Basic Concepts in Cyber Warfare

Lior Tabansky

Introduction

Developments in computers have made possible far reaching changes in all areas of life, and the rapid progress in computing, communications, and software has led to a dramatic reduction in the cost of producing, processing, and disseminating information.[1] The scientific-technological developments of recent decades gave rise to "the information revolution," which involves the processing and dissemination of information. Information technologies continue to develop at an accelerated pace, and a new era has arisen in the information revolution.

The rapid growth in the fields of computing and communications and the ongoing improvement in the performance of computerized systems have created a new space in the world.[2] Cyberspace, a space created not in nature but by human beings, has the potential for tremendous benefits as well as unknown risks. Since it has existed for forty years at most, an understanding of the phenomenon is just beginning. The interface between a new topic that enables unprecedented capabilities, a technical field that demands professional understanding, and mass media that compete for the consumer creates – perhaps predictably – the potential for obfuscation.

National security has also been affected by the information revolution and the cyberspace phenomenon. In the national security context, the far reaching changes in information technology that have brought about a quantum leap in the availability and quality of intelligence, in the pace of information transfer, and in weapons precision[3] spawned the notion of a "Revolution in Military Affairs" in the 1990s. Smart use of new

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

technologies allows previously unknown capabilities, which together with new methods have generated a qualitative change in the military field. However, a public discussion on the issue of cyber security, as of other new hi-tech fields, is lacking in Israel.

This essay focuses on the question of national security in light of the cyberspace phenomenon. It aims to survey the field and create a common language for a fruitful public discussion of the developing issue of cyber security, proposing operative definitions for the issues that can be applied in a discussion of Israel's national security. The essay first addresses the properties of cyberspace, its inherent vulnerabilities, and possible threats within its realm, and then proceeds to related issues of defense, attack, and deterrence in cyberspace.

Cyberspace: Fundamentals and Properties

The term "cyberspace" − cyber(netics) + space − appeared for the first time in science fiction.[4] The word comes from the Greek *kybernetes*, which means one who steers or governs,[5] and its modern form appeared in a 1948 book by mathematician Norbert Wiener to describe the study of command and control and communications in the animal world or the mechanical world.[6] "Space" has many meanings in English, referring to philosophical, physical, mathematical, geographical, social, psychological, and other properties. One definition of space is "a boundless, three-dimensional extent in which objects and events occur and have relative position and direction."[7] This simple definition is sufficient for most of the daily experience of human beings, but it is not sufficient for the computerized world, which is inherently different from physical space.

Thus, use of the word "space" without precise delimitation is apt to lead to conceptual difficulties, as indeed occurs with "cyberspace." Moreover, the simple joining of two words does not provide an adequate understanding of the concept. Rather, the concept must be defined by addressing the intended use, in this case, with an understanding of the processes taking place in the computerized world and their interaction with issues of national security. In contrast to land, sea, air, space, or electromagnetic spectrum, cyberspace is not part of nature and would not exist without the information technologies that were developed in past decades; cyberspace is much less concrete than natural spaces, and therefore this conceptual discussion is essential.

Cyberspace is composed of all the computerized networks in the world, as well as all end points that are connected to the networks and are controlled through commands that pass through these networks. By the end of the first decade of the twenty-first century, the public commercial internet became an integral part of daily lives.[8] In the first quarter of 2010, 2 billion people in the world were connected to the web, and the rate of internet penetration in developed countries is about 80 percent.[9] Access to the internet has moved quickly from stationary end points and fixed physical infrastructures to mobile devices and wireless infrastructure. The price for use continues to drop, and the web's dimensions and complexity are growing. A discussion of cyberspace developments tends to focus on the commercial internet.

However, the public internet is only part of cyberspace. That is, cyberspace includes the internet, but it also includes a range of other computer networks that are not accessible through the internet. Many networks have been designed and built in order to carry out defined tasks.[10] Some of the specific networks are built from the same building blocks as the public internet, but are separate from it, while others use completely different techniques from the internet. Cyberspace was formed by connecting computerized networks that communicate among themselves

Cyberspace can be described as composed of three layers.[11] The most concrete layer, the infrastructure of the cyber world, is the physical layer. Electrical energy, integrated circuits, processors, storage devices, communications infrastructures, copper cables, optical fibers, transmitters and receivers comprise the building blocks of this space.[12] These building blocks have natural properties of width, height, depth, mass, and volume. The second layer is software logic: a variety of systems of instructions for action and reaction that were programmed by human beings. The physical components are controlled largely by the various computer programs, and the stored information in computers is subjected to processing through software instructions. Most of cyberspace today uses standard hardware and software. The third layer of cyberspace is the layer of data that the machine contains and that creates information.

This is the least concrete layer of the three, mainly because information properties are very different from the properties of physical objects.

Much of cyberspace is organized and managed by private and cooperative organizations without state or geographical overlap. The internet, which is a central and growing component in this space, is built in a decentralized manner. The ideology of the internet's creators and its leading thinkers is opposed to any type of state management.[13] Moreover, the continuing development of information technologies enables new applications that take advantage of the internet's open infrastructure. Thus, for example, it is possible to transfer non-text content (picture, voice, and video) over the internet's infrastructure, and wireless communications and the reduction in the price of processing power allow internet connectivity for many devices that were not computerized such as industrial machines and technological accessories.

Given these structural and organizational properties, cyberspace has a high level of complexity and it is subject to frequent changes. Significantly, these properties accumulated empirically; the organizational properties in particular reflect the existing situation, but it does not necessarily follow that a priori these properties are an essential, inherent part of cyberspace.[14] Therefore, these properties will not appear in the definition of the field. However, the goal of this essay is to contribute to the public discussion of Israel's national security issues in cyberspace, and the working definition must faithfully reflect the existing situation in order to be applicable.

On this basis, what follows is an operative working definition of "cyberspace": inter-connected networks of information technology infrastructures, including the internet, telecommunication networks, mission-specific networks, computers, and computer embedded systems. The virtual environment – data stored and information processed by computers and transferred over these networks – is also included.[15]

Cyberspace and National Security

Security is one of the fundamental needs of human beings, societies, and states, and a significant portion of human endeavors in all natural spaces (land, sea, air, space, electromagnetic spectrum) stems from security issues. Yet historical experience, together with philosophy, has shown that scientific development has not changed human nature enough to eradicate conflicts between human beings and among societies.[16] Thus cyberspace, which is man made, will also be exploited by human beings for their purposes; in this space too, there will be fights and conflicts. However, the nature of cyberspace is such that fundamental familiar security-related concepts such as violence, identity, location, defense, attack, and speed do not necessarily describe events correctly. Rather, the properties particular to cyberspace require specific professional treatment of security as it pertains to the cyber realm.

The United States began to address cyberspace in the context of national security as early as 1996.[17] American attention to the issue of security in cyberspace has been increasing, and as expressed by President Obama, "It's now clear that this cyber threat is one of the most serious economic and national security challenges we face as a nation. It's also clear that we're not as prepared as we should be, as a government or as a country."[18]

The American investment in this area is not limited to the declaratory level, but is backed up by significant financial and organizational resources. Government agencies, the military, industry, and academic institutions lead the work in this field, and publish numerous research and position papers. A full discussion of the American approach to the issue is beyond the scope of this article; suffice it here to mention that this issue attracts a great deal of interest among a wide range of circles. Similarly, although cyberspace is a young field, its potential for impact has not escaped the notice of those involved in national security all over the world, even if practices and details are shrouded in obscurity and a veil of secrecy in most countries.

What follows is an explanation of some of the basic concepts in the field of cyber security, to allow a common language when discussing cyberspace and Israeli national security.

Weaponry

Cyberspace is dependent on physical infrastructures, which include computers, sources of electricity, communications cables, antennae, and satellites. It is clear that kinetic damage to the physical infrastructure will harm cyber capabilities, but there is a difference between traditional kinetic weapons, even if they are aimed at a cyber target, and the new phenomenon of cyber weapons.

Cyber weapons are composed mainly of software, though at times hardware as well. They can be divided into three groups:

a. Unequivocally offensive weapons: different types of malware (viruses, worms, Trojan horses, logic bombs, and the like); denial of service actions.

b. Dual use tools: network monitoring; vulnerability scanning; penetration testing; encryption; and camouflage of content and communications.

c. Unequivocally defensive tools: firewall, disaster recovery systems.

Vulnerabilities

Vulnerability refers to weak points that are built-in properties of a defined system. In risk analysis, vulnerability is part of the risk equation: risk is a product of vulnerability, threat, and probability. Table 1 charts the weak points in cyberspace in light of the properties reviewed above.

Table 1. Cyberspace Properties and Vulnerabilities

Property	Vulnerability
Rapid pace of change	Rapid obsolescence of means, including defensive systems.
Rapid reduction in price	Low entry threshold leads to a multiplicity of significant players.
Structure of TCP/IP protocol	Difficulty identifying the source of the signal that arrives via the network.
Wide scale use of standard, commercial off the shelf equipment	Narrowing of the gaps in capabilities among various players; vulnerability of hardware and identical operating systems endanger a wide range of systems.
High level of complexity	It is difficult to differentiate between a glitch and an attack. It is very difficult to determine cause and effect.
Asymmetry	No great investment is needed to develop and operate the weapons. Defense against cyber threats must include all channels of attack and be updated frequently, at progressively high costs.
Vague laws	There is no common definition of “cyber warfare” in the world; significant legal differences between various countries concerning cyber crime.

Defense

Defense from a cyber threat is derived from its broad common denominator, which is unauthorized access to a computer system. Therefore, defense is focused on using technological methods to identify an unauthorized intrusion, locate the source of the problem, assess the damage, prevent the spread of the damage within the network, and to the extent necessary, reconstruct the data and the computers that were damaged. Defense involves the ability to be positioned in the path of penetration, identify such an attempt, and foil it through preemption. For this purpose, computer systems are used to monitor activities and communications; block access routes; limit permissions; verify identity; provide encryption, and enable backup and disaster recovery.

While this appears to be a proper logical response to the threat, cyber-defense is necessarily limited. The volume of activity alone places the defending party in an inferior position. The decentralization of computer resources and networks complicates the attempt to define the areas of responsibility. The situation in compartmentalized networks is simpler: the compartmentalized body knows that the network is under its control and that it must maintain and defend it. (This is one of the reasons that this article does not address the subject of military networks and electronic warfare.) However, networks of this type are diminishing, and an increasing number of industrial systems exploit the advantages of IT and thereby become prone to risks of cyberspace. Critical infrastructures have been brought into cyberspace, and the security forces use commercial infrastructures for most of their communications, so that the burden of passive defense is growing.

Attack

A cyber attack does not include kinetic damage to cyberspace's physical infrastructure. An attack in cyberspace uses cyber tools, and its weapons are software and hardware. Again, the very identification of an attack is not simple. The symptoms of glitches and the possible results of an unauthorized intrusion into computer resources are often identical. Even identifying an intrusion and ruling out the possibility of a technical glitch is not sufficient. Such an intrusion is used for the entire spectrum of cyber threats, and when an unauthorized approach to a computer resource occurs, it can be used for all kinds of activities, and it is very difficult to determine the identity of the intruder and his motives. The properties of cyberspace today lend a clear advantage to attack over defense.[19]

Cyber War

Wars have been a part of human experience since the dawn of history. Cumulative experience of destruction has brought about a series of understandings intended to reduce the horrors of war: establishment of international institutions; creation of various international treaties that govern the boundaries of what is permitted in war; the establishment of humanitarian aid organizations; and a judicial system against war criminals. Because of the newness of cyberspace and its lack of correspondence to the fundamental concepts of the physical world, no definition of the concept of cyber war has been formulated. In Israel, discussions on the issue of war in the information age, computer warfare, and information warfare have been underway for at least a decade.[20]

Hostile activity in cyberspace can be ranked according to types of activity undertaken and damage caused. What follows is a proposed classification, arranged in descending order of severity.

a. An attack on various civilian targets that causes physical damage.
b. Disruption of and attack on critical national information infrastructures, which causes physical damage.
c. Disruption of and attack on military targets in the state’s sovereign territory.
d. Disruption of and attack on military targets outside the state’s sovereign territory.
e. Insertion of dormant attack tools, e.g., a Trojan horse or logic bomb that are likely to be preparations for an attack.
f. Criminal activity, industrial espionage.
g. Use of dual use weapons: intelligence gathering, probing for common security vulnerabilities, penetration tests.
h. Conducting a propaganda media campaign, abuse and defacement of official websites.

The difficulty in discussing cyber war derives from the non-trivial nature of the concepts of attack, defense, and violence in cyberspace. In order to determine that a cyber attack is part of a war, several properties must be examined:

a. Organizational source and geographic origin: is a nation state behind the action?[21]
b. Results: could the attack have caused damage, and did it in fact cause damage and casualties?
c. Level of complexity: did the attack require complex planning and coordinated resources that are available mainly to states?

In light of the properties of cyberspace today, it is very difficult to answer these questions, let alone answer them in a manner sufficient for designing public policy.

Deterrence

Advanced research on the subject of deterrence occupies researchers in political science, security studies, game theory, economics, and psychology. Thus far, the world has succeeded in coping with nuclear weapons that are capable of destroying the earth through deterrence based on assured retaliation.

However, the Cold War model of nuclear deterrence is utterly impracticable in the cyber battlefield, especially given the structure of cyberspace today, which makes it impossible to identify an attack with certainty and makes it impossible to pinpoint quickly the source and identity of the attacker.[22] Deterrence based on exacting a heavy price from the attacker is practically impossible; thus any deterrence in cyberspace today must be based on preventing the attacker from scoring an achievement. It is essential to invest in focused research on the subject of deterrence in order to reduce the threats to national security.[23]

Cyber Threats

Many actors with threat potential operate in cyberspace, including:

a. Hacktivists: individuals attacking websites in order to implant a political message, or acting to break censorship mechanisms and expose secrets.
b. Hackers: individuals who break into a computer system remotely through a communications network.
c. Writers of malware; spammers; collectors of personal user data.
d. Botnet herders: individuals who break into computers remotely through a communications network, but obtain partial control over many other computers in order to turn them, without their

knowledge, into a means of carrying out a future task. In recent years, there has been a fertile market in capabilities to attack networks, numbering tens of thousands to millions of computers.

e. Organized crime organizations use hackers, mainly botnet herders, for purposes of profit: identity theft, fraud, spam, pornography, camouflaging of criminal activity, money laundering, and so on.

f. Employees belonging to inner circles of a closed organization: an insider threat. Computer networks of compartmentalized organizations are separated from the general network in order to make break-ins difficult. In such a situation, recruiting an embittered employee is a good way to infiltrate a compartmentalized network. A hacker who confronts technical obstacles may exploit innocent workers in the target organization through social engineering.

g. The security services adopt cyberspace tools to achieve their goal; information technologies provide spies a wide range of ways and means to carry out their tasks.

h. Terrorists and radicals also take advantage of cyberspace to convey encrypted messages, recruit supporters, acquire targets, gather intelligence, camouflage activity, and so on.

There is no technical measurement to assess how critical a computer system is that it can exist on a national level isolated from the social values, goals, and forces that use it. Therefore, the relative importance of a computer system, and as a result, the amount of public investment required to defend it, are subject to a public discussion and a political fight. Critical infrastructures (manufacture and supply of energy and food, land and air transportation, water and sewage, communications systems, and the like) existed in developed societies before the appearance of the computer. Why do they receive attention in the discussion of the new phenomenon of cyberspace? After all, these infrastructures were essential to states even before computers appeared, and were mainly used for strategic goals in international conflicts. The current attention is a function of two factors.

First, when computers and communications penetrated into every aspect of life, cyberspace itself became essential to the full functioning of developed states. Cyberspace is like the body’s nervous system. Therefore, it has become essential to secure normal, undisturbed action in cyberspace, and to provide all strata of the populace with the ability to access it.[24]

Second, with the development of computing, computers were integrated into the existing production, command, and control systems of the traditional industries. The cyber layer, with its high level of complexity, was added to the already complex engineering systems. In fact, the old infrastructures were placed in cyberspace,[25] thereby making them vulnerable to the weaknesses of cyberspace. For the first time, potential arose to reach protected targets through the dimension of communications and software that does not depend on defense in physical space. Once essential infrastructures function at least in part in cyberspace, potential exists to directly harm essential state targets by exploiting their cyberspace vulnerabilities. The major threat is damage to the physical functioning of the essential infrastructures through cyber means, while bypassing the traditional military defense systems that guard the physical space, conceal the attacker's identity, and ultimately avoid a response and armed conflict.

A threat is made possible by exploitation of a vulnerability, and it is intended to disrupt a system or to harm the enemy's assets. There are threats to cyberspace (risks *to* cyberspace), which are intended to harm the cyber infrastructure, and threats that use cyberspace but do not harm it (risks *through* cyberspace).[26]

Defense against the first type of threat is called critical information infrastructure protection. A critical information infrastructure is a system with a computer dimension that controls the functioning of another physical system that is essential to the functioning of the economy and to state security. Defending such infrastructures is emerging as a major layer in the discussion of the security implications of cyberspace.

The second type of threat (risks *through* cyberspace) includes a range of actions made possible by cyberspace, including: encrypted communications for political opposition, instructions for terrorist activity, or international crime; traditional crime (fraud, theft, pedophilia) that is intensified by computer networks; new crime that is unique to cyberspace; computerized espionage; an attack on the provision of network services; and use of malware for a variety of purposes.

Threats can also be distinguished based on their geographic source: outside the country's borders or within, outside the computer network or within. The current structure of the internet communications protocol and the open architecture of the web, together with inherent vulnerabilities of software and hardware, make it almost impossible to locate the geographic source. In general, the path of data packets that move through the network is not fixed; the stations along the way are not required to examine the content of the data or their source, and are not required to document the path of the data packets. However, this is not a necessary property of cyberspace; rather, it is the result of a policy that encourages openness in access to information and free communications. This policy is rooted in the liberal ideology of the American pioneers of the web. With the privatization and commercialization of the information industries, the free market ideology, which recoils from any state intervention, also makes it more difficult to have a discussion about a different technical and legal organization of cyberspace.

Threats can also be distinguished based on the goal of the threat: crime, terrorism, industrial espionage, military espionage, cyber warfare. Such a classification ignores the fact that an identical method of operation can be used for many purposes. In addition, this classification is problematic in light of the great difficulty in tracing the source of the electronic signal moving through cyberspace and the identity of those who sent it.

Assessing the Cyber Threat

Unauthorized access to computer information resources is common to every kind of cyber threat. However, the unauthorized intrusion into a computer information resource opens a broad spectrum of possible results. What is the extent of the threat from the various actors? Are all the actors and the threats relevant to national security? How can we assess their importance and prioritize the response policy? A public discussion is needed in order to provide a serious answer to these questions.

Risk assessment is a wide and varied field used in various professions, and a professional discussion of it is beyond the scope of this article. For the purposes of the discussion, we will define threat assessment as the product of the probability of the event's occurrence and the assessment of the damage caused by the event.

In order to formulate policy, we need to assess the threat, i.e., the scenario that makes a policy necessary. However, it is not possible to make an assessment that is unequivocal, precise, and objective, because

Table 2. Characteristics of Cyber Threats

Type of Threat	Newness Level	Probability	Threat Effect
Harm to security forces' ability to function	Medium (relatively old threat)	Rising (widespread technological possibilities)	Intensified
Security espionage	Medium (relatively old threat)	Reasonable (widespread technological possibilities)	Intensified
Industrial, financial, information espionage	Medium (relatively old threat)	Rising (widespread technological possibilities)	Intensified (newness has great importance)
Direct harm to essential state services	*New* (not possible previously)	*Rising* (new technological possibilities)	*Highly intensified*
Full scale cyber war	New (not possible previously)	Low (cost/ benefit vs. kinetic war)	Medium

threat assessment on a national level requires that the social and cultural values of the country and the society be addressed. These values guide the relative importance of scenarios and potential threats to society. Such an assessment is a subjective one, but this is the most appropriate way to conduct a policymaking process. In a democratic state, the representative institutions and the media serve as a channel for the public to make itself heard and influence national security, wellbeing, and other issues. Regarding national cyber security, technical experts do not have a monopoly on assessing scenarios and making policy. Just as economists should not be allowed to determine the state budget by themselves, cyber security should not be entrusted to computer experts.

An approach to cyber warfare resembles an approach to any new weapon system. In order to assess the relative weight of the cyber threat in the framework of war, familiar variables such as effective range, extent of destruction by the attack, cost of use, political limitations on use, and others must be examined.

The cyber threat has the potential to be realized independently of the traditional security system. Cyberspace as it exists today is a wild battlefield. It makes possible direct transfer of data and commands while disregarding national and geographic borders and defensive arrays. As opposed to space, air, land, or sea, existing security organizations are only starting to function in cyberspace. There is a critical potential in cyberspace to undermine national security while bypassing traditional national defense frameworks and directly hitting critical targets on the home front. Thus, the developing phenomenon of cyberspace is creating a strategic change in the field of national security.

Table 2 is a proposed schematic summary of the types of cyber threats vis-à-vis their newness, probability of occurrence, and threat effect.

Conclusion: Strategic Properties of National Security in Cyberspace

The article is intended to conceptualize the developing field of cyber security and to create a common language for a public discussion. In light of the lack of conceptual clarity regarding cyber security, the article proposes explanations and operative definitions for these new topics. It reviews the properties of cyberspace and the existing weak points and threats, and presents problems of defense, attack, and deterrence in cyberspace.

Given the properties of cyberspace today, cyber warfare makes it possible to attack remotely tactical and strategic targets with little risk to the attacker. This limited risk is a function of: the difficulty in distinguishing between a glitch and an attack; the difficulty in connecting an event with a result; the difficulty in tracking the source of the attack and identifying the attacker; widespread use of inexpensive, off the shelf technologies; and the many vulnerabilities of a computer system. The cyber threat is asymmetric: no great investment is required for developing and using the weapons. In contrast, defense against cyber threats must encompass all channels of attack and keep up to date with new developments, and the cost of defense continues to grow.[27]

Do the cyber threats reviewed here threaten the national security of the State of Israel? A significant portion of the answer is derived from the concept of the role of the institution of the state and is beyond the scope of this article, which is not intended to provide an authoritative answer to the troubling questions that arise with the development of cyberspace. In an open, democratic state, the answers to questions of this type emerge through public debate and political process. The article is intended to contribute to an informed public discussion in Israel, and to focus the attention of the political system on new issues in national security.

The state has responsibility for national security, even when the playing field is developing and changing in form. The information age is causing far reaching changes in national security. Any computer network is exposed to an attack. There is no system that is immune from an attack or a glitch, and it is important to recognize this in order to free ourselves from the futile aspiration for total security. Nevertheless, it is necessary to aspire to optimal security while adapting to the nature of the threat and the target. An answer to the cyber security threat will be adapted to its special characteristics. To formulate a policy that suits the needs of the state, a public discussion and professional research are needed. Scientific and organizational work methods should be harnessed in order to provide security in the information age.

Notes

[1] There was a reduction in price of at least three orders of magnitude between the early 1970s and the middle of the first decade of the 21st century. A gigaflop cost $15 million in 1984 and $.14 in 2009. Regarding storage capacity on magnetic media, the price per gigabyte in 1993 was $1000; the price per gigabyte in 2009 was $.02.

[2] Since the dawn of history, human beings have aspired to survive and develop in the physical spaces surrounding them, first of all in the immediate physical space, the near environment: from animal domestication and agriculture and building, and extending to control and processing of raw materials using mechanical, chemical, and other methods. Since the scientific revolution, developed societies have learned to maneuver and sometimes even control their environment with the aid of the scientific method. The land space has naturally attracted most of the efforts. The maritime space was conquered by different civilizations throughout history, and states that succeeded in controlling the maritime space first enjoyed long term wellbeing. The aerial space was conquered in the last one hundred years, and there too those who were in control had a major relative advantage over their competitors. Since the 1950s and the launch of the first satellite in 1957, there has been competition between the superpowers over the means of reaching and staying in space, and over nearby planets. Progress in this field gained momentum as a result of the appearance of computing and electronics. Cyberspace is a new phenomenon. See Isaac

Ben-Israel, "From the Sword's Blade to Computer Memory," *Odyssey* 9 (October 2010).

3 For a discussion of the information technology revolution in military affairs (IT RMA), see Michael E. O'Hanlon, *Technological Change and the Future of Warfare* (Washington, D.C.: Brookings Institution Press, 2000); Stuart E. Johnson and Martin C. Libicki, *Dominant Battlespace Knowledge: The Winning Edge* (Washington, D.C.: National Defense University Press, 1995); Isaac Ben-Israel, "Security, Technology, and the Future Battlefield," in Haggai Golan, ed., *The Texture of Security* (Tel Aviv: Maarachot, 2001), pp. 269-327.

4 Andrew M. Colman, *A Dictionary of Psychology* (Oxford University Press, 2009), "cyberspace *n*." *Oxford Reference Online*, Oxford University Press, http://www.oxfordreference.com/views/ENTRY.html?subview=Main&entry=t87.e2037.

5 Julia Cresswell, *Oxford Dictionary of Word Origins*, "cybernetics." *Oxford Reference Online*, Oxford University Press, http://www.oxfordreference.com/views/ENTRY.html?subview=Main&entry=t292.e1374. The Hebrew word *kvarnit* [captain, leader] also derives from the Greek *kybernetes*.

6 Norbert Wiener, *Cybernetics or Control and Communication in the Animal and the Machine* (New York: John Wiley and Sons, 1955).

7 *Encyclopædia Britannica*, 2010, "space," *Encyclopædia Britannica Online*, http://www.britannica.com/EBchecked/topic/557313/space.

8 The internet is an open network of end points, devices, and computer networks that communicate with each other using the TCP or IP communications protocol. It is built in an open, decentralized manner, and from any end point in it it is possible to communicate with any other end point. Countless applications have been created on top of this basic design, and among them are those that are intended to limit access, verify identify, encrypt information transferred over the web, verify receipt of information, and so on.

9 "World Internet Usage Statistics News and World Population Stats."

10 For example, GPS, ACARS, SWIFT, GSM Cellular, and thousands of other mission-specific computer networks.

11 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009).

12 Electronics is the infrastructure of the computer world today. However, before electronics, computers were mechanical, and electronics is not immune to the future: the possibility of exploiting a biological infrastructure for computer purposes has already been proven. The computerization of DNA uses molecular biology and DNA instead of electronic components. Another possibility is the computerization of peptides: bio-molecular computerization, which is based on compounds made of at least two amino acids.

13 The pioneers, such as Reinhold or Barlow, saw the internet as being an open system, not hierarchical, and also anti-establishment. They hoped it would

allow a collaborative and egalitarian community and organization. See John Perry Barlow, "A Declaration of the Independence of Cyberspace." Lawrence Lessig describes the internet's principle of action: "Like a daydreaming postal worker, the network simply moves the data and leaves interpretation of the data to the applications at either end. This minimalism in design is intentional. It reflects both a political decision about disabling control and a technological decision about optimal network design." Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999). However, the reality is more complicated. For a discussion of the control structure of the internet, see Jack L. Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (New York: Oxford University Press, 2006).

[14] Induction (drawing conclusions from the specific to the general) is a very widespread tool, but it has a built-in limitation of logic: a view of an event and its recurrence does not offer a valid logical inference that this event is unavoidable. The problem of induction is that an inference from the specific to the general does not necessarily have validity.

[15] The definition proposed here intentionally resembles the definitions appearing in official documents of the various arms of the United States government. The United States and Israel share significant values and have similar scientific and economic levels, and therefore they see and interpret the situation with similar tools. The United States leads the scientific-technological research and development in the world, and at the same time, it leads policy on cyber topics. A comparative study that includes countries like China, Russia, India, France, and others will identify very different definitions. However, this research is beyond the scope of this article.

[16] Thucydides, *The Peloponnesian War*. The realistic theory of international relations enlists the history of ancient Greece to understand fixed human nature and international anarchy, which guide current events: Steven Forde, "International Realism and the Science of Politics: Thucydides, Machiavelli, and Neorealism," *International Studies Quarterly* 39, no. 2 (1995), and Azar Gat, *War in Human Civilization* (Oxford and New York: Oxford University Press, 2006).

[17] The Presidential Critical Infrastructure Board was established in 1996.

[18] Barack Obama, May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

[19] William Lynn III, "Defending a New Domain," *Foreign Affairs* 89, no. 5 (2010).

[20] Isaac Ben-Israel, "Information Warfare," *Maarachot* 369 (February 2000): 18-25.

[21] Following the terrorist attacks of September 11, 2001, the threshold for state support was lowered: it was enough that there be circumstantial evidence, such as ideological support of the enemy or provision of logistical services to terrorists, to be held accountable.

[22] Lynn, "Defending a New Domain."

[23] Libicki, *Cyberdeterrence and Cyberwar*.

[24] In France, Finland, Estonia, and Greece various government institutions have recognized the right to internet access as a basic right.

[25] This should be regarded as an expected phenomenon: the exponential development of information technologies is liable to fundamentally change existing fields of practice. As futurist and entrepreneur Ray Kurzweil writes, in this way the paradigm of biological research changed from traditional experiments to computation and simulation.

[26] Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4, no. 1 (2010).

[27] The argument about the difficulty of protection is similar to the argument against active anti-missile defense and today's argument about the Iron Dome system. It is also similar to the argument about the futility of defense against suicide bombers. Nonetheless, with the aid of the scientific method it is possible to create an answer to the new threats. See Lior Tabansky, *The Anti-Terrorism Struggle in the Information Age: Palestinian Suicide Bombers and the Implementation of High Technologies in Israel's Response, 2000-2005*, position paper published by Tel Aviv University, May 2007.