An Interdisciplinary Look at Security Challenges in the Information Age

Isaac Ben-Israel and Lior Tabansky

Introduction

Developments in electronics and computers since World War II have affected a broad range of fields and created the "information age." This article focuses on interrelationships among information technology, the information age, and security. More specifically, it aims to contribute to a discussion of the national security issues stemming from the development of information technology.

Much of the driving force behind computer development has been derived from military applications. Following new possibilities, thinking about the effect of technological change on defense issues has also progressed. In addition, the information age, which continues to develop rapidly, along with advances in computer communications and the penetration of computers into every area of life, has given rise to cyberspace. These developments challenge existing perceptions and force reconsideration of basic concepts. The need for an informed public debate and the design of a firm policy has likewise grown, given the fact that the cyberspace risk is already concrete – as dramatized by events in Estonia in the spring of 2007, as well as the Stuxnet affair.[1] In Estonia, daily life was disrupted following a technically simple but massive attack on internet-based services. With Stuxnet, it appears that a technically complex cyber weapon was used, designed to cause precise damage to the system controlling the industrial process at a protected nuclear fuel enrichment

Prof. Isaac Ben-Israel is head of the Yuval Ne'eman Workshop for Science, Technology and Security at Tel Aviv University. Lior Tabansky is a Neubauer research associate working on the Cyber Warfare Program at INSS, which is supported by the Philadelphia-based Joseph and Jeanette Neubauer Foundation.

facility in Iran. The weapon's design and method of operation included camouflage of its activity for a prolonged period. This cyber weapon apparently caused cumulative physical damage of strategic significance. The consensus is that in both incidents, states were behind the cyber attacks, though in both cases no definitive evidence exists.

A basic theoretical understanding of the information age is essential in order to consider cyber security issues. This article relies on ideas by philosopher Karl Popper, futurists Alvin and Heidi Toffler, and economist Paul Romer to illuminate the characteristics of the information age and to clarify the issues that emerge when technological development interfaces with national security. It analyzes the current characteristics of cyberspace, and discusses the implications for national security questions. It then reviews the field known as information warfare and focuses on the totally new phenomenon of computer warfare in cyberspace. The article then reviews cyber weapons and methods of warfare, discusses defense, attack, and deterrence, and presents key issues in the cyber defense realm. It appears that in order to maintain security and peace, a multidisciplinary assessment of the new issues and challenges is required.

Theoretical Background

Technological change occupies many thinkers who struggle to assess its social effects. Although the scope of this article does not permit a full review of the field, three thinkers relevant to an understanding of the dynamic reality must be mentioned.

The term "Third Wave," taken from the theories of the bestselling authors Alvin and Heidi Toffler, refers to a time period (table 1). According to the Tofflers, we are in the midst of a transition to the Third Wave, in which the economy is based on knowledge and control of information,[2] instead of on industrial mass production. Similarly, the form of warfare is changing as well. The name of the game has become obtaining information about the enemy and denying it information about yourself. The side that controls information technologies will win the war, even if it faces many weapons rolling off Second Wave assembly lines.

Table 1. The Waves According to the Tofflers

	Principal Resource	Who is Rich	Symbol	Weapons	Method of Waging War
The First Wave	Organized agriculture	Landowner	Sickle	Sword	Face-to-face battle at point blank range; land conquest
The Second Wave – from the mid-17th century until the end of the 20th century	Automated industry, mass production	Industrialist	Machinery of mass production assembly lines	Tank, airplane	Machines used at medium range, poor accuracy, attempt to damage production capacity
The Third Wave – from the end of the 20th century onwards	Knowledge	Bill Gates	Computer	Cyber warfare	Attempt to damage information through the use of computers. Remote damage to functional capacity, without physically reaching the target

Concepts developed by philosopher Karl Popper, who died in 1994, enhance the theoretical stage. Popper analyzed the world of knowledge as another existing concept, in addition to the material and spiritual worlds (table 2).[3] Popper insists that an entire "world" of human knowledge exists (World 3), populated by "beings" that are objective contents of thought, such as the Pythagorean Theorem and the laws of physics. These are neither "material" nor subjective "mental experiences." Once the Pythagorean Theorem was formulated, it became an objective truth independent of the spirit that created (or discovered) it. In other words, knowledge is objective, even though it is a product of the (subjective) human spirit.

Table 2. Popper's Three Worlds and Cyberspace

	Contents	Status	Examples	Example in Cyberspace
World 1	Material	Objective	Tables, airplanes	Hardware
World 2	Mental experiences	Subjective	Pain, happiness	Displays (the user experience)
World 3	Knowledge	Objective	Mathematics, physics	Software

Unlike material, knowledge can be used again and again and shared with many consumers without being diminished. Knowledge or information is a non-rival, partially excludable good. Paul Romer, a pioneer researcher in the new theory of economic growth, discusses the economic consequences of knowledge, and lays the foundations for a "different" knowledge-based economy.[4] He argues that growth in the economy, the basis of power and prosperity, is not solely a result of changes in capital and manpower. The development of knowledge is a new, potent source of endogenous growth. The character of this knowledge-based growth differs from what is familiar in the traditional economy.

If we combine Popper's metaphysical basis with Toffler's sociology and Romer's economic theory, we can suggest that the wars of the First and Second Wave were conducted mainly in World 1 ("material"). In these wars, the side with the largest and strongest army that was best able to mobilize troops and develop the mental factors (World 2) among its troops (e.g. the spirit of battle, motivation, and courage) would be victorious. According to this theory, future wars will also spread to World 3, the world of information. Without derogating the value of these elements in the future, while past wars relied on physical force (the First Wave) and present wars rely on the power of machinery (the Second Wave), future wars will rely more and more on brainpower.

Intellectual Approaches to National Security in the Information Age

The outstanding symbol of the information age – the electronic computer – was built at the end of WWII to help the US military in artillery ballistic calculations. In the decades following, especially after the invention of the transistor and the integrated circuit, computers have continually shrunk in size. Gordon Moore, co-founder of computer processors manufacturer Intel, stated in 1965 that the number of transistors that could be placed on an integrated circuit would double every 1-2 years, while the price would remain constant.[5] When this rule proved valid for semiconductors, the prediction was dubbed "Moore's Law." Futurist Ray Kurzweil presents persuasive arguments for extending Moore's Law to information technologies in general.[6]

With the development of the computer and its shrinking physical dimensions, defense institutions employ computing to improve the

performance of many systems. The chief benefit was a revolution in the accuracy of munitions, manifested first in airpower. Computers initially contributed to better operational planning. When it became possible to install a computer in warplanes, the power of computing was harnessed for the purpose of attack missions. An important strategic change occurred when the computer's dimensions and price were downsized enough that it could be embedded in ammunition itself. Thus was born the era of "smart weapons" – precision guided munitions that were initially adopted in aerial warfare. The operational results were stunning. In an attack on a specific individual target, such as a tank, one airplane armed with smart weapons can now do what 15 airplanes could do 30 years ago, or what 60 airplanes could do 40 years ago.[7] No wonder this technological revolution has had a decisive effect on the theory of warfare.

In order to adapt the art of war to information technology, a new theory of warfare dubbed "the Revolution in Military Affairs" (RMA) was developed in the early 1990s, based on four fundamental elements: precision strike, space power, dominant maneuver, and information warfare.[8] Information warfare involves several different aspects: computer warfare (computers are the main technological means of storing and transporting information), electronic warfare (mostly against sensors and communications systems), psychological warfare and managing the media (media briefings, embedding reporters in combat units, and manipulation of the information released to the public). These terms must be used accurately and the meaning of "information warfare" must be fully understood, particularly as these concepts have evolved with the advent and development of cyberspace.

The direct result of RMA is the absolute military superiority of the developed countries on the battlefield,[9] as reflected in the US wars in Iraq and Afghanistan, and in Israel's wars in Lebanon and against terrorist organizations. Indeed, a critical benefit of RMA is the unprecedented capability to conduct accurate and effective low intensity warfare, and the ability to defeat terrorism through military means, without causing widespread collateral damage.[10] As computer development continues, however, a change in approach is required. What follows is intended to provide a basis for an updated concept of national security in a reality that includes the new cyberspace.

Cyberspace

The ongoing growth of computers and communications networks generated a new situation at the beginning of the 21st century: an additional computerized layer above the existing older systems that effectively controls their function. The spread of computers, their integration in various devices, and their connectivity to communications networks have created a new space. Cyberspace is composed of all the computerized networks in the world, as well as of all computerized end points, including telecommunications networks, special purpose networks, the internet, computer systems, and computer-based systems. The concept also includes the information stored, processed, and transmitted on the devices and between these networks.[11] This picture enables us to understand what is happening in World 3[12] while focusing on the encounter with national security issues.

Unlike land, sea, air, outer space, and the electromagnetic spectrum, cyberspace is not a product of nature. Cyberspace is created by human beings, and would not exist without the information technologies developed in recent decades. Knowledge – which is perhaps the most important element in cyberspace – is a product of cumulative human endeavor.[13] The structure and design of cyberspace as it is today has significant consequences for national security (table 3).[14]

Table 3. Characteristics of Cyberspace and their Weak Points

Characteristic	Weak Point
Rapid change	Rapid obsolescence of means, including defense systems
TCP/IP protocol architecture	It is difficult to track the signal in the network and attribute it to a source.
High level of complexity	It is very difficult to connect an event to its cause, and difficult to distinguish a malfunction from an attack.
Extensive use of standard commercial off-the-shelf equipment	A narrowing gap between small and large players. The vulnerability of identical hardware and operating systems puts a broad range of systems at risk.
Entry-level cyber weapons are relatively cheap	The scope and price of defense is increasing.
An unclear legal environment	A gray area with a low probability of punishment encourages instability.

Cyberspace can be described as consisting of three layers.[15]

a. The most tangible layer, which currently provides the infrastructure of the computer world, is the physical layer. The physical components are the concrete building blocks of cyberspace – building blocks with natural characteristics: width, height, depth, weight, and volume.[16] In Popper's theory, the material layer corresponds to World 1.
b. The second layer is software logic, a variety of command systems programmed by people, intended to instruct a computing device. The physical components are controlled to a large extent by software, and the information stored on computers can be processed through software commands. The software layer is partly physical (World 1) and partly logical, meaning, again, World 3.
c. The third layer of cyberspace is the data layer that a machine contains and processes. The data and its processing generate information and knowledge. This layer is the least tangible of the three, mainly because the characteristics of information are very different from objective physical characteristics. This layer definitely belongs to Popper's World 3.

From Information Warfare to Cyber Warfare

In American and European professional literature,[17] information warfare is considered a significant feature of the information age. In American military terminology, information warfare is called "information operations," and its computerized component is called "computer network operations" (CNO).[18]

Table 4. Topics Included in Information Warfare

Topic	Relevant Systems and Technologies
Information collection	Various sensors in all parts of the electromagnetic spectrum
Transporting information for processing and the consumer	Broadband communications, compression, encoding, encryption
Storage and retrieval	Databases, de-duplication, compression
Processing and filtering information	Digital signal processing (DSP), automatic target recognition (ATR), data fusion, artificial intelligence (AI)
Making information accessible	Broadband communications, display systems, and a human-machine interface
Denial of information	Jamming, electronic warfare (EW), encryption, deception, obfuscation
Information protection	Denying unauthorized parties access to your information, encryption

Table 4 shows that the topics listed under information warfare are actually "classic" topics existing throughout the history of war. In the course of history, several classic methods of warfare have been developed for "information warfare," including intelligence gathering by human "sensors" (as in Joshua's use of spies in the conquest of the Promised Land) and the development of special gathering technologies (such as airborne intelligence sensors, satellites, etc.). Classic methods have also been developed in the prevention aspect of information warfare, such as camouflage, dummies and masks, jamming and blocking, deception and misdirection, propaganda, and so on.

Further analysis of table 4 indicates that the increasing dependence of information systems on computing is practically the only innovation in this field. In other words, while information warfare is not new, this is not true of computer-based information systems. Cyberspace makes it possible to define new targets, weapons, and methods of warfare. What is new about Third Wave warfare or war in the information age is not information warfare per se, but computer warfare. For this reason, it is best to limit the discussion by focusing on computer warfare in cyberspace. The change in cyberspace is so great that the basic concepts, such as "war," "weapon," "attack," and "defense," require a new explanation.

Computer warfare in cyberspace is unauthorized access to the adversary's computer systems for the purpose of intelligence gathering, disruption, deception, and prevention and delay of the use of information, while preventing the enemy from doing the same to one's own computer systems. A traditional attack (barrage, bombing, physical sabotage) on computer systems will also certainly cause disruption, prevention, and delay in the use of information. Such a physical attack, however, is not classified as cyberwar.

The characteristics of cyberspace[19] also define warfare in this sphere. The characteristics of cyberspace make it difficult to distinguish between a deliberate attack and malfunction, and complicate the effort to attribute action to a specific party, thereby also making it difficult to respond to an attack. The characteristics of cyberspace today empower marginal players, and give the attacker an advantage over the defender.

In recent years, a discussion has developed about the vulnerability created by the indispensability of cyberspace in all life processes in a developed society.[20] Computer warfare is not confined to military systems;

with the spread of computers and communications networks, it has become applicable to all areas of life. Most systems in the civilian economy and the entire critical infrastructure are now dependent on computers, and are part of cyberspace. This fact generates vulnerability and new possibilities for warfare, and also requires defensive preparation in developed countries.

Attack and Defense in Cyberspace

Cyber weapons[21] are malware and harmful hardware that damage the victim's computer resources and disrupt his data, deceive, and cause deprivation of service or the collection and transfer of intelligence. "Malware" is hostile software designed to disrupt orderly activity of a computer system and damage the process managed by that system. "Spyware" is hostile software designed for covert data collection and its potential transmission over a network. "Phishing" is a stratagem based on software and social engineering designed to fraudulently obtain personal data and details of user identities to gain unauthorized access to sensitive resources.

Hardware can be implanted through the addition of an electronic component to an existing unit, or an addition within an integrated circuit. The implant can take place during manufacture, transportation, operation and maintenance.[22] The use of software as a logical weapon, more common than the use of hardware, is what enables the most advanced methods of warfare. Knowledge and technology are non-rival, partially excludable goods; these inexhaustible characteristics make them hugely important in all matters pertaining to information warfare. Not all the consequences of this potential have been fully clarified.[23]

When there are good grounds to suspect that a cyber attack is underway, it is very difficult to identify the source and the attacker's identity. All parties operating in cyberspace use common tools and methods. Commercial cooperation, a kind of outsourcing, frequently takes place between the technical parties possessing attack capabilities (programmers, encoding hackers, owners of "captive networks") and those ordering the services (private investigators, organized crime, espionage organizations). In order to determine that a cyber attack is an act of war, several aspects must be examined:

a. The organizational and geographic source: whether a state is behind the action[24]

b. Motive: whether it is possible to identify an ideological, political, economic, or religious motive for the attack
c. Level of complexity: whether the attack required complex planning and coordinated resources that are available primarily to state agencies
d. Results: whether the attack caused damage and casualties, and whether it would have caused damage without the defensive actions taken.

The characteristics of cyberspace make it difficult to answer these questions, and answers sufficient for setting policy will undoubtedly be lacking.

For adequate defense, it is necessary to discern there is an attack, which is no simple matter in cyberspace. Early implantation of malicious hardware or software, especially before testing plans have been formulated, reduces the chances of detection. More accurate cyber weapons cause little collateral damage, which makes detection of the attack by the victim less likely. Defensive actions involve three aspects:[25]

a. Detection: the Achilles' heel − how to realize that a computer attack has taken place
b. Prevention: a means of stopping the attacker at the penetration stage
c. Response: recovery measures to limit the attacker's achievements, forensic means, and even retaliatory action.

Key Issues in Cyberwar

The technological change underlying the transition to the Third Wave, the rapid expansion of World 3, and the development of the information economy raise new questions. One of the most important is the debate on critical infrastructure protection. The feasibility of a cyber threat to the infrastructure of a modern society was presented through experiments, such as a power generator being put out of action and blown up by broadcasting commands to its command and control system.[26] It appears that this threat became a reality in the summer of 2010, when the Stuxnet worm virus that infected "Windows"-based computers was discovered. It searched for computers running Siemens-produced industrial command and control software of a certain type connected to an industrial controller of a specific model. Only if it located the relevant computers, the virus activated software code that disrupted the activity of the computerized controller, while concealing the change from the control software and equipment operators. Stuxnet allegedly damaged the proper operation

of the centrifuges for uranium enrichment in Iran. The source and duration of the attack are unknown.[27]

The US, the world's only superpower, is a pioneer and leader in the discussion of its cyber vulnerability.[28] A country's critical infrastructure is an obvious target in any conflict. Nonetheless, why has such concern been raised now, and in the strongest countries? The answer lies in the transition from the wars of Toffler's Second Wave to the wars of the Third Wave, the information wave. Discussion of critical infrastructure protection has been renewed because of the emergence of a new threat that could not have been carried out before. The development of cyberspace makes it possible, for the first time in history, to attack critical infrastructure systems in cyberspace, without physical access to the site and without exposure during or after the attack.

Critical infrastructure protection is one of the key issues of cyber security. The topic is outside the scope of this study, and deserves a specific discussion of its own.[29]

"Information warfare" immediately invites examination of the concept of war itself: is a cyber attack on computerized information involving no use of firepower an act of war? What constitutes a legitimate target in such a war? The extensive military use of civilian infrastructure (mainly communications) complicates the distinction between military and civilian targets. For example, the computer infrastructure of the US Department of Defense consists of 15,000 networks and seven million facilities dispersed all over the world. Most of the US Defense Department communications, however, are channeled through commercial civilian networks.[30] Civilians (even women and children) can be as effective as soldiers in computer warfare. Does this make them potential targets of a response? How should we act in a case of widespread economic damage? Moreover, the meaning of such an attack is unclear. Assume that one day the computer systems of the Israeli banks crash. Assume also that we manage to determine with certainty that the enormous damage was caused deliberately by a deliberate penetration, and assume that we succeed in tracing the attacker to the territory of a neighboring country. Now, is this an act of war? Ostensibly, the damage caused is "only" economic; there are no (direct) human casualties. Countries have frequently responded with restraint to traditional attacks that caused economic damage but did not take human life.[31] Economic damage, however, is liable to paralyze

an entire country. How do we estimate the indirect damage caused by an attack? Assume that a cyber attack caused prolonged disruption in the supply of electricity. Assume that one of its results is putting road lights and traffic lights out of commission, and the resulting darkness causes fatal traffic accidents. Should a victim of such an accident be considered a cyber warfare casualty? Should we respond with firepower and ground maneuver, or with a cyber counterattack? The problem is more complicated than the scenarios described, because a computer attack does not require a base in a country, and it can also be conducted by organizations and even by individuals.

Computer warfare is also conducted between friendly countries competing for diplomatic and economic intelligence. Is this "warfare?" Is it acceptable or advisable to use computer warfare in peacetime for such purposes?

A special problem in cyber warfare is detecting an attack; in contrast to a traditional attack occurring in World 1, the material world, the location of the strike and the attacker's identity are not necessarily exposed following the attack. There are no defined "front lines" in computer warfare, and geographic distance has almost no meaning in electronic networks. Given the characteristics of cyberspace, detecting an attack cannot be taken for granted: an attack and a malfunction have similar effects. While the computer world has become more sophisticated, as reflected in the multiplicity of software and applications and the growing number of transistors in each component, malfunctions are not less likely. The statistical probability of a software "bug" or programming error is constant, and its nominal value rises with increased complexity of software.[32]

The capability to detect that computers have been attacked and damaged, rather than malfunctioning "naturally," is inadequate. Without the ability to distinguish in real time between an attack and malfunction, large scale investment in constant cyber readiness is necessary. Defense against cyber threats must encompass all aspects of attack and be updated with new developments, and its cost is rising steadily. The argument on difficulty of defense is similar to the argument against an active anti-missile defense and the argument that defense against suicide terrorists is futile. Nevertheless, it is possible to devise a response to the new threats,[33] although the burden is substantial, since the characteristics of today's cyberspace give a clear advantage to attack over defense.[34] The field of

encryption is one of the few areas in cyberspace in which the defender still enjoys an advantage over the attacker.[35] Given the difficulty of identifying the fact of an attack, its geographic location, and the identity of the attacker, a state of uncertainty results that makes an escalating response difficult. Table 3 above summarizes the characteristics and many weak points that create the "attribution problem": it is hard to know the attacker's source and identity and on behalf of whom he operated, and it is certainly hard to prove guilt. In the traditional defense realm, great effort is expended on intelligence, advance warning, and deterrence in order to limit as much as possible the resources spent on a state of continual readiness. The problem of deterrence is particularly difficult in cyberspace, mainly because of the attribution problem.[36]

The characteristics of cyberspace give rise to problems for an attacker as well. How can one tell whether the cyber-attacked computers have really been damaged? In order to rely on a cyber attack, battle damage assessment is necessary. From this perspective, an open loop attack, i.e., one whose degree of success is unknown, is of limited utility. This problem is especially acute if the cyber attack was not intended to destroy data but to manipulate it.

In conventional warfare, rules have been developed that are anchored in international conventions. These conventions, which were written before the emergence of cyberspace, deal in "armed conflict," "physical confrontation," "territorial attack," and so on. These concepts are irrelevant to computer warfare, and the existing conventions require adaptation to cyber warfare – Third Wave warfare. Despite widespread research in this field, it is reasonable to assume that an assessment of the issues from a legal standpoint will take many years. The absence of rules makes it difficult to cope on a daily basis with the special problems of cyber warfare. The issues reviewed are not purely legal; they are essential issues for policymaking and taking decisions. In late 2011, NATO was in the midst of formulating a legal framework to enable it to respond to cyber attacks using methods currently of uncertain legality. An understanding of the theoretical foundations of the field is critical for improving the ability to cope with it.

Conclusion

Cyberspace is a fairly new product of the information age, and cyber security is part of the transition to the information age. In order to cope

with this challenging change, a multidisciplinary perspective should be adopted. Therefore some of the information age's important theoretical origins were presented, including ideas of the Tofflers, Karl Popper, and Paul Romer. Clearly there are other sources, and further multidisciplinary research on the information age is welcome.

The problems in dealing with security challenges are a function of the characteristics of cyberspace: rapid action, the rate of change, intricacy, and complexity. Cyber attack and defense take place in World 3, the world of knowledge. The significant consequences of the key issues of cyber warfare described in the last section of this study should be investigated in depth.

The key development is not "information warfare"; it is computer warfare in cyberspace. Discussion of solutions to "computer matters" tends to focus on the technical realm, far away from public debate and public policy. Clearly professional understanding of the field under discussion is essential, and it presents enormous challenges requiring a solution at the national public policy level. However, a review of the main issues of cyber security paints a complicated picture, beyond the technical computer professions. In order to provide national security in the dynamic environment of the information age, it is therefore correct to utilize inputs from every relevant field of knowledge, including the social sciences, psychology, biology, medicine, and philosophy. This study aims to encourage interdisciplinary research into the cyber security challenges, contribute to the development of an informed national security policy, and thereby contribute to security and prosperity in the information age.

Notes

1 "The Meaning of Stuxnet: A Sophisticated 'Cyber-Missile' Highlights the Potential – and Limitations – of Cyberwar," *Economist (GBR) Economist* 397, no. 8702 (2010), September 30, 2010, from the printed edition.

2 Information or data is distinguishable from knowledge, which also requires conceptualization and understanding of the raw information. This distinction is unimportant for the purposes of this article.

3 Karl Popper, *Objective Knowledge: An Evolutionary Approach* (Oxford: Oxford University Press, 1972), chapters 3-4.

4 Paul M. Romer, "Endogenous Technological Change," *Journal of Political Economy* 86, no. 5, pt. 2 (1990): S71-S102.

5 E. Mollick, "Establishing Moore's Law," *Annals of the History of Computing, IEEE* 28, no. 3 (2006): 62-75.

6 Ray Kurzweil, "The Law of Accelerating Returns," (2001).

7 Isaac Ben-Israel, "From Sword Blade to Computer Memory," *Odyssey 9*, October 2010.

8 For information on RMA, see: Michael E. O'Hanlon, "Technological Change and the Future of Warfare" (Washington, DC: Brookings Institute Press, 2000); Stuart E. Johnson and Martin C. Libicki, "Dominant Battlespace Knowledge: The Winning Edge" (Washington, DC: National Defense University Press, 1995).

9 This ascendancy has caused the enemy to retreat to a strategy of survival and asymmetric warfare.

10 This capability was demonstrated for the first time in Israel's victory in 2000-2005 over Palestinian suicide bombers during the intifada. 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.

11 The great resemblance between the American and Israeli definitions is a result of shared values and a similar scientific and economic level. China, Russia, India, France, and other countries define cyberspace and cyber threats differently. Such a comparison, however, falls outside the bounds of this study.

12 See the discussion above of Karl Popper's theory.

13 A discussion of the status of knowledge appears in Karl Popper, and was mentioned in the preceding section.

14 For a discussion of cyberspace in the context of national security, see Lior Tabansky, "Basic Concepts in Cyber Warfare," *Military and Strategic Affairs* 3, no. 1 (2010): 75-92.

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

16 Today, the infrastructure of the computer world is electronics. Before electronics, there were mechanical calculators. And in the future? The practicality of utilizing biological infrastructure for computational purposes has already been demonstrated. DNA computing uses molecular biology and DNA instead of electronic components. Another possibility is peptide computing: bio-molecular computing based on amino acid compounds.

17 Compare the definitions of the US Defense Department, "Joint Publication Jp 3-13: Joint Doctrine for Information Operations," edited by United States Department of Defense, Washington, DC, 2006, with those of the European Union as defined in the tender of the European Defence Agency Study, "Computer Network Operations (CNO) for EU-led Military Operations," 10-CAP-OP-37 (EU Milops CNO Capability) – Annex, August 16, 2010.

18 This includes computer network defense (CND), computer network exploitation (CNE), and computer network attack (CNA). The technical basis for the three types of action is identical.

19 See table 2 above.

20 For example, see Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What To Do About It* (New York: Ecco, 2010); Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, *Cyberpower and National Security* (Washington, DC: Center for Technology and National Security Policy, National Defense University Press: Potomac Books, 2009); William Lynn III, "Defending a New Domain," *Foreign Affairs* 89, no. 5 (September-October 2010); Martin Coward, "Network-Centric Violence, Critical Infrastructure and the Urbanization of Security," *Security Dialogue* 40, no. 4-5 (2009): 4-5; Walter Gary Sharp, "The Past, Present, and Future of Cybersecurity," *Journal of National Security Law and Policy* 4, no. 1 (2010).

21 For a discussion of the technical issues, see Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (O'Reilly Media, 2009); and Rick Lehtinen, Deborah Russell, and G. T. Gangemi, *Computer Security Basics* (Sebastopol, CA: O'Reilly & Associates, 2006).

22 Faulty hardware implanted by the CIA in a system for transporting gas purchased by the Soviet Union allegedly caused an enormous explosion in Siberia in 1982. See W. K. Clark and P. L. Levin, "Securing the Information Highway: How to Enhance the United States' Electronic Defenses," *Foreign Affairs* 88, no. 6 (2009).

23 For the economic consequences, see the discussion by Paul Romer mentioned above.

24 Following the September 11, 2001 terrorist attacks, the policy support threshold was lowered: sometimes circumstantial evidence, such as ideological support of an enemy or provision of logistic services to terrorists, is sufficient.

25 A detailed discussion of these matters is beyond the scope of this study.

26 "The Aurora Experiment," conducted in the national laboratories in Idaho, US; See James Andrew Lewis, "Thresholds for Cyberwar," Washington, DC: Center for Strategic and International Studies, 2010.

27 "The Meaning of Stuxnet," note 1.

28 United States, President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection," Washington, DC: US GPO, 1997.

29 See Lior Tabansky, "Critical Infrastructure Protection against Cyber Threats," *Military and Strategic Affairs* 3, no. 2 (2011): 61-78; Myriam Dunn, "Securing the Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory," in Johan Eriksson and Giampiero Giacomello, eds., *International Relations and Security in the Digital Age* (Routledge, 2007).

30 Lynn, "Defending a New Domain."

31 Israeli governments behaved in this manner for years, when thousands of rockets "trickled" into Israel from Gaza and hit open areas in the western Negev.

32 One of the measures of software complexity is the number of source lines of code (SLOC). *Windows NT 3.1*, the Microsoft operating system, which was introduced in 1993, had 4.5 million SLOC. *Windows XP*, introduced in 2001, had 45 million SLOC. Linux Fedora 9 has 204 million SLOC.

33 See Tabansky, "The Struggle against Terrorism in the Information Age."

34 Ibid., and Lynn, "Defending a New Domain."

35 The dominant encryption method is based on a mathematical principle that it is difficult to factor a number whose factors are prime numbers. Quantum computing has features that will completely eliminate the advantage of the existing encoding methods. When a quantum computer is built, the security field will undergo an upheaval caused by the foundations of encryption being made obsolete.

36 Libicki, *Cyberdeterrence and Cyberwar*. See also Amir Lupovici, "Cyber Warfare and Deterrence: Trends and Challenges in Research," *Military and Strategic Affairs* 3, no. 3 (2011): 49-62.