft underbelly quickly and without engaging its ground forces. The development of the aerial domain as a strategic sphere came about because of thee factors: technological developments and their utilization for military needs, national security challenges, and the construction of security establishments to see to the operational implementation of the new technology and its being leveraged for strategic ends using national resources.

The development of security establishments for cyberspace is now analogous to the point at the end of World War I on the aerial power timeline. The construction of security establishments for cyberspace may generate a similar revolution in military thinking and action. Cyberspace has the potential for more rapid development than the aerial domain, but its realization depends on political motivation affected in part by security events. In any case, it seems that in the near future nations will probably seek superiority in their cyberspace and establish cyberspace branches of their armed forces to act beyond the domain to realize national goals independently or together with other forces, similar to the development of air forces throughout the world.

Chapter 3

Preparations for the New Security Challenge in Selected States

This chapter deals with state preparations for the cyberspace challenge, including a description of their respective strategies and organizations to confront the challenge. It gives examples of practical expression of the characteristics and concepts described in the previous chapters. Discussed below are US preparations, focusing on the new Department of Defense strategy, as well as actions taken by France, Germany, Great Britain, and Australia in terms of cyberspace security, with emphasis on the preparations of the civilian sector at the national level. This will be followed by a review of China's offensive strategy.

American Preparations for Cyberspace Defense

The Cyberspace Threat to the United States

Over the past decade, American awareness of the cyber threat against it – emanating from nations, terrorist organizations, criminals, and others – has grown, leading to the formulation of a cyber strategy. In *The National Strategy to Secure Cyberspace*, issued by the White House in February 2003, President George W. Bush wrote: "The way business is transacted, government operates, and national defense is conducted have changed. These activities now rely on an interdependent network of information technology infrastructures called cyberspace."[61] The document points to the dramatic increase in cyberspace threats and to ways of dealing with these threats. In the years since the document's publication, cyber threats against the United States have only increased.

In mid 2009, President Barack Obama defined the cyberspace threat as "one of the most serious economic and security challenges we face as a nation." According to Obama, "the digital infrastructure we depend on every day is a strategic national asset, so keeping it secure must be a top national priority. Cyberspace is real and so are the risks that come with it." He stressed that the United States depends on cyberspace in every way, from military systems to the power grid, while the growth of America's economy in the twenty-first century depends on cyberspace security. He expressed concern about the possibility that the United States would come under cyberspace attack.[62] The *US National Security Strategy*, published in May 2010 by the White House, similarly highlights the cyberspace threat against the United States and determines: "The space and *cyberspace* capabilities that power our daily lives and military operations are vulnerable to disruption and attack."[63]

An example of the military's strategic dependence on cyberspace is the GIG (Global Information Grid), which contains a wide range of communications means (including satellites) deployed globally. The network allows the United States to transmit information between different points around the globe quickly, reliably, and securely. This capability allows the US to transmit commands to its troops, guide smart bombs to targets using GPS, control UAVs from one end of the world to the other, and more. Should the network be damaged, the US is liable to lose the dominance it currently enjoys in battlegrounds around the globe.

On February 15, 2011, Deputy Secretary of Defense Lynn listed three types of cyberspace threats: network exploitation, network disruption (e.g., denial of service), and sabotage for the purpose of destruction. In his opinion, the latter is the most severe, and is coming into being only now; the means already exist and it is now apparent that the capability to realize the threat exists as well: "It is possible to imagine attacks on military networks or critical infrastructure – like our transportation system and energy sector – that cause severe economic damage, physical destruction, or even loss of life." According to Lynn, the transition in cyberspace currently occurring – from disruption to destruction – is an expression of the escalation of the threat. As the threat develops, there will be more ways to manifest that threat:

> We stand at an important juncture in the development of cyber threats. More destructive tools are being developed, but have not yet been used. And the most malicious actors have not yet laid their

> hands on the most harmful capabilities. But this situation will not hold forever. Terrorist organizations or rogue states could obtain and use destructive cyber capabilities. We need to develop stronger defenses before this occurs. We have a window of opportunity – of uncertain length – in which to gird our networks against more perilous threats.…It is possible that destructive cyber attacks will never be launched. Regrettably, however, few weapons in the history of warfare, once created, have gone unused. For this reason, we must have the capability to defend against the full range of cyber threats. [64]

In November 2011 the Pentagon's Defense Advanced Research Projects Agency (DARPA) convened a "cyber colloquium" for what it called a "frank discussion" about the persistent vulnerabilities within the Defense Department's data networks. The agency posited that the Pentagon lacks the capacity to defend those networks. In reference to the Internet, DARPA's director Regina Dugan said:

> It is the makings of novels and poetry from Dickens to Gibran that the best and the worst occupy the same time, that wisdom and foolishness appear in the same age, light and darkness in the same season. These are the timeless words of our existence. We know it is true of everything.[65]

American Establishments for Cyberspace Security

The White House is in charge of the US comprehensive view and strategy for cyberspace defense. At Obama's side in the White House is Howard Schmidt, Cyber Security Coordinator and Special Assistant to the President. Schmidt was appointed to this position in December 2009 and is, among other responsibilities, in charge of coordinating and synchronizing the administration's policies and assisting the president in managing crises in cyberspace security.

The National Cyber Security Division within the Department of Homeland Security is the specific entity in charge of implementing cyberspace strategy. The NCSD sees its role as follows: "The National Cyber Security Division (NCSD) works collaboratively with public, private and international entities to secure cyberspace and America's cyber assets."[66] Its focus is on security of federal networks and protection of critical infrastructures. It is in charge of implementing the National Cyberspace Response System, which coordinates administrative matters, procedures, and protocols in the case of unusual events identified in cyberspace. Furthermore, the division is responsible for

the Cyber-Risk Management Program, designed to map the risks and reduce them using cost-benefit considerations. The Division deals with coordination between official state authorities and with information sharing between various institutions and agencies (including sharing with the private sector), and also focuses on early warning about hostile activity in cyberspace. There is also close cooperation between the division and the US Cyber Command (CYBERCOM) in the United States Department of Defense.

The Department of Defense is in charge of cyber defense and offense in the military and assisting civilian organizations. In this regard, it states:

> DoD's depth of knowledge in the global information and communications technology sector, including its cybersecurity expertise, provides the Department with strategic advantages in cyberspace.… DoD will continue to embrace this spirit of entrepreneurship (continued investments in people, research, and technology) and work in partnership with these communities and institutions to succeed in its future cyberspace activities.[67]

To this end, CYBERCOM was established in May 2010 as part of the strategic command structure of the Pentagon. Lieutenant General Alexander, who heads CYBERCOM, said in his testimony before Congress that CYBERCOM is responsible for carrying out cyberspace missions in order to ensure freedom of action in cyberspace and reduce threats to national security. Among the concrete tasks of CYBERCOM are (based on statements made both by Lieutenant General Alexander and Deputy Secretary of Defense Lynn):

a. To be in charge of protection of all networks of the military and the Department of Defense.
b. To create a single, clear chain of command for making cyberwar decisions, from the US president to the secretary of defense to the commander of the Strategic Command to the commander of Cyber Command and on to the individual military units around the world.
c. To create partnerships with elements outside the military and Department of Defense (other government departments, the private sector) and outside the United States to share information about threats and to address shared vulnerabilities to cyber threats.
d. Operationally, to integrate cyberspace missions and synchronize effects in the global security environment; to implement a range of cyberspace missions.

e. To create awareness of cyberspace missions against the United States and issue warnings about enemies.
f. To serve as the military's representative in cyberspace in communications with various elements, including other defense establishments as well as American and foreign companies.

The American intelligence community is the most important component in America's array of agencies for cyberspace defense. A strategy document of the US intelligence community of August 2009[68] shows that strengthening cyberspace capabilities is one of the first five most important tasks currently facing the American intelligence agencies. Cyberspace provides these organizations with a wide field for intelligence gathering, attack, and defense assistance. The agencies in question, such as the FBI, also deal with criminal activity, including foiling cyberspace fraud. Intelligence agencies are charged with increasing the use of information technologies to leverage their intra-organizational functioning, e.g., to improve information and knowledge integration, manage organizational missions of the community, and mechanize purchase procedures. Currently the army and intelligence community are redoubling their efforts to develop cyberwar capabilities. It may be that this trend requires – or will in the future – the formal division of responsibility and authority for cyberwar among the agencies. Note that the NSA is part of the American intelligence community as well as part of the army and the United States Department of Defense.

America's Cyberspace Security Strategy

*P*ublished by the White House in February 2003, *The National Strategy to Secure Cyberspace* states that the objective of the strategy is to provide "a framework for protecting this infrastructure that is essential to our economy, security, and way of life." The document defines the securing of cyberspace as a difficult and unusual strategic challenge requiring cooperation between the federal and local governments, the private sector, and the citizens of America. In this context, President George W. Bush invited the private sector to become a partner of the administration in realizing the strategy, because only joint work could ensure a secure cyberspace future. Top priority was given to those matters relating to national security exposed to cyberspace, critical national infrastructures, vulnerable sectors, and large industrial

plants. A lower priority was assigned to securing smaller businesses and homes, and the lowest priority was assigned to global cyberspace.[69]

This strategy was intended as a framework to combine forces and delegate functions among all the operational agencies acting to secure America's cyberspace, including a coordinating office and a presidential assistant for securing cyberspace, the National Cyber Security Division within the Department of Homeland Security, CYBERCOM within the Department of Defense, the intelligence agencies, elements within the Department of Justice, and more. In addition, government departments were charged with coordinating all the relevant agencies in the nation to secure critical infrastructures under their authority. For example, the Treasury is responsible for securing critical infrastructures in the capital market, the Department of Energy is responsible for important energy installations, and so on.

In general, the strategy objectives remain valid to this day. The main change that has occurred is the leap that the United States has accomplished in recent years in terms of preparing for cyberwar, in part because of the realization of some of the threats. Another significant change is apparent in the American attitude to securing cyberspace outside the borders of the United States.

In May 2011 the White House presented its *International Strategy for Cyberspace.*[70] Introduced by Secretary of State Hillary Clinton, the strategy completes and updates its predecessor in the field of cyberspace activity outside the United States and attributes much importance to this subject in America's foreign affairs, defense, and economic policies. According to the new strategy, the United States will act to advance and develop a secure global information infrastructure that is dependable and free and allows international commerce, the strengthening of global security, and the encouragement of freedom of expression and innovation, and does so by constructing a culture of responsible conduct, training nations, creating partnerships, and supporting the rule of law in cyberspace. The strategy is supposed to promote at least three major considerations in securing cyberspace outside US borders:

a. The United States aims to increase its own security and the security of its allies: The United States understands that cyberspace security in a nation cannot be attained without cooperation, because networks are interconnected (even security networks, such as the one serving all NATO

members). This cyberspace feature affords opportunities (the ability to receive early warnings) but also entails risks that must be addressed together. To this end, the DoD holds that its "relationship with U.S. allies and international partners provides a strong foundation upon which to further U.S. international cyberspace cooperation."[71]

b. The United States and its allies share economic, social, political, and security interests that all depend on global networks. By means of a more secure internet and international cooperation, for example, it will become possible to promote American trade around the globe, secure intellectual property, and improve America's capabilities to deal with criminals working in or through cyberspace.
c. The United States strives to promote American values of freedom of expression and individual rights in and through cyberspace. In the introduction to the new strategy, President Obama determines that "cyberspace, and the technologies that enable it, allow people of every nationality, race, faith, and point of view to communicate, cooperate, and prosper like never before."

Several different organizations have been charged with implementation of the strategy: the State Department, the Department of Defense, Homeland Security, the Department of Commerce, and the Department of Justice.

The Pentagon's Comprehensive Cyberspace Security Strategy (Cyber 3.0) is currently in the final stage of review, and some parts have already been implemented. The strategy is both unique and innovative, and is being introduced by the Americans in a detailed manner unlike anything in other countries. The strategy dovetails with the White House strategy discussed above.

In addition, in July 2011 the Department of Defense introduced five strategic initiatives in line with the Strategy for Operating in Cyberspace:

a. Treat cyberspace as an operational domain to organize, train, and equip US forces so that the DoD can take full advantage of cyberspace's potential**.** Treating cyberspace as a domain means that the military must operate in this new domain in a fashion similar to action in traditional domains in order to defend national security. It also means that the military services must organize, train, and equip forces to perform cyber missions. Each of the services has recently created organizations to do that. To this overall end, the United States established the US Cyber Command.

b. Employ new defense operating concepts to protect DoD networks and systems**.** Unlike passive defenses that employ only after-the-fact detection and notification (based on firewalls), active defenses rely on a dynamic approach. Active defenses operate at network speed, using sensors, software, and signatures derived from intelligence to detect and stop any malicious code before it causes any damage. Because sophisticated intrusions will not always be caught at the nation's boundary, active defense also makes it possible to hunt and deflect malicious software globally. According to Lynn, although no network will ever be 100 percent secure, active defenses have significantly enhanced the security of Department of Defense networks.
c. Previously Lynn noted[72] that the cyberspace defense system deployed by the Pentagon includes three overlapping lines of defense. Two are based on commercial best practices – ordinary computer protection (anti-virus, firewalls). The third line of protection is based on government intelligence capabilities. The function of this layer is to provide highly specialized active defenses, transmit information about attacks from external sensors to defense mechanisms in the nation's cyberspace, coordinate the forces operating in the nation's cyberspace, and manage the battle on the basis of a comprehensive overview.
d. Partner with other US government departments and agencies and the private sector to enable a whole-of-government cyber security strategy. Lynn stressed the importance of securing civilian cyberspace infrastructures, without which the power grid and government offices cannot function. This, he said, is why the Department of Homeland Security's cyber mission is so crucial, and the Department of Defense must assist this effort. For example, during a natural disaster such as a hurricane, the Federal Emergency Management Authority (FEMA) uses army personnel. In this same way, military capabilities should be available to civilian leaders in order to protect networks and critical infrastructures and support government agencies' work. Lynn stressed that in any case of military assistance to civilian agencies, resources would be under civilian control and would be operated only on the basis of civilian law. To effect this, the United States established a formal cyberspace partnership between the Department of Defense and the Department of Homeland Security in October 2010.

e. As part of a pilot plan, military technologies, including active defense technologies, were given to the Department of Homeland Security in order to secure government networks. Furthermore, frameworks were instituted for joint defense between the two departments and personnel exchanges. In Lynn's assessment, these initiatives have significantly improved the capabilities of the federal government to confront cyber threats. Lt. Gen. Alexander's testimony before Congress indicated that in emergencies, the authority of the Department of Defense supersedes that of the Department of Homeland Security in everything having to do with national security, including the security of civilian cyberspace. The strategy is based on the understanding that civilian cyberspace infrastructures are critical to the functioning of the military, while it is impossible to secure civilian infrastructures properly without military involvement.
f. Build robust relationships with US allies and international partners to strengthen collective cyber security. The *International Strategy for Cyberspace* deals with this issue as well. One of the objectives of the strategy is the creation of new military alliances and the improvement of existing alliances in order to confront potential threats in cyberspace. One of the manifestations of this goal is the American effort to promote a cyberspace coalition in NATO. This effort gained momentum at a conference held at NATO headquarters in November 2010,[73] where it was agreed to confer higher priority on confronting cyber threats. It was also decided to advance the date of the establishment of the NATO Cyber Incident Response Center by three years over the original date, so that it would already become operational in 2012.[74]
g. Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

Furthermore, in November 2011, as part of the 2011 Defense Authorization Act, the DoD reported that the US reserves the right to retaliate militarily to any "significant cyber attacks directed against the U.S. economy, government or military":

> When warranted, we will respond to hostile attacks in cyberspace as we would to any other threat to our country. We reserve the right to use all necessary means - diplomatic, informational, military and economic - to defend our nation, our allies, our partners and our

> interests....If directed by the president, DoD will conduct offensive cyber operations in a manner consistent with the policy principles and legal regimes that the department follows for kinetic capabilities, including the law of armed conflict.[75]

In addition, in the National Defense Authorization Act for Fiscal Year 2012 (H.R. 1540, sec. 954, "Military Activities in Cyberspace"), Congress affirmed the policy principles and legal regimes applicable on conflicts in cyberspace:

> Congress affirms that the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, subject to –
> (1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and
> (2) the War Powers Resolution (50 U.S.C. 1541 et seq.).[76]

In his April 2010 testimony before Congress, Lieutenant General Alexander noted three tracks for such cooperation that must be promoted in order to improve the defense of the United States in cyberspace. The first track is information sharing.

> Telecommunications providers have unparalleled visibility into global networks. They can detect attacks transiting their systems, and in many cases alert customers. Often, they have the best operational capacity to respond. [The Pentagon] is working with key technology and defense companies to exchange information that improves cyber security practices and capabilities. Senior executives now meet regularly with top officials from the Department of Defense, Department of Homeland Security, and the Director of National Intelligence. This public-private partnership, called the Enduring Security Framework, not only helps identify vulnerabilities but also mobilizes government and industry expertise to address security risks before harm is done.[77]

The second track involves cooperation to strengthen internet network architecture (structure, organization, hierarchy, rules, defense protocols, and so on). In order to address the inherent imbalance between defense and offense on the internet and in order to reduce attackers' advantage, the Pentagon is seeking the help of the scientific community to strengthen internet architecture, including embedding higher levels of security and

authentication in hardware, operating systems, and network protocols. According to Lynn,

> The National Strategy for Trusted Identities in Cyberspace, a White House initiative, will lay one building block of this more secure future. [America's] digital infrastructure will not change overnight, but over the course of a generation [America has] a real opportunity to engineer [its] way out of some of the most problematic vulnerabilities of today's technology….To help spur this effort, the Department of Defense will add half a billion dollars in new research funds for cyber technologies, with a focus on areas like cloud computing, virtualization, and encrypted processing. Through our 'Cyber Accelerator' pilot, we are also providing seed capital for companies to develop dual-use technologies that serve our cyber security needs.[78]

At the same time, there is an effort underway to ensure the defense establishment's familiarity with these technologies. Lynn noted that the government sector is slow: "We must also accelerate the introduction of them inside the Department. It currently takes the Pentagon 81 months to field a new computer system. The iPhone was developed in just 24 months… We have to close this gap. Silicon Valley can help us." According to Lynn, the Department of Defense wants senior IT managers in the Pentagon to incorporate more commercial practices, and "we want seasoned industry professionals to experience first-hand the unique challenges faced by the DoD." Lynn also announced a program to better utilize cyber expertise within the National Guard and Reserve. The "Department has many soldiers, sailors, airmen, and marines who work in the civilian IT world and continue to serve their country in the National Guard or Reserves. To make better and more systematic use of their specialized skills, [the Department of Defense] will increase the number of Guard and Reserve units that have a dedicated cyber mission."

The third track of industry-government cooperation is extending the high level of protection afforded by active defenses to private networks that operate infrastructures crucial to the military and the economy. Because of America's intelligence capabilities, the government has a particular awareness of certain cyber threats. This classified "threat-based" information and the technology the Department of Defense has developed to employ it in network defense can significantly increase the effectiveness of cyber security practices that industry has already adopted. The DoD already shares

unclassified threat information on a limited scale with defense companies whose networks contain sensitive information. How classified signatures and the technology to employ them should be shared across the full range of industrial sectors that support the military and underpin the economy is a pressing policy question. There are common interests: owners and operators of critical infrastructure could benefit from the protection that active defenses provide, whereas the Department of Defense has the technology and know-how to apply them in a civilian context. The real challenge at this point is developing the legal and policy framework to do so. Lynn cited as a positive example the partnership between government and industry to solve the Y2K bug question before January 1, 2000. According to Lynn, "The challenge we face today in cyber security is similar in several respects. It is global in scope. It involves nearly everything digital. And it will require government working with industry at all levels. But unlike Y2K Bug, we now face malicious, adaptive actors, bent on harm, rather than inanimate computer code written without the millennium in mind." According to Lynn, this third track of industry-government cooperation is also the most challenging.

It appears that the Deputy Secretary of Defense introduced Department of Defense involvement in civilian cyberspace cautiously, especially when addressing the military's involvement in securing critical civilian infrastructures, apparently because of the disagreements that came to light in the past about the army's involvement in the civilian sector. For example, the survey of cyber threats undertaken by the NSA in 2009 at the request of the Obama administration aroused opposition in the Department of Homeland Security. Rod Beckstrom, who resigned as Director of the National Cyber Security Center, said he was concerned that the survey would enable the NSA to examine every e-mail, text message, or Google search of any US federal employee. According to Beckstrom, American intelligence services are supposed to gather information about occurrences outside of the United States and are not supposed to have such extensive control of information transfer within the nation.[79] In addition, after the June 2009 announcement by the Secretary of Defense of the intention to establish the US Cyber Command, there was criticism in Washington that a military organization was going to handle defense of civilian computer networks, thereby exposing their contents to the military. Other criticism focused on the fact that the

Cyber Command would give priority to securing military computer networks over defending civilian ones.[80]

The information available about US cyber strategy stresses the defensive nature of the American approach. The strategy is supposed to preserve US national assets and the nation's position as a superpower, in part based on its technological advantage over enemies, rivals, and competitors, such as China. At the same time, the cyberspace battlefield entails both defensive and offensive activity, and it seems that the United States has an advantage over every other country in terms of offensive capabilities and presence in cyberspace. Attacks in cyberspace are part and parcel of the Cyber Command's missions, not – understandably – highlighted by senior officials in America's defense establishment.

At the 2010 Black Hat security convention in Las Vegas, General Hayden spoke about possibilities of actions discussed by the administration in the past to limit attacks from other countries, be these attacks with or without the knowledge, approval, encouragement, or financing of their governments. One approach was to cease asking questions about how to identify attackers and instead lay the responsibility for attacks on the nation from which the attack was launched and act against it. According to Hayden, one could consider responses such as threats or attacks on the flow of internet traffic of the country that was the source of an attack, slowing down e-commerce, and even interfering with that nation's communications capabilities. One possibility of action discussed was launching a denial of service attack since it lies within the limits of the Geneva Convention. According to Hayden, it is possible to make nations understand that they are responsible for their cyberspace and for what comes out of it.[81]

According to Lieutenant General Alexander's testimony before Congress, if the president determines a cyber event does meet the threshold of a use of force/armed attack, s/he is authorized to determine the nation's response policy. This determination involves an objective and subjective analysis of considerations, and relies on a nation's right of self defense as recognized by the UN Charter. Today there are no agreed upon definitions, and every nation may define for itself its own threshold for the use of force, subject to international law that is not specific to cyberspace.

Prior to approving American-led airstrikes in Libya without Congressional go-ahead, the White House considered using cyber warfare against the

forces of Colonel Muammar Qaddafi. The *New York Times* reported that the Obama administration was hoping to cripple the computer systems as well as the air defense network of Qaddafi's government.[82] According to the report, the administration officials "intensely debated" if hacking into foreign computers would be a smart move during the beginning of the NATO missions in Libya, which were supported by the US. They were primarily concerned that officially entering an era of high scale computer warfare could cause competing nations across the globe to respond with cyber crimes of their own against the Pentagon. Indeed, the US has already accused China, Russia, and North Korea of cyber warfare in the past, and has denied responsibility for similar crimes against Iran.

The *Times* also reported that the Obama administration debated if cyber warfare would be required in the Navy SEAL operation in May 2011 that led to the execution of Osama Bin Laden at his Abbottabad, Pakistan compound. According to the report, the US ultimately decided against hacking al-Qaeda computers, instead relying on more traditional military routes, such as stealth helicopters and boots on the ground. "These cybercapabilities [sic] are still like the Ferrari that you keep in the garage and only take out for the big race and not just for a run around town, unless nothing else can get you there," one of Obama's officials told the *Times*.[83]

Western Europe and Cyberspace Defense

In recent years, leading West European nations such as Great Britain, France, and Germany have also accelerated preparations for securing cyberspace.

France

Recognizing the decisive impact of cyberspace on the economy, society, security, and fabric of life, France formulated a cyber defense strategy in 2009.[84] Its objectives include:

a. *To be a global power in securing information systems*: France strives to be a member of the small circle of nations that are leaders in the field, and intends to play an active role in the group of developed nations in order to formulate a shared response to the threats.
b. *To maintain a secure information system domain*: This will make it possible to make decisions and ensure the functioning of command and control mechanisms in times of routine and during emergencies.

c. *To strengthen security of critical networks and critical targets that rely on them*: France defined a list of infrastructures critical to the state, some of which are within the private sector. Securing them necessitates training the nation's industrial sector.
d. *To ensure a secure cyberspace*: To this end it is necessary to build defenses against cyber attack threats directed against government targets, private companies, and citizens.

The ways to attain the strategic objectives include:

a. Promoting monitoring of cyberspace attacks on France and providing rapid response in case of attack.
b. Increasing scientific knowledge and capabilities in cyberspace, including advancing research on the cyberspace environment in order to identify technological trends that entail potential risks. Also, a research center that focuses on subjects such as encryption, analysis of cyber attacks, and development of secure software will be established cooperatively by the academic world and private companies.
c. Securing information systems of both government and private critical infrastructures. To this end, France issued "The National Strategy of France for Securing Classified Information," and a secure internet network for government ministries was established.
d. Adjusting legislation to developments in the field of information and network technologies.
e. Developing international cooperation in fields such as information security and protection, fighting crime in cyberspace, and others.
f. Raising awareness of the issue among decision makers and the public at large.

In order to realize the strategy, several organizations at the national level were established. The Strategic Commission for the Defense of National Information Systems, headed by the Director General of the Ministry for Homeland Security, was established as a result. The commission members include the Chief of Staff, the heads of the civilian intelligence organizations, the Director General of the Ministry of Foreign Affairs, the Director General of the Ministry of Defense, a special arms representative, and senior personnel from industry. The commission's job is to outline in detail the national strategy for securing information systems and direct the Agence

Nationale de la Sécurité des Systèmes d'Information (ANSSI) – the National Agency for Information System Security.

ANSSI, established in July 2009, is organized as follows:

a. The Centre Opérationnel de la Sécurité des Systèmes d'Information (COSSI) – Operational Center for Securing Information Systems – works around the clock and is supposed to monitor cyberspace for infiltrations and respond accordingly. The Center includes the following functions: an applied cryptology center (code, identification, permissions), a control center in the field of information systems security, a response center to deal with cyber attacks, a monitoring center, a coordination function, a war room, and a planning and drilling office.
b. The Strategy and Regulation (SR) Division formulates strategy, engages in regulations, coordinates between ministries, and follows up on global progress in the field.
c. An Assistance, Consulting and Training Division (ACE).
d. A Secure Information Systems Division deals with developing and approving secure communications means for use by the professional and state echelons (does not include military communications systems).

Germany

German preparations to secure cyberspace at the national level share some features with French measures, including the establishment of a National Commission and an Operational Center to confront attacks. The strategy was published in a document entitled, "The New Cyber Security Strategy for Germany" ("Nationale Cyber-Sicherheitsstrategie"),[85] and while it deals with the civilian sector it also notes that there are complementary steps that the German military should take in order to defend its capabilities and secure Germany's national cyberspace. The strategy paper emphasizes the desire for cooperation between the public and private sectors as well as the desire for cooperation between Germany and foreign nations and institutions. The strategy names the following objectives:

a. Securing critical infrastructures.
b. Strengthening information system security in the state by, e.g., controlling computerization providers and security companies to make sure they do not spare any security measures and providing incentives to providers of security products to citizens, such as electronic proof of identity.

c. Strengthening cyberspace infrastructure security in government ministries.
d. Establishing a mechanism for responding quickly to cyber attacks (National Cyber Response Center). Accordingly, the Nationales Cyber-Abwehrzentrum (NCAZ), which is located in Bonn-Mehlem and is under the authority of the Federal Office for Information Security (BSI), became fully functional in June 2011. It brings together specialists from the Office for the Protection of the Constitution, the Federal Criminal Police Agency, the German Intelligence Agency, the customs office, the Federal Office for Civil Protection, and the military.
e. Establishing a commission for formulating policy and coordination at the national level (National Cyber Security Council).
f. Establishing a cyber codex ("Kodex") on cyber foreign policy. Among other topics, it speaks of pursuing German interests in data security in international organizations such as the UN, the OSCE, the European Council, the OECD, and NATO – in that order.
g. Strengthening the capabilities of the legal and law enforcement authorities in order to improve the nation's ability to confront cyber crime and espionage.
h. Improving cooperation and coordination with European nations and other nations in the world to secure cyberspace.
i. Using reliable information technology means.
j. Training personnel in the field of information system security in the government sector.
k. Building the capabilities for cyberspace attacks. The document notes: "If the state wants to be fully prepared for cyber attacks, a coordinated and comprehensive set of tools to respond to cyber attacks must be created in cooperation with the competent state authorities."
l. Conducting transnational cyber warfare exercises. In November 2011 Germany conducted the so-called LÜKEX (Länder Übergreifende Krisenmanagement-Übung/ EXercise) Transnational Crisis Management Exercise, led by the Academy for Crisis Management Emergency Planning and Civil Protection. The exercise simulated how Germany would react if national computer systems were to suddenly fail, ATM machines no longer paid out cash right before Christmas, or safety systems failed at airports. It involved around 3000 people from 100 different institutes, including 11 federal departments led by the Home Office, 21 federal and

37 state ministries, and 33 private companies — operators of so-called critical infrastructure — such as telecommunications, air transport, or water utilities.

Great Britain

London too has responded proactively to the decisive impact of cyberspace on the economy, society, security, and fabric of life. The summary of the Cabinet Office document published in June 2009 *Cyber Security Strategy of the United Kingdom (safety, security and resilience in cyber space)*[86] states that the digital world is a fact of our life. It further states that:

> Just as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we also have to secure our advantage in cyber space. This Strategy – our first national Strategy for cyber security – is an important step towards that goal.

The strategy of Great Britain strives to secure cyberspace by:

a. Reducing threats of hostile cyber operations by reducing enemies' motivation and capabilities.
b. Defending British interests against hostile cyber operations and defending Britain's ability to take advantage of the opportunities afforded by cyberspace for its own benefit, by means of reducing exposure and vulnerability of British interests and the impact on them if attacked by hostile cyberspace operations.
c. Gathering intelligence about threats and threatening players and actions against enemies.
d. Improving knowledge and awareness, developing a doctrine and policies, developing cyberspace decision making and governability, leveraging technological and human capabilities.

To achieve these objectives, Great Britain has decided to take several steps at the national level. One such measure is institutionalizing cross-ministerial programs to promote the strategy objectives, e.g., giving additional funding to innovative initiatives to develop future technologies for securing British networks, and developing and promoting critical skills for securing cyberspace. A second measure involves working closely with the entire public sector, industry, groups active in civil liberties, the public, and international partners. The government, together with industry, has

already engaged in a range of noteworthy activities in the field of cyberspace security. At the same time, according to the strategy paper, the challenges are so great and the task so critical that these activities must be developed even further. One of the main principles behind the strategy is the creation of patterns of cooperation that will draw on the joint knowledge and expertise of these bodies in order to achieve these goals.

In order to implement the strategy, the Office of Cyber Security (OCS), subject to the Cabinet Office, has been established. It is meant to provide consistent strategic leadership at the government level. The office is responsible for developing a strategy for securing cyberspace, coordinating between government ministries, and increasing cooperation between the government and the private sector. In addition, the Cyber Security Operations Centre (CSOC) has been established. The CSOC is an interdisciplinary operations center charged with actively overseeing cyberspace security, coordinating responses and responding to events, attaining better and quicker understanding of attacks against British networks, and providing consulting and information about cyber risks to the business and public sectors.

Australia and Cyberspace Defense

The Australian government has joined other Western nations in designing its own cyber security policy as part of the Cyber Security Strategy, which was launched in 2009. Cyber security, as the government defines, is "measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means."[87] The goal of the cyber security policy is "the maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy."[88]

In February 2011 the Kokoda Foundation, an Australian think tank dealing with security matters, released a special report titled "Optimizing Australia's Response to the Cyber Challenge." Subsequently, the Australian Attorney-General Robert McClelland stated:

> The report acknowledges the need for an integrated whole-of-government approach on cyber security and identifies a number of important issues for consideration.…The Australian Government has made cyber security a top national security priority and will continue to invest significantly in enhancing Australia's cyber security capabilities.…The Cyber Security Strategy is at the heart of the

> Government's approach to cyber threats, and recognizes the important contribution of all levels of government, business and industry in securing cyberspace.[89]

In line with the "Strategy," the Australian government has implemented a number of steps to address a variety of cyber threats, among them:

a. Establishing the Computer Emergency Response Team (CERT Australia), which works with the owners as well as operators of critical infrastructure and systems, and aims to detect and mitigate threats and vulnerabilities;
b. Establishing the Cyber Security Operations Centre (CSOC) within the Defence Signals Directorate (DSD) to coordinate operational responses to cyber events of national importance across government and critical infrastructure;
c. Creating the "Stay Smart Online" website (www.staysmartonline.gov.au), which provides an alert and information service on the latest cyber threats and vulnerabilities as well as how to address them;
d. Moving to accede to the Council of Europe Convention on Cybercrime, currently the only binding international treaty on cyber crime;
e. Working with state and territory governments to ensure a nationally coordinated response to cyber crime, including consideration of a national online reporting portal;
f. Working with the Internet Industry Association to implement a voluntary ISP code to help inform, educate, and protect customers in relation to cyber security issues;
g. Partnering with industry, community, and consumer groups on cyber security awareness initiatives, for instance, releasing the "Protecting Yourself Online – What Everyone Needs to Know" booklet, which provides information and advice in regards to online security; and
h. Establishing a cyber policy coordinator within the Department of the Prime Minister and Cabinet.

Additionally, the Department of the Prime Minister and Cabinet is developing a document called the "Cyber White Paper." The document, scheduled to be released to the public in mid 2012, will detail Australia's position in the cyber era, its approach to cyberspace issues, and likely future opportunities and challenges, as well as its strategic interests in cyberspace. The document will outline the roles and responsibilities of the government in ensuring that Australia can connect in cyberspace securely, and provide

a framework for interaction between Australian governments as well as between governments and industry. Furthermore, the Cyber White Paper will detail how Australia will work with international partners to advance a vision of a safe, secure, and resilient presence for Australia in cyberspace based on clear international norms.[90] Regarding the document, the Department states:

> Importantly for industry and the Australian community, it will also look at ways we can improve our assistance to businesses and the public so that we can all enjoy the benefits of cyberspace. The development of the Cyber White Paper will be informed heavily by the public consultation process beginning in the second half of this year, which will commence with the release of a discussion paper and website.[91]

China and the Cyber Challenge

While the strategies of Western nations bear a great deal of resemblance to one another – being essentially defensive and designed to counter similar threats and enemies – the Chinese approach affords a different strategic view of cyberspace: cyberspace as a domain of opportunities whose potential requires, among other elements, the ability to carry out intrusions in order to engage in aggressive information gathering and attack.

As a superpower of 1.35 billion people, China sees digital technologies as a rare opportunity to promote its strategic, economic, and military capabilities and its standing. The local rapid spread of the internet and cellular communications is in part evidence of this perspective. By means of advanced technologies, China is attempting to take the leap from an agrarian society (about half of China's population still lives in farming villages) to an information society, while skipping as quickly as possible over the industrial society stage. With the help of digital technologies that can be used to their advantage in the large Chinese market, China is attempting to do in a condensed period of time what took Western nations decades to achieve.

Since the late 1990s, China's activity in cyberspace in terms of security has focused on espionage in the West and attacks on political opponents around the world. According to American research on China's cyberspace strategy, in recent years China has constructed military cyberspace capabilities designed to gain strategic advantages commensurate with its status as a superpower. China sees the development of military cyberspace capabilities as a necessary strategic element to redress its strategic inferiority vis-à-vis the United States in the conventional domains. It seems that China

sees the development of cyberspace capabilities as an opportunity to achieve a strategic advantage it had no chance of attaining in the past. This is true both of taking advantage of cyberspace in order to improve the capabilities of the Chinese army and of its desire to attain offensive cyber capabilities, which in turn would endow it with cyberspace dominance that could then be translated into other domains.

According to Western publications, China represents a danger to the West in several cyber-related areas. The first area is intelligence gathering that can be turned to military advantage, e.g., exposing American weak spots and military plans, as well as gathering military and civilian technological secrets, which are the US's greatest advantage; theft of cyberspace assets (software and databases) for military and civilian use; and more. According to Western experts, the Chinese are acting primarily against targets in the United States and Europe by means of intrusion from afar and close contact, including providing hardware components encrypted with malware. In 2009, there was a report of an intrusion into American computers attributed to China, during which the plans for the future F-35 Lightning II fighter jet were stolen.

The second area concerns the development of offensive capabilities in cyberspace, liable to threaten advanced civilian and military infrastructures in Western nations. China's high technological and operational capabilities in terms of intelligence gathering in cyberspace may also be indicative of its offensive capabilities.

A third area is the economic and cultural struggle in which China challenges Western values in global cyberspace, such as freedom of information and protection of intellectual property rights. China is said to be responsible for intrusions into the computers of commercial companies for the purpose of intelligence gathering as well as for attacks against opponents of the regimes (e.g., Operation Aurora in 2009). The United States has disclosed a number of reports in this context, including the comprehensive GhostNet report released by the Information Warfare Monitor in March 2009.[92] However, China has denied any connection to the invasive cyber activity attributed to it.

More specifically, a document prepared by the American defense corporation Northrop Grumman describes China's offensive strategy,[93] whereby the Chinese military sees its developing cyberspace capabilities

as a force multiplier, both for improving its internal systemic functioning and for acting against enemies. As part of the process of modernization in the military, there are efforts to develop network architecture capable of coordinating military operations in all domains. At the same time, the Chinese view the attainment of information dominance as a key component for attaining victory in a confrontation. They are striving to gain control of the enemy's flow of information, thereby earning dominance on the battlefield. To that end, they are developing the capability of intruding into the enemy's advanced information systems for intelligence gathering, by means of which they intend to ensure success in future confrontations.

As part of its offensive approach, China is developing the capability to combine computer network attacks, electronic warfare, and kinetic blows (firepower) in order to destroy the enemy's communications systems (military and civilian) and create blind spots, which Chinese forces would then be able to exploit in real time. Command and control and logistical structures are also inviting targets for cyberspace attack because of their key to attaining military strategic objectives. Such attack operations would be used by the Chinese in the early stages of a confrontation, and perhaps even as part of a preventive move. Actions of this sort are considered a component of China's strategic deterrence, whereby this constitutes a non-violent "small war" that does not necessarily require an enemy's response and is possibly capable of preventing the "big war." Personnel in the Chinese army contend that cyber weapons have the deterrent potential equal to that of nuclear weapons, only better: they cause no physical damage. The damage they do cause is controlled and pinpointed, and the weapons can be aimed at essentially unlimited ranges.

Experts in the field of cyberspace security feel that China is currently in the midst of a concerted effort to gather classified information from the West before the latter's cyberspace information security capabilities grow stronger. Partners in this effort are Chinese governmental cyberspace units, Chinese subcontractors, and elements active in cybercrime. There is evidence of connections between Chinese establishment sources and warlike or gathering activities carried out by hackers against American and other foreign targets. Moreover, the scope of the operations, the capabilities displayed and the types of objectives targeted indicate that these were state-sponsored events.[94]

According to the document, China's intelligence gathering activities in the United States are technologically at a very high level, simultaneous, and sustained, even when aimed at several targets in tandem. Sites in the United States that China has targeted via cyberspace include military infrastructures, defense industries, the space program, private hi-tech companies connected to defense, cyberspace security elements, centers where decisions likely to affect Chinese interests are made, and more. Furthermore, in a confrontation with the United States it is quite likely that China would use cyberspace in order to attack civilian infrastructures, as these are relevant to the military, the Department of Defense, and companies employed by the defense establishment. China would in all likelihood also attack American allies in order to delay the expected American deployment in the areas of confrontation and impede the conduct of forces massed in the arena.

Unlike the United States, which desires to provide full freedom of action in cyberspace to its citizens, China acts very differently in defensive terms, maintaining close control of its internal cyber domain, especially in order to prevent political subversion. China therefore views companies such as Google as enemies. In early 2011, China went so far as to increase its oversight of cyberspace as a result of lessons learned from the use made of cyberspace by protestors in the Arab nations for their revolutionary activities.[95] In this sense, China's security services have an advantage in defending against external enemies because they enjoy complete freedom of action in cyberspace, whereas the security services of the United States are subject to rigid civil liberties laws. In another sense, a tightly controlled cyberspace's contribution to the economy is likely to be smaller than that of a domain that is free and open to ideas.

Furthermore, China has increased its protective measures against cyber attacks. In September 2011 the Supreme People's Court (SPC) and Supreme People's Procuratorate (SPP) issued legal interpretations on hacking and other internet crimes. They posited that a crime against information network poses a threat to both national security and public interests. They also stated than one million IP addresses in China were controlled from overseas in 2009, 42,000 websites were distorted by hackers, and in 2009, 18 million Chinese computers – about 30 per cent of computers infected worldwide – were infected by the Conficker virus every month.[96]

State Preparations for Cyberspace Operations

Until recently, there was little need for nations to establish special mechanisms for conducting war in cyberspace other than information security authorities. It seems that militaries, intelligence organizations, and internal security ministries all tried to manage such activity by the establishment of operative bodies in already existing units. Events of recent years and a growing understanding of the risks and opportunities inherent in the cyberspace battlefield have changed the picture and given rise to the need for reorganization. This is already underway among different nations.

To confront the challenges of cyberspace, states have reorganized in several new ways. First, there has been a transition from an information security approach to a defensive understanding. In the early 2000s, several nations founded national bodies charged with securing information systems, which were information security organizations in nature. Towards the end of the decade, organizational developments recognized that cyberspace was in fact a domain of warfare, and strategies were formulated to defend the cyberspace of the nation.

The organizational response to the cyber challenge reflected in a number of nations consists of two levels of defense. The upper level consists of the higher state echelon, coordinated by a body at the level of a government ministry (in the United States and Great Britain) or a national council (in France and Germany). This level formulates strategy and policy rules and ensures coordination and synchronization among all organizations in the nation dealing with cyberspace security. The lower level consists of operative security units or organizations, both military (such as the US Cyber Command) and civilian (such as the Cyber Security Division in the Department of Homeland Security in the United States).

There is a distinction between defensive organization, which crosses sectors, and the offensive field, which lies entirely within the purview of military establishments and the intelligence community (such as the Pentagon and the CIA in the United States). The decision to construct and use offensive capabilities takes place via a direct chain of command between these security outfits and the leaders. The chain of command in the United States starts with the president and goes through the secretary of defense, the commander of the strategic command, and the commander of CYBERCOM, and does not go through civilian organizations, such as the Department of

Homeland Security (even though out of security considerations, it should be aware of and prepared for an attack against the United States).

At the same time, the recognition of cyberspace as a domain shared by the security and civilian sectors encourages organization of a joint operative force. One of the manifestations of this kind of thinking is the establishment of shared operations centers (such as in Great Britain, France, and Germany), whose purpose is to formulate the situation assessment and assist with providing the required response. Nonetheless, these nations and the United States maintain a fairly clear separation of functions between the sectors. The civilian bodies are in charge of most of the defensive activity within these nations, while the militaries and intelligence organizations (which have the offensive capabilities) defend themselves, provide defenders with information about enemies, assist civilian units in defending critical infrastructures (especially during emergencies, in which the armies' authority is expanded), and leverage their presence and offensive capabilities in cyberspace to neutralize the sources of attack and respond against enemies. In addition, the goal of cyber cooperation with friendly nations is a prominent element in the strategies of Western nations.

Bodies of cyberspace warfare can be organized alongside nations' SIGINT organizations. In at least some places, these bodies have one commander (the commander of CYBERCOM in the United States is also the head of the NSA). The ostensible reason for this is that SIGINT organizations have the relevant human and technological infrastructures for confronting cyberwar, in addition to their vast experience in cyberspace intelligence gathering activity and their familiarity with the enemies. In other words, it seems that effective action in cyberspace requires the integration of national SIGINT capabilities.

In conclusion, it appears that the establishment of security mechanisms may generate an ongoing process of constructing tools and operational approaches and even the establishment of additional cyberwar units. Security events and the emergence of political motives for using force may of course accelerate these developments. In light of the cyber capabilities currently being constructed, one may assume that cyberwar will play a role in every modern war. As for the frequency of its use in the intervals between conventional wars, it is difficult to draw as unequivocal a conclusion: cyber powers are also subject to restraining considerations and the use of cyber

weapons also requires political motivations. Either way, in terms of force construction, the global cyberspace arms race has already begun. The United States, Russia, and China are in the lead, though other nations are also active participants.

Chapter 4

Israel's Cyber Security Challenge

Information technologies and cyberspace are strategically important for Israel. Like the economies of the most advanced nations in the world, the Israeli economy relies to a large extent on cyberspace infrastructures. Israel is one of the world's leaders in development of information technologies, and branches of information technologies, which contribute both directly and indirectly to Israel's economic growth, are of special importance. They are capable of competing on the global market (a significant portion of the products are directed abroad), which is a crucial phenomenon, because the only way for Israel to grow quickly is by increasing exports.

According to a survey by the international consulting giant McKinsey & Company,[97] the internet economy of Israel may be divided into two fields. The larger portion is the field of ICT – information and communications technology – and includes the development, production, and sale of equipment, software, and services. The smaller and rapidly growing part is the field of electronic commerce involving the sale of goods and services on the internet. According to the survey, Israel's internet economy (according to the McKinsey definition) contributed about NIS 50 billion directly to the national product in 2009, representing 6.5 percent of the GDP. This figure positions Israel as one of the leading internet economies in the world. According to the survey, Israel's internet economy is expected to grow at an annual rate of 9 percent – double the growth of the economy itself. By 2015, the contribution of the Israeli internet economy is expected to hit NIS 85 billion, which will represent about 8.5 percent of the GDP.

The internet economy contributes greatly to employment, especially of academics in various fields of technology. In addition, information technology branches make both a direct and an indirect contribution to Israel's defense

and security sector. Information technology and communications branches are integral to Israeli technological capabilities that have been recognized internationally,[98] thereby strengthening Israel's image and status in the world. Furthermore, the Israeli hi-tech industry is internationally acclaimed for its contribution to cyber security (e.g., Check Point Ltd.).

Cyberspace allows Israel to breach its geographical isolation in the Middle East and maintain close contact with the rest of the world. It can enable a stronger connection between Israel's outlying areas and the center of the country. It is a major component in social activity and an important factor in strengthening the connection between government authorities and the population.

Israeli Preparations for Securing Cyberspace

There are a number of significant milestones in the country's preparations for securing cyberspace. TEHILA (a Hebrew acronym for the Government Infrastructure for the Internet Era), established in 1997 in the office of the Accountant General in the Ministry of Finance, was intended to provide secure browsing services to government ministries and institutions. According to its website, TEHILA maintains a server farm through which hundreds of thousands of citizens receive government services and information about government ministries every month. TEHILA operates various tools to ensure security of the government internet network, from a team of information security experts to products and services offered by leading global companies.

The Center for Israel Government Information Security was established at TEHILA; among its functions are following up on information security events around the world with particular attention to network attacks of concern to Israel, coordinating among governmental bodies in order to solve security problems, connecting government bodies with external bodies, and conducting research in the field. The Center publishes information security warnings to organizations in the field of information technology that have contact with TEHILA or non-classified government sources. The project also maintains contact with international sources in order to defeat computerized attacks.[99] A CERT team (Computer Emergency Response Team) operates as part of TEHILA; its purpose is to provide immediate response to information security events in government organizations or bodies of international size.

"CERT representatives maintain an available call-in center to respond to network attacks, manage risk, create information security procedures, control traffic, deal with viral outbreaks, prevent Spam and phishing, fight network piracy and identity theft, maintain information privacy, and raise awareness about security; the team also shares information with internet providers, the police, and security forces and keeps them updated."[100] The body assumes some important tasks, yet the mandate for its activity relates to providing secure internet browsing for government ministries and institutions. It is not a shared operational-integrative organization for all institutions charged with cyberspace security, as is the case in Western countries.

In March 2011, the government approved the establishment of the governmental Information Systems Authority, an inter-ministerial body charged with coordinating the entire field of government computerization. The authority, subordinate to the Ministry of Finance, is meant to guide the computerization units of the various government ministries and be directly responsible for all lateral governmental computerization projects, including TEHILA. Concentrating all government computerization projects in one location is a great step forward in organizing the country in the field of computerization, but it would be preferable for the body in charge of securing the information systems to be outside the entity establishing and operating these infrastructures.

In 2002, the Government Authority for Information Security in the General Security Services (GSS) was established on the basis of a government decision. "The authority is charged with providing professional guidance to the bodies under its purview in the field of critical computer infrastructures security against threats of terrorism and sabotage of classified information and against threats of espionage and exposure."[101] The original rationale of placing the authority in the GSS seems to be linked to the GSS' authority to foil espionage and terrorism. Nearly one decade later, it is possible to see both the advantages and disadvantages of this assignment. An important advantage is the close connection between this authority and the capabilities and powers of the GSS (as specified in the GSS Law) and the intelligence community, in which the GSS is a partner. On the other hand, organizations in the private sector are liable to prefer not to be exposed to a unit in an organization with excessive tasks and powers that exceed this sole dimension.[102] In addition, by its very nature the GSS is an operational

organization that works clandestinely to foil attacks; it is not charged with other tasks necessary to confront the cyber challenge, such as maintaining close ties with the private sector, increasing the citizenry's awareness of information security, dealing with organizations that have been victims of cyber attacks, and so on.

The Government Authority for Information Security in the General Security Services is guided by the steering committee on computerized system security at the National Security Staff, led by the head of the Terrorism Warfare Staff there.[103] The role of the steering committee is to confirm the Information Security Authority's expansion of the list of guided or secured organizations that will be required to strengthen their security and come under the Authority's control. According to Gabi Siboni, this activity is not based on a statutory or systematic process of identifying these organizations. Thus, it turns out that large critical companies in certain sectors are included in the list while large companies in other sectors are not on the list (e.g., food and pharmaceuticals), despite their significant contribution to the national product, employment, and the fabric of life. Another shortcoming of this system lies in the fact that it focuses on guiding selected companies in certain sectors and assisting in pinpoint security. It does not provide systemic security, which would require broader coverage of institutions connected to the same critical system. An example is the water system:

> Protection of water supply and water quality infrastructures in Israel does not only affect processes in Mekorot, Israel's national water company, but also dozens of other water suppliers, associations, water corporations, desalination and delivery facilities, sewage and wastewater treatment facilities, and so forth. A large number of these facilities are operated by private entrepreneurs who do not see activating protective mechanisms as a top priority. The situation is similar in other industries.[104]

By contrast, an example that reflects a high awareness of information system security may be found among the leaders of the financial institutions in the Ministry of Finance and the Bank of Israel. The Ministry of Finance (the Capital Market, Insurance, and Savings Division) has published detailed directives for financial institutions on information security and protecting information systems.[105] The Inspector of Banks at the Bank of Israel also issued a comprehensive detailed circular that stresses: "Information technology is a central component in the proper operation and management

of a banking corporation, as information, in all its aspects and implications, has a decisive effect on the stability of the banking corporation and its development."[106] Such a directive may serve as an example for other government ministries regarding associated state institutions.

The IDF Cyber Staff: In 2009, IDF Chief of Staff Gabi Ashkenazi defined cyberspace as a strategic and operative domain of warfare. Accordingly, the IDF's Cyber Staff was established to serve as a General Staff group to coordinate and direct army activities in cyberspace. The Cyber Staff was established within Unit 8200 of Military Intelligence,[107] and has representatives from Intelligence and the Computerization Division.[108] Then-head of Intelligence Maj. Gen. Amos Yadlin referred to the subject in a lecture delivered at the Institute for National Security Studies in December 2009. He noted that Israel's vulnerability as a result of computer break-ins is a threat to national security and said, "The IDF intends to provide good security for networks and also engage in its own cyber attacks."[109] The IDF's Cyber Staff can be a partner in securing the nation's cyberspace, similar to CYBERCOM in the United States, though it too is not the body designed for fully integrating national cyberspace defense.

The National Cyber Staff: On May 18, 2011, Prime Minister Benjamin Netanyahu announced the establishment of the National Cyber Staff: "The primary function of the Staff is to expand the state's capabilities to secure critical infrastructure systems against cyber terrorism, carried out both by foreign nations and by terrorist groups."[110] The Staff was established on the basis of a recommendation by a team headed by the Chair of the National R&D Council, Maj. Gen. (ret.) Isaac Ben-Israel. Netanyahu announced that he had adopted the recommendations in full and explained: "In the defensive sense, Israel is exposed to cyber attacks that could paralyze life-supporting systems upon which the country depends, such as the electric grid, communications, credit cards, water, and transportation. Each of these areas is computerized and therefore vulnerable. It is necessary to formulate a defensive response to this threat." It was also reported that the new staff is expected to encourage Israeli companies specializing in cyber security in an attempt to carve out a slice of the extensive and developing global market in this niche.[111]

On August 7, 2011, the government of Israel approved the establishment of the National Cyber Staff.[112] According to the government decision,

> The Staff will lead the development of the field of cyberspace in Israel, coordinate the activities of the various organizations working in the field, expand the security of national infrastructures in the face of cyber attacks, and encourage the promotion of the subject in industry, turning the State of Israel into a global focus of knowledge, maintaining cooperation between the academic world, industry, defense systems, and other public institutions.

The decision also determined that the purpose of the Staff is to be "a staff group for the Prime Minister and government committees that will make recommendations about national policies and promote their implementation in the field of cyberspace subject to all government discussions and decisions." According to the government decision, the tasks of the Staff are:

a. To consult for the prime minister, the government, and its committees on cyberspace in relation to foreign affairs and security. Consulting for the government and its committees will occur through the National Security Staff.
b. To coordinate staff work of the government and its committees in the field of cyberspace, prepare their hearings, and follow up on the implementation of their decisions. In foreign affairs and security, coordinating the work of the staff, preparing discussions, and following up on the implementation of decisions will be effected by means of the National Security Staff.
c. To recommend national cyberspace policy to the prime minister and the government, consult with the relevant sources about policy decided by the government and/or prime minister, implement the policies, and oversee the implementation.
d. To issue as necessary to all relevant bodies complementary policy directives derived from government and government committee decisions in the field of cyberspace.
e. To determine and validate annually the national reference threat to secure cyberspace.
f. To promote cyberspace R&D.
g. To encourage Israel's cyberspace industry.
h. To formulate a national doctrine for confronting cyberspace emergencies.
i. To hold national and international exercises to improve Israel's cyber preparedness.
j. To assemble the intelligence picture of cyber security from all elements within the intelligence community.

k. To assemble the national situation assessment in terms of cyber security from all the elements working in the field.
l. To promote and raise the public's awareness of threats and ways to confront them in cyberspace.
m. To formulate and publicize warnings and information to the public about existing cyberspace threats, as well as rules of preventive conduct.
n. To promote national educational programs for smart use of cyberspace.
o. To promote cooperation between Israeli cyber security institutions and their counterparts abroad.
p. To promote coordination and cooperation between government, security, academics, industry, business, and other organizations with cyberspace relevance.
q. To promote cyber legislation and regulation.
r. To be the regulatory body with the final word among the various organizations dealing with cyber security.
s. To undertake any other task in the field of cyberspace to be determined by the prime minister, subject to law and government decisions.

Ramifications

In the rapidly developing field of cyberspace, there are both risks and opportunities for Israel. Similar to other developed nations, cyberspace exposes Israel to significant fundamental risks, including damage to critical infrastructures, the defense establishment, the economy, and so on. Unlike many countries, Israel faces enemies driven to cause it as much harm as possible, e.g., Iran, which is working also to attain offensive cyber capabilities.[113] Similarly, one could imagine terrorist organizations becoming active in cyber attacks against the State of Israel. At the same time, Israel is a global leader in information technology and the cyberspace field, and its advanced capabilities allow it to take full advantage of the opportunities inherent in cyberspace, both for civilian and military purposes.

As part of accelerating Israeli preparations, a national strategy for Israeli cyberspace security must be formulated, with implementation headed by the National Cyber Staff. Furthermore, cyber warfare should be incorporated into Israel's national security strategy.

It is recommended that Israel formulate a national strategy for securing cyberspace that would lead to achieving its strategic goals with minimal

resources and serve as an operational framework for all the institutions involved in securing cyberspace. The strategy would be approved by the National Security Cabinet and serve as a guideline both for joint operations of the various institutions and for the operations of each institution acting within its own sphere of responsibility. The strategy's objectives should be:

a. To maintain a secure cyberspace in Israel that will allow the country to fulfill its national goals in governance, security, the economy, society, foreign affairs, science, and more.
b. To strengthen Israel's cyberspace security and preserve freedom of action in it for the welfare of all of Israel's citizens.

The strategy is meant to promote the attainment of these objectives by the country's relevant institutions joining forces, according to the following principles of action:

a. Acknowledgment of cyberspace as a new national domain that must be secured in unique ways (unlike the traditional domains), with a comprehensive view and cooperation among all relevant institutions and individuals.
b. Risk management from a comprehensive point of view. This includes giving priority to defense systems and critical national infrastructures but also securing other components of Israel's economy and society, e.g., securing government databases (the population registry, land ownership registry, tax records, court records, the Knesset, National Insurance Institute, local government, and so on), securing universities and research institutes, securing companies affecting the economy (beyond the category of critical infrastructures, such as medicine, food, heavy industry, insurance, etc.), securing companies connected to critical infrastructures, and so on.
c. Construction of dynamic, integrative, and comprehensive defenses. This includes integration between passive and active defense systems (along the lines of the Cyberspace Security Strategy of the Pentagon), integration between securing critical targets and components of "domain security" (traffic entering the country, communication hubs), improvement of network architecture, closer cooperation between physical and cyber security mechanisms, and more.
d. Joining of forces in the public (government) sector, between the security and the private sectors; cooperation and joint efforts among the units

within each of the sectors, e.g., integrating efforts and sharing knowledge between the army and other security organizations.

e. Close cooperation between the government (security and civilian) and the private sector in securing cyberspace. This includes sharing knowledge and capabilities so that every government and private organization will be aware of the risks, attacks, and new defensive capabilities.
f. Close cooperation with external bodies, e.g., constructing collective monitoring systems with allies.
g. Legislation and enforcement to allow the maintenance of a secure cyberspace.
h. Assistance to the public at large in cyberspace security, e.g., leading PR campaigns to raise the public's awareness of threats and solutions, giving incentives to businesses and citizens acquiring security software, increasing oversight of providers of security services and communications to the public in terms of cyberspace security.
i. Construction of capabilities of rapid recovery from attacks.
j. R&D, development, and acquisition of the most advanced technological capabilities and methods of action.
k. Formulation of a policy of deterrence, foiling attacks, and response as complementary components of the strategy, including: direct response capabilities against offensive cyberspace systems and capabilities of damaging attackers. This is within the purview of the defense establishment.

The addition of a new domain of warfare to the traditional domains obligates Israel to incorporate cyberspace into its security strategy or at least into its defense doctrine.[114] There are interrelations between the domains: physically, cyberspace exists in each of the other domains, connects them, and enhances capabilities of operating in them, while activities in the traditional domains are also manifested in cyberspace. Therefore, incorporating cyberspace presents a challenge of integration, and intelligent use of cyberspace capabilities may be a force multiplier in every form of battle.

Implementing concepts that underlie the traditional defense doctrine (such as deterrence, early warning, decision, and defense) in cyberwar differs in essence from implementing them in the traditional domains. As discussed above, it is very difficult to implement deterrence in cyberspace

because of the difficulty in determining the identity of attackers; in many cases operative early warning may be applicable only for active defense mechanisms responding to attack with superhuman speed (there is no time to apply human considerations); cyberspace defense is supposed to rely on the unique features of cyberspace and therefore requires unprecedented cooperation between the defense establishment and the public sector. In addition, in light of the acknowledgment of cyberspace as a domain of warfare, it is necessary to examine new strategic capabilities and perhaps even generate a change in ORBAT, i.e., invest more in establishing a cyber army.

Israel has the potential to be one of the leading nations in the world in the field of cyber security, considering the remarkable human capital and technological knowledge it already has. Taking advantage of this potential largely depends on government policy formulation and implementation.

Notes

1 ITU Toolkit for Cybercrime Legislation, p. 12, www.itu.int/cybersecurity.
2 The United States Army's *Cyberspace Operations Concept Capability Plan 2016-2028*, 22 February 2010, p. 6.
3 Cabinet Office, "Cyber Security Strategy of the United Kingdom" (Safety, Security and Resilience in Cyber Space), June 2009, p. 7.
4 Federal Ministry of the Interior, "The New Cyber Security Strategy for Germany," Berlin, February 2011, p. 14.
5 Sebastian M. Convertino II, Lou Anne DeMattei, Tammy M. Knierim, *Flying and Fighting in Cyberspace* (Alabama: Air University Press, July 2007).
6 Amos Granit, *Cyberspace as a Military Domain – In What Sense?* Institute for Intelligence Studies at IDF Military Intelligence, March 2010.
7 "RSA Computerization Infrastructures Breached; Risk to Customer Information Security," *The Marker*, March 19, 2011.
8 For example, Martin Libicki, a senior management scientist at RAND Corporation, claimed at the February 2011 Herzliya Conference that it is possible to deal relatively easily with cyberspace attacks, in part by using rapid fixing and resetting. In his assessment, the weakness of cyber attacks stems from the inability to generate constant effects.
9 U.S. Department of Defense, Office of the Assistant Secretary of Defense, "Remarks on Cyber at the RSA Conference," as delivered by William J. Lynn, III, San Francisco, California, February 15, 2011 [hereafter: Lynn, February 15, 2011]. See http://www.defense.gov/speeches/speech.aspx?speechid=1535.
10 The strategic environment is the security and political environment affecting a nation's ability to realize its national goals and includes the players operating in it, the tools they have, and the rules of the game.
11 Richard Clarke, a security expert, defines cyberwar as follows: "Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." See Richard Clarke, *Cyber War* (New York: Harper-Collins, 2010), p. 6.
12 John Markoff, "A Code for Chaos," *New York Times*, October 2, 2010, based on Thomas C. Reed, a former secretary of the Air Force, in his book *At the Abyss: An Insider's History of the Cold War* (New York: Ballantine Books, 2004).
13 Lynn, February 15, 2011.
14 Siobhan Gorman, August Cole, and Yochi Dreazen, "Computer Spies Breach

Fighter-Jet Project," *Wall Street Journal*, April 21, 2009.

15 Lynn, February 15, 2011.

16 Yitzhak Ben-Horin, "War on the Web: Fictitious Bloggers Serving the US," *Ynet*, March 18, 2011.

17 Anshel Pfeffer, "Weapon against Oppression: Plane for Internet Connection," *Haaretz*, February 9, 2011.

18 The editors of the website *People and Computers*: "Former CIA and NSA head: Unless we're careful, cyberattacks will become the atomic bomb of the 21st century," www.pc.co.il, August 2, 2010; William Jackson, "U.S. understanding of cyber war still immature, says former NSA director," *Government Computer News* (*GCN*), http://gcn.com, July 29, 2010.

19 This distinction – between intrusion for the sake of intelligence gathering and intrusion for the sake of attack – was presented in Lieutenant General Keith Alexander's testimony before Congress on April 15, 2010. See "Advance Questions for Lieutenant General Keith Alexander," USA Nominee for Commander, United States Cyber Command, U.S. Senate, Committee on Armed Services, Washington, DC, April 15, 2010 [hereafter: Alexander, April 15, 2010].

20 Lynn, February 15, 2011.

21 William J. Lynn, "The Pentagon Cyber Strategy," *Foreign Relations*, August 2010 [hereafter: Lynn, August 2010].

22 Lynn, February 15, 2011.

23 See note 18.

24 Lynn, August 2010.

25 Thomas Rid and Peter McBurney, "Cyber-Weapons," *RUSI Journal* 157, no. 1 (February 6-13, 2012).

26 Alexander, April 15, 2010.

27 E.g., the warning issued by Secretary of State Hillary Clinton on January 21, 2010, directed primarily at China: "States, terrorists, and those who would act as their proxies must know that the United States will protect our networks. Those who disrupt the free flow of information in our society or any other pose a threat to our economy, our government, and our civil society. Countries or individuals that engage in cyber attacks should face consequences and international condemnation. In an internet-connected world, an attack on one nation's networks can be an attack on all." (Hillary Rodham Clinton, "Remarks on Internet Freedom," Washington, DC, January 21, 2010).

28 According to Lynn (February 15, 2011), certain types of poisonous worms are liable to wriggle loose from their creator, spread throughout the world in a matter of minutes, and among other results, cause the disruption of critical networks. Therefore, the Pentagon's defense strategy in cyberspace assumes the worst possible scenario.

29 Alexander, April 15, 2010.

30 *Cyberspace Operations Concept Capability Plan 2016-2028*.

31 Ibid.

32 Markoff, "A Code for Chaos"; "Cyberwar: War in the Fifth Domain," *The Economist*, July 1, 2010.

33 Yaniv Leviatan, "This is how we Fought with Computers, about Computers, and through Computers in the Last Decade," *Maariv Online*, December 31, 2009.
34 "The NATO Cyber War Agreement," *Strategy Page* (www.strategypage.com), May 1, 2010.
35 U.S. Cyber Consequences Unit, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008," 2009, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.
36 Yaakov Lappin, "Anti-Israel Hackers Strike El Al, TASE Websites," *Jerusalem Post*, January 16, 2012, http://www.jpost.com/NationalNews/Article.aspx?id=253809.
37 *Reuters*, January 7, 2012.
38 Yaakov Lappin, "Israeli Hacker Team Brings Down Iranian Websites," *Jerusalem Post*, January 26, 2012, http://www.jpost.com/MiddleEast/Article.aspx?id=255300.
39 Tobias Buck, "Hackers Attack Arab Stock Markets," *Financial Times*, January 17, 2012, http://www.ft.com/intl/cms/s/0/7981c42a-4142-11e1-936b-00144feab49a.html#axzz1orjfkdIa.
40 AFP, "Anti-Israeli Hackers Target Azerbaijani Sites," *Ynet*, January 16, 2012, http://www.ynetnews.com/articles/0,7340,L-4176458,00.html.
41 "Bank Hapoalim Hit by Iranian Cyber Attack," *Haaretz*, February 19, 2012, http://www.haaretz.com/print-edition/business/business-in-brief-1.413388.
42 Matan Mittelman, "Another Step in Exposing the Mystery Surrounding Stuxnet," *The Marker*, November 16, 2010.
43 "Ahmadinejad Admits: Virus Damages Nuclear Computers," *Walla,* November 29, 2010.
44 Yossi Hatoni, "The War for the Atom," *People and Computers* website, September 26, 2010.
45 "Iran Accuses: Israel and the United States Created the Stuxnet Computer Worm," *Haaretz Online*, April 16, 2011.
46 See, e.g., William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011; John Markoff, "Malware Aimed at Iran Hit Five Sites, Report Says," *New York Times*, February 11, 2011.
47 Trent Nouveau, "Iran: Cyber Attack Downed US Drone," *TG Daily*, December 8, 2011, http://www.tgdaily.com/security-features/60102-iran-cyber-attack-downed-us-drone.
48 "Cyberwar: War in the Fifth Domain."
49 "*The New York Times*: Findings of Crash of 1,000 Points on the Dow Jones – Fault of an Algorithm and One Sell Order," *The Marker*, October 1, 2010.
50 See note 11.
51 Martin Libicki, Herzliya Conference, February 2011.
52 Lynn, February 15, 2011.
53 "Cyberwar: War in the Fifth Domain."
54 Lynn, February 15, 2011.

55 Aki Peritz, "Fears Aside, al-Qaeda Ill-Equipped for a Major Cyberattack," http://articles.philly.com, March 20, 2011.
56 "Cyberwar: War in the Fifth Domain."
57 "UN Calls for Global Cyber Treaty," www.cpccci.com/blog, February 2, 2010.
58 Ellen Nakashima, "15 Nations Agree to Start Working Together to Reduce Cyberwarfare Threat," *Washington Post*, July 17, 2010.
59 John Markoff and Andrew E. Kramer, *New York Times*, June 28, 2009.
60 "US vs. Russia Cyberspace Dispute," *New New Internet Cyber Frontier* (www.thenewnewinternet.com), June 29, 2009.
61 The White House, *The National Strategy to Secure Cyberspace*, February 2003.
62 "President on Cybercrime: It has Happened to Me," *THE OVAL*, May 29, 2009; "President Obama: Focus on Cybercrime," *Ecommerce Journal*, June 9, 2009.
63 The White House, *US National Security Strategy*, May 2010.
64 Lynn, February 15, 2011.
65 Spence Ackerman, "Darpa Begs Hackers: Secure our Networks," November 7, 2011, http://www.wired.com/dangerroom/2011/11/darpa-hackers-cybersecurity.
66 Home Land Security Office website; National Cyber Security Division, March 2011.
67 Department of Defense Strategy for Operating In Cyberspace, July 2011.
68 *The National Intelligence Strategy of the USA*, DNI Office, August 2009.
69 *The National Strategy to Secure Cyberspace,* The White House, February 2003.
70 *International Strategy for Cyberspace,* The White House, May 2011. See http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
71 See note 62.
72 Lynn, August 2010.
73 Allied Command Operations (ACO), "NATO's 'Cyber Coalition' Exercise a Collaboration in Cyber Defence," www.aco.nato.int, November 18, 2010.
74 *Spacewar*, "US: NATO Networks Vulnerable to Cyber Threat," www.spacewar.com, January 25, 2011.
75 "DOD Report Cyber Attacks Could Elicit Military Response," November 16, 2011, http://www.infosecisland.com/blogview/18218-DoD-Report-Cyber-Attacks-Could-Elicit-Military-Response.html.
76 See http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540rh/pdf/BILLS-112hr1540rh.pdf.
77 Alexander, April 15, 2010.
78 Lynn, February 15, 2011. This is also the source for the Lynn statements that appear in the following two paragraphs.
79 "The White House Completes Preparation of Report on Information Security in the American Administration," *People and Computers* website, April 19, 2009.
80 Yossi Hatoni, "The United States: The Pentagon to Establish Headquarters for Online Warfare against Terrorism and Crime," *People and Computers* website, June 24, 2009.
81 See note 11.
82 "White House Consider Cyberwar with Libya," *Russian News from Russia*,

October 18, 2011, http://news.windowstorussia.com/white-house-considered-cyberwar-with-libya.html.

83 Ibid.

84 "The French Strategy for Information System Security," the website of the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). The document uses the term "information systems" instead of "cyberspace."

85 Federal Ministry of the Interior, "The New Cyber Security Strategy for Germany," Berlin, February 2011.

86 Cabinet Office, *Cyber Security Strategy of the United Kingdom (safety, security and resilience in cyber space)*, June 2009.

87 The Government of Australia website, http://www.ag.gov.au/cybersecurity.

88 Government of Australia, "Australia Outlines New Cyber Security Strategy," *TheGovMonitor*, February 6, 2011, http://www.thegovmonitor.com/civil_society_and_democratic_renewal/governance/australia-outlines-new-cyber-security-strategy-45925.html.

89 John Blackburn and Gary Waters, "Optimising Australia's Response to the Cyber Challenge," The Kokoda Foundation, Paper No. 14, February 2011.

90 The Australian Department of the Prime Minister and Cabinet, "A Public Discussion Paper: Connecting with Confidence - Optimising Australia's Digital Future," http://cyberwhitepaper.dpmc.gov.au/white-paper.

91 Australian Policy Online, "Cyber White Paper: Inquiry on Now," forthcoming, mid 2012, http://apo.org.au/notice/cyber-white-paper-inquiry-now-paper-due-mid-2012.

92 Joel Harding, "China's Cyber Strategy – Too Much or Too Little?" *Infosec Island*, January 10, 2012.

93 *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman Corporation, Information Systems Sector, October 9, 2009.

94 "Chasing The Night Dragon," *Strategy Pa*ge website, March 8, 2011.

95 Sharon LaFraniere and David Barboza, "China Tightens Censorship of Electronic Communications," *New York Times*, March 21, 2011.

96 See Cyber Crime Law, http://www.cybercrimelaw.net/Cybercrimelaw.html.

97 Noa Peleg, "Growing Big, Reaping Small," *Globes*, March 9, 2011.

98 See an interview by Steve Forbes of *Forbes Magazine*, with George Gilder, a well known American expert on IT and the economy, February 16, 2011: "*Forbes*: Now, you've made the point, as a handful of others have, that knowledge is about the past, entrepreneurship is about the future. Even looking at the world today in terms of foreign policy: You say 'Middle East' – people think oil. You've made the point that Israel, with its brains and what it's doing in high technology, is really a functional part of the U.S. economy, which is where the real value is. Gilder: Well, it's just wonderful that Israel has become a new Silicon Valley just as our own Silicon Valley gets paled over by green goo. Israel is moving to the forefront in developing new technologies that are based on fundamental advances. And these technologies instantly propagate to the United States. So, Israel is a substitute for a somewhat temporarily declining

Silicon Valley. *Forbes*: So it's sort of like a baseball team. It's our farm system. Gilder: Yeah, it's our farm system. And it's just been great. Israel is the key asset in the Middle East. This idea that oil, a fungible element that can be sold anywhere, is comparable to the genius of the Jewish people in Israel is just an absurdity. Israel is where it's at in the Middle East. And the leading edge of the U.S. economy today is in Israel, surprisingly enough. I was surprised to discover it, but in the last five years I've been increasingly turning to Israel for my new companies." See http://www.forbes.com/2011/02/11/gilder-nanotechnology-fiber-optics-intelligent-investing-video.html.

99 TEHILA website, www.tehila.gov.il.

100 Israel Government Information Security website, www.cert.gov.il.

101 General Security Service (Shabak) website, www.shabak.gov.il.

102 Brig. Gen. Nitzan Nuriel, head of the Terrorism Warfare Staff (who also serves as the chair of the Steering Committee on Computerized System Security at the National Security Staff), has said that different Israeli institutions, including large private companies, refused government protection until the Terrorism Warfare Staff broke into their systems in order to prove to them the potential for damage. See Barak Ravid, "Prime Minister Binyamin Netanyahu Establishes Staff to Prepare Israel for Attack on Computer Systems," *Haaretz*, April 3, 2011.

103 The cyberspace security tasks with which the head of the Terrorism Warfare Staff at the National Security Staff was charged will presumably be transferred to the head of the National Cyber Staff.

104 Gabi Siboni, "Protecting Critical Assets and Infrastructures from Cyber Attacks," *Military and Strategic Affairs* 3, no. 1 (2011): 96, at http://www.inss.org.il/upload/(FILE)1308129638.pdf.

105 *A Circular for Institutional Organizations*, 6-9-2006, October 16, 2006.

106 *Proper Banking Management* [4] (09/03): Information Technology Management.

107 Amir Oren, "IDF's New Fighting Arena – in Computer Networks," *Haaretz*, January 2, 2010.

108 The IDF Computerization Division was established in March 2003 on the basis of a merger between the Communications Force and the Computerization Brigade (Communications and Computers), marking the establishment of a General Staff body charged with defining computer policy in the IDF (website of the Computerization Division).

109 Nehama Almog, "Maj.-Gen. Amos Yadlin, Head of AMAN: Israel Leads the Field of Cyberwar," *People and Computers* website, December 17, 2009.

110 "Prime Minister Announces Establishment of National Cyber Staff," Prime Minister's website, May 18, 2011.

111 Jonathan Liss, "Prime Minister Binyamin Netanyahu Announces the Establishment of National Cyber Staff," *Haaretz*, May 18, 2011.

112 Government Decision No. 3611 of August 7, 2011; website of the Prime Minister.

113 Amy Kellogg, "Iran is Recruiting Hacker Warriors for its Cyber Army to Fight 'Enemies,'" *FoxNews.com*, March 14, 2011.

114 The defense doctrine is a condensed model that includes deterrence, early warning, decision, and defense (according to the April 2006 Meridor Commission

proposal). The doctrine embodies the interrelations between these concepts in the context of operating the IDF and embodies important strategic components, including aerial superiority and intelligence superiority. At the same time, the defense doctrine does not include other components of Israel's security, such as reliance on a superpower (e.g., the United States), various defense arrangements (demilitarization, thinning of forces, or use of international forces) as part of various political arrangements, and so on. While Israel's defense doctrine is not written down, it is nevertheless made clear by Israel's actions.

INSS Memoranda 2010 – Present

No. 117, May 2012, Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts and Strategic Trends*.

No. 116, April 2012, Yoel Guzansky, *The Gulf States in a Changing Strategic Environment* [Hebrew].

No. 115, March 2012, Emily B. Landau, *Decade of Diplomacy: Negotiations with Iran and North Korea and the Future of Nuclear Nonproliferation*.

No. 114, March 2012, Yoel Guzansky and Mark A. Heller, eds., *One Year of the Arab Spring: Global and Regional Implications* [Hebrew].

No. 113, March 2012, Yoel Guzansky and Mark A. Heller, eds., *One Year of the Arab Spring: Global and Regional Implications*.

No. 112, Uzi Rabi and Yoel Guzansky, eds., *The Gulf States: Between Iran and the West* [Hebrew].

No. 111, December 2011, Benedetta Berti, *The Ongoing Battle for Beirut: Old Dynamics and New Trends*.

No. 110, November 2011, Meir Elran, Owen Alterman, and Johannah Cornblatt, eds., *The Making of National Security Policy: Security Challenges of the 21st Century – Conference Proceedings*.

No. 109, June 2011, Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts, Trends, and Implications for Israel* [Hebrew].

No. 108, May 2011, Emily B. Landau and Tamar Malz-Ginzburg, eds., *The Obama Vision and Nuclear Disarmament* [Hebrew].

No. 107, March 2011, Emily B. Landau and Tamar Malz-Ginzburg, eds., *The Obama Vision and Nuclear Disarmament*.

No. 106, November 2010, Yehuda Ben Meir and Olena Bagno-Moldavsky, *Vox Populi: Trends in Israeli Public Opinion on National Security 2004-2009*.

No. 105, August 2010, Meir Elran and Yoel Guzansky, eds. *Vision and Reality in the Middle East: Security Challenges of the 21st Century – Conference Proceedings*.

No. 104, June 2010, Gallia Lindenstrauss, *Mediation and Engagement: A New Paradigm for Turkish Foreign Policy and its Implications for Israel* [Hebrew].

No. 103, May 2010, Tamar Malz-Ginzburg and Moty Cristal, eds., *A Nuclear Iran: Confronting the Challenge on the International Arena* [Hebrew].