Not Merely a Technological Advantage: The United States' Organizational Change in Cyber Warfare

Amit Sheniak

The cyber arms race is part of the state security reality in our times, resulting in a sharp increase in the allocation of resources for the technological development of new defensive and offensive cyber capabilities. This article stresses that a different policy should be taken, arguing that due to the unique characteristics of the cyber dimension and the declining level of technological sophistication needed for offensive and defensive cyber capabilities, a security advantage in this field will results from a creative advancement and development in force organization specifically by formulating a new doctrine of warfare, which will aim to improve the integration of security activities in both cyberspace and in physical spaces. The review stresses the changes and increased scale of cyber threats, the changing perception of the threat, and the transition from a technical approach to one that regards the internet as a new operational space with unique characteristics. This article is based on a comprehensive review of the legislation, plans, and decisions concerning the force building organizational process, and cyber operations doctrine in the United States from the early 1980s through 2012. Although the article focuses on the United States during a limited timeframe, its aim is to shed light on the field of organization as a relevant and significant theater in which a political advantage in cybersecurity can be achieved, in contrast to the current state in which researchers and decision makers focus

Dr. Amit Sheniak is a post-doctoral research fellow in the Science, Technology, and Society (STS) study program at the Harvard Kennedy School of Public Administration.

more on technological development as the tool for acquiring an advantage in this sphere. The conclusions of the article are relevant to both professionals and decision makers.

Keywords: Cyberspace, cyber security, force building, organization, theory of warfare, United States, strategic advantage, dominance

Introduction

The struggle between countries in the cyber realm has been evident for quite some time and has been a frequent subject of research in the fields of security studies and international relations.[1] The arms race and military force building in the cyber realm have been manifested by a significant increase in the allocation of national resources for securing cyberspace.[2] In view of this intensive activity, it is worthwhile to ask how a state can achieve an advantage within the existing cyber arms race.

In this article, I will argue that "Cyber-Dominance" is not only a reflection of the technological development of new and more advanced tools and the operational experience in cyberspace, but also by organization and methods of the security forces and military units in this space, coordinating between the political and military echelons to reflect the changing cyber threat on the countries and the necessary military action. In other words, because we live in a period in which cyber warfare capabilities can be developed relatively easily and the level of sophistication required of the attacker is declining, the distinguishing factor between countries and other international players

1 The following are several known examples of this: Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Washington: CCSA Publication, 2013); Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2007); Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2009); Ben Buchanan, *The Cybersecurity Dilemma: Hacking Trust and Fears between Nations* (New York: Oxford University Press, 2016); P. W. Singer and Allen Friedman, *Cybersecurity and Cyberwar: What everyone Needs to Know* (Oxford: Oxford University Press, 2014); Harris Shane, *@ War: The Rise of the Military-Internet Complex* (New York: Mariner Books, 2015).

2 This can be seen in the figures of international insurance companies. See, for example, "Risk Nexus: Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Future," *Atlantic Council and Zurich Insurance Group Report*, September 10, 2015, Figure 13, http://publications.atlanticcouncil.org/cyberrisks/.

in cyberspace may be the investment in organizational processes and the building of force to achieve a political advantage in cyberspace.[3]

Although the article is not based on a comparative study,[4] the American example, which will be described extensively below, is significant, because it indicates a conceptual and organizational change. In this framework, the United States adopted an approach that regards the cyber realm as cyberspace, or more accurately, as a cyber battlefield.[5] This is the basis for the current military concept in the United States, which led to the organization of American cyber force. This battlefield requires integrated state and military action, similar to the action required to preserve the territorial security and interests of a country in physical space—the air, sea, and land.[6] This assertion will be tested in the article by analyzing the development of the security approach, especially the organization and force building in the cyber realm, as reflected in unclassified official documents. This analysis will be presented according to three timeframes: The first is 1983–1998, when the process of realizing the potential risks posed by the cyber realm to state interests began, and American intelligence units were organized to safeguard sensitive information existing in different computer-mediated communications systems. The second is 1998–2008, when the American defense establishment realized the significance of computer-mediated communications systems and their consequences for the regular functioning of critical infrastructure and key resources needed in a modern country (e.g., water and food, energy, and transportation). The third is 2008–2012, when the concept of cyberspace was

3 The term "organization and force building" refers to the process of planning, change, and arranging responsibility among various agencies in a specific area of warfare for the purpose of control, command, and development of special personnel, weapons, and doctrine.

4 For a comparison of cybersecurity policies in the United States, Israel, and China, see Amit Sheniak, "Cyberspace as a Border Area: Creating Sovereignty and Enforcement Capability in Cyberspace in Israel, the United States, and China," published by the author, Jerusalem, 2015 (in Hebrew).

5 This approach is also reflected in a change in the definition of the professional terms that currently refer to cyber as an environment, dimension, or space.

6 It should be noted that several studies dealing with the use of language, metaphors, images, and models from other security spheres and technologies, especially nuclear weapons, also mention the importance of the conceptual change in cybersecurity. They do not, however, emphasize the organizational and institutional change on which this article focuses.

revolutionized, and the attitude that was adopted was that military effort in this sphere was an endeavor comparable and tangential to other dimensions (sea, air, and land).

The survey presented in this article indicates that the logic guiding the force building for action in cyberspace among countries and powers like the United States has undergone changes over the past thirty years, given the increase in cyber threats and their effect on a range of state interests. These changes support the article's assertion that the United States is the leading player in the cybersecurity field, to a large extent because it has reorganized its military cyber force based on the same logic that guided the organizing of its aerial, naval, and ground forces. The article does not intend to analyze the disputes within the military and security personal about the advantages and disadvantages of different approaches to organization of force building in the cyber realm or to reconcile them.[7] Rather, the article seeks to highlight the importance of moving ahead with the organization of a national cyber force under the notion that the cyber realm is a battlefield comparable to physical battlefields. This contrasts with the prevailing idea among cybersecurity researchers and decision makers today who focus on technological development and operational experience as the important tools and as the main foci of investment for gaining an advantage in this field.[8]

It can be argued that this organizing concept of cyber power distinguishes between military action of countries leading in cybersecurity (such as the United States) from other political entities and from state, super-state, and sub-state players. The leading countries conduct a regular and coordinated military effort, executing plans and orders that are aimed at achieving a specific tactical and or strategic goal in cyberspace (similar to aerial, naval, and ground operations). Other entities operate irregularly in cyberspace in a "parasitic" network pattern similar to terrorist actions and guerilla warfare, seeking to sabotage, disrupt, intimidate, and influence consciousness by means of computerized communications.

---

7 For example, on the question of whether defensive, offensive, and intelligence gathering personnel should be integrated in the agency, whether the dominance of intelligence or technological personnel should be maintained, and so forth.

8 See, for example, the trend towards technological analysis in articles in cyber policy journals such as *Cybersecurity Journal* and *Journal of Cyber Policy*, which emphasize technological development and operational experience as important tools in assessing and promoting cybersecurity.

1983–1998: The Information Security Concept

The perception of the threat to information and communications technology (ICT) and accordingly the US organization and force building in cyberspace shifted between 1983, when the US military computer system (Milnet) separated from the civilian computer network, and 1998 when the characteristics of the threat had changed. The crux of the change resulted from a more ambivalent attitude towards the advantages and disadvantages of computer-mediated communications technology. This was reflected in a shift from state actions designed in principle to improve and streamline the flow of information to operations aimed at creating control, command, and barriers for protecting sensitive state information (defense and civilian).

The practical significance of the US force building in cyberspace was then reflected mainly by defensive operations for securing sensitive information, such as information collected by armies and intelligence agencies; and computer databases, which over the years became the main means of storing and managing this information. The main actions taken vis-à-vis the computer networks of the intelligence organizations and the army were to upgrade the ability to control secret and classified information (for example, by creating a separate and closed communications network for the army), and for the first time, to obtain valuable covert information within the framework of intelligence and information warfare for formulating the state's legal authority needed for this action. During this period, special institutions and units were founded; the definitions of the responsibility of existing government and defense agencies were changed; and legislation was passed that banned unauthorized entry into sensitive computerized databases and permitted punishment and enforcement. These changes nevertheless did not lead to a substantial shift in military thinking.

The physical and institutional separation between military and civilian computer-mediated communications greatly affected the control and security of computerized information. A series of actions led to this separation, namely the removal of the military communications system from the civilian communications system in 1983; the creation of a classification system that only allowed people in relevant jobs to operate within it;[9] legislation in 1984 that forbade civilians without permission from entering into federal systems

9 Tamar Ashuri, *From the Telegraph to the Computer: A History of Electronic Media* (Tel Aviv: Riesling Publishing, 2011), p. 138 (in Hebrew).

(defined as "protected computers");[10] and expanding the authority of the American Secret Service to protect these systems.[11]

Reports of espionage and criminal cases of breaking into computer systems, such as the "Cuckoo's Egg"[12] and the arrest of the "414 Gang" in 1983, brought about additional legislation called the Computer Security Act of 1987,[13] which mandated the development of criteria and standards for securing computerized information in the federal authorities;[14] the training of special personnel; and instruction of employees about the potential risks of the computer systems.[15] In addition, the same law stated that the civilian bureaucratic system would be subject to the supervision and instruction of the National Security Agency (NSA).[16] This subordination, which is one of the main institutional changes created then and enforced to this day, was given added validity by Presidential National Security Directive 42 in 1990, which ordered the strengthening of security for national communications systems and the differentiation of those systems from other public communications systems.[17] This directive placed the head of the NSA as the senior supervisory authority for all government departments, by means of a committee led by the secretary of defense established in the framework of the National Security Council.[18]

In 1988, following the public storm caused by the destructive effect of one of the first computer viruses—the Morris worm—which damaged 10 percent of all the computers that were connected to the internet at that time,[19] a Computer Emergency Response Team (CERT) was founded at the initiative of the Software Engineering Institute (SEI) at Carnegie Mellon University to

10 18 U.S.C. § 1030: Fraud and related activity in connection with computers, §a2C, (1986).

11 Ibid., §D.

12 Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy through a Maze of Computer Espionage* (New York: Doubleday, 1989).

13 Computer Security Act of 1987, Public Law No. 100-235 (H.R. 145), (1988).

14 Ibid, paragraph 1.

15 Ibid.

16 Ibid, paragraph 5.

17 The White House Office, "National Security Directive No. 42: National Policy for the Security of National Security Telecommunications and Information Systems," (1990), §2.

18 Ibid., §§4–6.

19 Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, p. 26.

deal with and minimize damage caused by attacks via computers. Although an academic institution took the initiative for establishing the center, the US administration worked to enforce and regulate its activity as the administration usually did with academic institutions—through a contract that stipulated that the US Department of Defense would fund its activity but would also define the framework for its actions.[20] The center later constituted the model for the frameworks of supervising and monitoring threats in cyberspace in the United States and many other countries.

During this period, the prevailing concept regarded the internet as a tool for enhancing capabilities in physical space and not necessarily as a new space for maneuvering between countries. This originated with the security approach and the American military doctrine published in 1996, which had been formulated by the US Armed Forces Joint Chiefs of Staff in their vision about the needs of the future battlefield by 2010. Even though computerized capabilities were already significant at the time,[21] the internet—which was conceptualized for the first time in the military framework as a "network of networks"— was perceived mainly as basic infrastructure that facilitated the ability to use advanced weapons based on an information grid.[22]

This doctrine led to the establishment in 1995 in the US Air Force of a special unit for defensive and offensive warfare using computer-mediated communications, called the 609th Information Warfare Squadron.[23] The highest command regarded fighting by means of computers as only another form of warfare and not as an independent battlefield with its own defensive and offensive efforts,[24] which therefore required the reorganizing of the military

20 "US Department of Homeland Security Announces Partnership with Carnegie Mellon's CERT Coordination Center," *SEI Press Release*, September 15, 2003, http://www.sei.cmu.edu/newsitems/uscert.cfm.

21 For example, the defense of computerized infrastructure was addressed in the joint chief of staff's document, but it was mentioned as a tool whose main purpose was to enable superiority in information warfare.

22 US Office of the Joint Chiefs of Staff, "Joint Vision 2010," (1996), p. 16.

23 The unit operated from 1995 until 1999, when it was subordinated to the new military organization in cyber warfare. For the official history of the unit, see US Department of the Air Force, "609th IWS: A Brief History, October 1995–June 1999," (1999).

24 It should be noted that in contrast to this concept, the working echelons that founded the 609th Information Warfare Squadron realized that they were pioneers of the new battlefield. They even compared themselves to the first squadron that developed the theory of air warfare in 1913. See Ibid., p.1.

force.[25] This approach is expressed in an official memorandum published by the Air Force commander and the secretary of the Air Force in 1997, which stated that "information warfare is a means, not an end, in precisely the same manner that air warfare is a mean, not an end."[26] The quote indicates that military thinking did not realize the importance of the concepts of "space" or "dimension" as a basis for determining defense policy in general (not only in the air or only in the cyber realm). It is possible that even today, there are those operating aerial, naval, and ground weapons who regard cyber operations as merely an act of support. At the same time, however, the approach of the writers of the memorandum held that the cyber threat was aimed only at information, and they had difficulty in predicting the extent of the current military endeavor in the cyber realm.

1998–2008: The Infrastructure Concept

During this period, the threat posed by computer networks shifted significantly, both in terms of the level of urgency and the risk posed to a state's sovereignty and its ability to function under attack. The reason for this shift was the changing technical characteristics of hacking into computer systems, which became increasingly complex, while the level of technical sophistication and knowledge needed by parties that committed the hacking declined substantially from the mid-1990s.[27]

A number of hacking events into the Pentagon computer systems in the late 1990s, both in the framework of the ER97 military exercise and in the Solar Sunrise espionage affair, were a wakeup call to the American defense system. These events also made it clear that the US military and security system did not have a single entity responsible for operations against threats of this type.[28] In November 1998, a special task force—the Joint Task Force for Computer Network Defense (JTF-CND)— was created, which

25 Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, p. 31.

26 US Department of the Air Force, "Cornerstones of Information Warfare," (1997), http://www.c4i.org/cornerstones.html.

27 US Department of Homeland Security, "Securing the Nation's Critical Cyber Infrastructure," (2010), p. 3. Note the graph on page 3, which marks the balance between the knowledge needed by the attacker and the level of sophistication of the attack in 1990s. In 1995, ready-to-use sophisticated attack tools could already be purchased.

28 Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, p. 36.

was subordinated to the Defense Information Systems Agency and later to the US Space Command. The task force acted in synchronization with the NSA and was designated for cyber warfare and for dealing aggressively (not passively) with attacks by foreign countries in order to secure computer networks.[29] This force, which was dismantled in 2010, was an important factor in promoting the readiness of the United States to defend itself in cyberspace, particularly as a result of the diverse and relevant personnel that established bodies capable of coping with offensive computer operations: computer specialists, military personnel from a variety of armed forces branches, intelligence personnel, and security personnel. Later, military personnel were also sent for advanced computer studies, creating an ideal combination with their professional training.[30]

In 2004, the task force assumed responsibility for all defensive and offensive operations in the cyber realm. It shifted from being directly involved in these areas to becoming a regular military staff agency that did not itself engage in defense or attack but rather synchronized and guided all the operative headquarters and tactical units responsible for security operations in cyberspace in the various branches and departments.[31] The new agency—JTF-CNO—led changes in both the bureaucracy-organization and in the practical defensive capability of the American security system. From an organizational standpoint, these changes were the turning point that later led to the establishment of the Cyber Command; from a practical standpoint, the task force—which had originally been formed to deal with security challenges—also achieved significance in capacity building for handling tangential matters that were not part of its original purpose but that jeopardized operational readiness and US sovereignty in cyberspace. Among other things, this involved independent viruses that contributed to the feeling of being under threat, due to the possible consequences of damage to computer-mediated communications.

This new perceived threat led to recognizing the need for an ongoing national status assessment to detect security problems in computer-mediated communications, as a tool for designing policy, and for planning and handling these problems. The assessment revealed that the main weak point was the

29 Ibid., pp. 38–40.

30 Ibid., pp. 38–39.

31 Ibid., p. 57.

country's critical infrastructure and basic civilian resources, which were not protected and not subjected to supervision and concealing of information, and were susceptible to possible damage via the computer communications upon which they relied. One measure for handling this risk was the Critical Infrastructure Information Act of 2002. This law defined the term "critical/essential infrastructure information" as part of a plan for dealing with damage to this sensitive infrastructure,[32] and expanded the definition of the term "protected systems" to also include civilian public systems.[33]

In 2003, President George W. Bush and the secretary of Homeland Security issued the Homeland Security Presidential Directive No. 7 (HSPD7), which validated the need for non-military security activity for defending civilian infrastructure. The agencies founded in this framework under the Department of Homeland Security assumed responsibility for the monitoring, planning, guidance, defense, and determining priorities in cyberspace (without operational forces; these were retained by the army and the intelligence agencies). Authority was also delegated to the various governmental departments to conduct a comprehensive survey that would include an assessment and review of all infrastructure and interests within their field of responsibility in order to locate possibilities of attacks against infrastructure by terrorist organizations using computerized means.[34] The directive also created an analogy between damage to computer systems of specific infrastructure and the use of weapons of mass destruction.[35] This comparison had doctrinal significance, as it led to the conclusion that the United States had to undertake the same kind of preparation and level of investment for cyber threats as they did for threats by conventional weapons and ballistic missiles. This comparison also led cyber warfare theory to

32 The complete definition stated in the law is "Critical infrastructure information means information not customarily in the public domain and related to the security of critical infrastructure or protected systems." See Homeland Security Act of 2002 – Critical Infrastructure Information Act, Public Law 107-296: Sec. 211/3 (2002).

33 Ibid., Sec. 211/6.

34 US Department of Homeland Security, "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection," (2003), §12.

35 Ibid., §13.

widely adopt the Cold War terminology—such as "deterrence" and "active defense"—which is still prevalent to this day.[36]

In 2003, the Bush administration published a national strategy for cybersecurity that was based on a survey of dangers and that included components indicating an important shift in consciousness and organization in both the federal administration and the private sector;[37] the formation of a security response team for cyberattacks on the basis of CERT; a plan for reducing security risks and national weak points vis-à-vis cyber threats; improvement of government cybersecurity; international cooperation for the purpose of improving national cybersecurity; and the establishment of two institutions in order to improve supervision of security for computerized financial infrastructure.[38]

The national strategy for cybersecurity included the private sector as an essential partner in creating security and preserving sovereignty, based on the realization that the steep increase in e-commerce had led to the ability to damage US economic interests. The Presidential Directive EO 13286 in 2003 further legitimized this approach and led to an additional organizational change: the appointment of official agencies to mediate between the defense sector and the private sector, such as the National Infrastructure Advisory Council and the Information Sharing and Analysis Center.[39] Despite the importance of the private sector, the focus of this article on the change in organizing the military force and security agencies does not allow for extensive discussion of the organizational change that was created in order to expand the cooperation between the security and private sectors in the United States, which currently is a key factor in monitoring cyber threats.

Another law from 2004 was designed to reform the American intelligence services so that they could adapt to the current threats.[40] For the first time, the law openly referred to the possibility that the United States would make

36 For a discussion of the question of deterrence in the cyber realm, see, for example, Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2016–2017): 44–71.

37 The White House, "The National Strategy to Secure Cyberspace," (2003), p. X.

38 "Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, p. 56.

39 The White House, "Executive Order No. 13286: Critical Infrastructure Protection in the Information Age," (2003).

40 Intelligence Reform and Terrorism Prevention Act of 2004, Public Law No. 108-458 (2004).

passive and active use of computer-mediated communications in order to improve its self-defense. The law also mentioned two different types of actions in cyberspace: offensive action against computerized transactions carried out by electronic means and designed to finance trans-border crime and terrorism, and intelligence action for gathering existing information in cyberspace in order to prevent members of terrorist and criminal organizations from entering the United States.[41]

The National Infrastructure Protection Plan[42] was published in 2006. It implemented the above-noted processes of organization and established the Department of Homeland Security as the agency that would coordinate and determine policy for the defense of critical national infrastructure and resources, including coordination between the civilian state bodies and the military and intelligence bodies. The plan defined cyberspace for the first time as critical national infrastructure that should be defended, rather than merely a tool through which infrastructure is damaged.[43]

The transition from policy decisions to reorganization of the military force took place in 2006, following the publication of the "National Military Strategy for Cyberspace Operation," which defined the military knowledge needed for integrating the American army into the efforts to defend cyberspace. This document defined the strategic context, the sensitivities, and the outlines for formulating a plan of action and a special doctrine for regular military activity in cyberspace,[44] but it did not stipulate the formation of a specific general command body for this matter.

2008–2012: The Spatial Concept

This period constitutes the peak of the institutional change in organizing the American forces in the cyber dimension. This change is characterized by two principles derived from the approach that regards cyberspace as militarily important: 1) organizing military power based on a spatial concept

41 Ibid., Sec. 6302§bl.

42 The document requires a periodic status assessment, the updated version of which is published every few years. This article relies on a later version of the document from 2009; see US Department of Homeland Security, "National Infrastructure Protection Plan," (2009).

43 Ibid., §3.2.5.

44 US Office of the Joint Chiefs of Staff, "The National Military Strategy for Cyberspace Operations," (2006), p. 1.

(cyberspace); and 2) the cyber dimension as a source of information and social and political interaction, which requires monitoring and supervision in order to maintain state security and promote national interests.

The attitude of the American administration towards the internet as a space having both specific characteristics and a complexity requiring a unique bureaucratic approach is evident in the documents accompanying the 2008 US presidential elections between Obama and McCain. Policy on cyberspace, especially its security dimension, became one of the key issues of that period. As a result, the Center for Strategic and International Studies published a report by cybersecurity experts, which was aimed at the incoming president.[45] The report called for increasing the federal government's involvement in cyberspace and opposed the approach that relied on internal arrangement led by the private sector. The report's recommendations also included a call for creating a balance of deterrence against enemies in cyberspace.

In 2009, at the beginning of Obama's term, the administration published a new policy entitled the "Comprehensive National Cyber Initiative" (CNCI).[46] The declared goals of the CNCI were to set in motion a widespread inter-agency measure aimed at improving the feeling of security in cyberspace among American citizens.[47] In this framework, the plan declared an organizational change in the handling of cyber threats, divided into two main efforts: 1) improving centralization in a way that would raise the level of state control and supervision in the cyber dimension; and 2) strategic planning and management of partnerships with international parties in this area. Improved centralization was reflected by technical development of command and control systems of federal information and computer networks.[48] The strategic planning was manifested by the establishment of institutions for long-term development and procurement that would prevent, among other

45 Center for Strategic and International Studies, "CSIS Commission on Cybersecurity for the 44th Presidency: Securing Cyberspace," (2008).

46 The plan was an implementation of President Bush's National Security Presidential Directive (NSPD), no. 54, which President Obama adopted. It included the recommendations of the CSIS report. See the White House, "Comprehensive National Cybersecurity Initiative," (2009), http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

47 Because the plan was an implementation of NSPD no. 54, which was classified in principle and reportedly focused on offensive and intelligence measures, it can be assumed that it also had undisclosed objectives.

48 "Comprehensive National Cybersecurity Initiative," pp. 2–3.

things, penetration of infected hardware components, and by setting targets for educating the administration's employees to be aware of the need to defend against cyber threats.[49] International partnerships were formed with various parties (countries, companies, and organizations) in order to create deterrent capability in the cyber realm.[50]

The need for regular and orderly strategic planning from the presidency on down was expressed in a series of documents written early during the Obama administration, including a founding document published under the title "Cyberspace Policy Review." This document recommended the establishment of the "Cybersecurity Office" as part of the presidential advisory team, in combination with the National Security Council.[51] The recommendation was applied in the Information and Communications Enhancement Act of 2009,[52] which also stipulated that the presidential cybersecurity advisor would head the Cybersecurity Office and would be part of the president's limited team of advisors.[53] The importance of establishing the Cybersecurity Office lay in improving the coordination and ability to carry out an overall security policy from the level of the president (the commander in chief of the US Armed Forces) to the various security agencies to the army units, and especially the capability to formulate measures for supervision that would be based on the development of standards for security in cyberspace in general and the national information systems in particular.[54]

Another significant result of the measure to centralize the cyber realm was improving the ability to formulate policy for the new legitimate use of force in cyberspace. This resulted from a policy of orderly response led by

49 Ibid., pp. 4–7.

50 Ibid., p. 5

51 The White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," (2009), p. 7.

52 The background for the law was a Senate hearing held in 2008 about the capabilities for defending the federal IT infrastructure as well as criticism of the FISMA law from 2002, based on the claim that the measures provided by the law for an assessment were murky and that it was not clear to each agency the extent of the information that it was supposed to oversee. See Information and Communications Enhancement Act of 2009 (S.921/ ICE Act), 111th Congress, Sec. 2/4, 5 (2009).

53 Ibid., Sect. 3552.

54 Ibid., Sect. 3556.

the president and was based on a report by the National Research Council,[55] which analyzed the legal and ethical consequences of cyberattacks and recommended that such attacks be perceived as constituting the "use of force," i.e., as justifying a military response (in the physical dimension).[56]

The most significant expression of the organizational and conceptual change relating to the internet as a space has been in the organization of the military forces and the doctrine for their deployment. The most prominent organizational change in the US military, reflecting its recognition of the existence of cyberspace, has been the official establishment of the US Cyber Command (USCYBERCOM). The decision to establish the command was made in 2009, declared operational a year later, and subordinated to the US Strategic Command (USSTRATCOM).[57] The new command was defined as a sub-unified/subordinated command; that is, a military body established by presidential order as a command entrusted with a specific spatial task requiring local expertise and operating under the spatial command of the US Armed Forces.[58]

Although fighting units using computers and computerized communications networks had already existed in the United States since the 1990s (see above about Unit 609), the creation of a sub-unified/subordinated command for this purpose reflected a shift in the concept and had profound symbolic and organizational significance. From an organizational perspective, even though a full spatial command or a branch/corps for cyber operations has still not been established,[59] the new military command currently guides and

55 This comprehensive report, which was written by a special committee formed by the National Research Council, analyzes many other aspects relating to online attacks in criminal and civil law.

56 William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds. *Technology, Policy, Law and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities* (Washington DC: National Academies Press, 2009), pp. 33–34.

57 US Department of Defense, "US Cyber Command Fact Sheet," (2010).

58 Other sub-unified/subordinated commands in the US Armed Forces were established to manage security in Alaska, provide aid in South Korea, and for the war in Afghanistan. See US Office of the Joint Chiefs of Staff, "Joint Publication 1," (2009), p. V–9.

59 The commands in the US Armed Forces are divided into spatial commands responsible for the use of force in various regions of the world (for example, CENTCOM, the central command, is responsible for the Middle East), and specialist functional commands are responsible for force building, training, and the allocation of forces, such as the Special Forces Command (SOCOM). This second category of commands also includes the conventional branches, such as the Air Force, Navy, and Army.

synchronizes all US military operations in cyberspace and constitutes the headquarters for cyber warfare in the various branches of the Armed Forces (Army, Navy, Air Force, Marines) that are professionally subordinate to it. Furthermore, the US Cyber Command is responsible for finding and developing personnel and weapons and for formulating a doctrine for the cyber realm. The creation of the US Cyber Command is a clear and overt symbol, emphasizing to other countries the advanced stage that the United States has reached in the militarization of cyberspace. This status of the United States as a leading—and possibly the only—military power in cyber warfare has led to similar organizational changes within the armies of other countries (for example, China established its cyber command in 2010).[60]

The organizational change, which culminated in the establishment of the US Cyber Command, accompanied—and possibly also led—a change in the military doctrine as published in official documents of the US joint chiefs of staff. Recognition of cyberspace as a space in which warfare takes place simultaneously with and in addition to the existing battlefields began in 2006, but it appears that this knowledge did not crystallize into a regular doctrine until 2012 when its main points were published.[61] The purpose of this doctrine was to provide integrated guidance to the US Armed Forces on how to carry out offensive and defensive battle operations in cyberspace.[62] The high level of maturity in developing weapons, training personnel, and formulating a special theory of warfare for cyberspace that the American defense establishment had reached since the creation of Cybercom was exposed in 2012 by President Obama in Presidential Policy Directive 20, which deals with offensive activity in the cyber realm, including "active defense."[63] This document, which is classified as "secret," was published in the British newspaper the *Guardian* as part of the documents exposed and leaked by

60 Tania Branigan, "Chinese Army to Target Cyber War Threat," *Guardian*, July 22, 2010.

61 US Office of the Joint Chiefs of Staff, "Joint Publication 3-13 Information Operation," (2012).

62 US Office of the Joint Chiefs of Staff, "Compendium of Key Joint Doctrine Publications," (2014).

63 The White House, "Presidential Policy Directive 20: US Cyber Operations Policy," (2012).

Edward Snowden.[64] It constitutes substantial evidence of the institutional change that the American defense establishment underwent in its attitude towards computer-mediated communications prior to regarding it as a theater of activity. The presidential directive includes detailed definitions of types of attacks and defensive measures in the cyber realm, including passive network defense, offensive cyber activity, cyber campaigns, intelligence gathering from within or using cyberspace, cyber warfare for defense purposes, non-invasive defensive operations, and so forth.[65] The directive refers to the fact that the United States already had proven offensive capabilities, which it uses to exercise its right to self-defense, following a scrupulous process of authorization.[66]

Another conceptual and organizational change that began during this period, in addition to the concept of cyberspace as comparable to a physical space, was the treatment of cyberspace as an important social and public theater that has both negative and positive potential and requires monitoring and protection. The classification of cyberspace as an infrastructure in its own right—not merely as a space that mediates between interests in physical space—was added in 2010 as part of a policy of the Department of Homeland Security, entitled, "Securing the Nation's Critical Cyber Infrastructure." This plan referred to cyberspace as a social, political, and economic theater, which included countries, criminal elements, terrorist organizations, and individuals.[67]

The defense involvement in social interaction in cyberspace also influenced the revision of the US Armed Forces' doctrine of implementation of information operations. A doctrinal document from 2012 stated that cyberspace was essential for the existence of information operations as part of an ongoing military effort,[68] and that it was one of the channels for influencing the "information environment," because it could be used to both disrupt or prevent

64 Edward Snowden was a former employee of the CIA and NSA who specialized in online intelligence. In 2012, Snowden leaked a large number of documents to leading global media. The documents exposed the depth of intelligence gathering and active operations by the United States and its allies (the joint intelligence community of the United Kingdom Canada, New Zealand, and Australia) in cyberspace.

65 "Presidential Policy Directive 20: US Cyber Operations Policy," pp. 2–4.

66 Ibid., pp. 4–11.

67 US Department of Homeland Security, "Securing the Nation's Critical Cyber Infrastructure," (2010), pp. 7–10.

68 US Office of the Joint Chiefs of Staff, "Joint Publication 3–13: Information Operations," (2012), p. III.

messages and to disseminate messages and carry out deception through use of the social media.[69] The treatment of cyberspace in official presentations by the spatial commands of the US Armed Forces, where it was portrayed as a basic part of the operational concept, made it clear that cyberspace had become one of the areas of action of the US military.[70]

In addition, from an organizational standpoint, the United States recognizes that the ability to operate in public-civilian cyberspace is not an exclusive one; therefore, it must cooperate with sub-state and supra-state players, particularly local and international consultancy and software companies that constitute a partner and source of information for improving security in cyberspace, as evident from the recommendations of various official committees and reports.[71] For example, these recommendations indicate that despite the organizational changes that have led to the training of specialist military and government cyber personnel, areas in which external non-military parties have an advantage still exist and that the United States is unable to close this gap in the near future and must therefore rely on the relative advantage of these external parties. This is especially true of areas such as forensic identification, for which there is still no solution at the state level.[72]

Force Building in the Cyber Domain as an Expression of Organizational Conceptual Change

In February 2016, President Obama published an "Op-Ed" in the *Wall Street Journal*, in which he argued that the United States should allocate more money to the development of technologies for cyber defense, with an emphasis on protecting government information systems infrastructure.[73] The publication of the article slightly predated the US administration's

69 Ibid., p. II–9.

70 See, for example, "The Operational Art of Fighting in and Through Cyberspace (Unclassified PP presentation)," slide 12, a non-classified conceptual presentation prepared for General Moulton, head of planning and operations in the European Command of the US Armed Forces, given to a college of Army officers.

71 Center for Strategic and International Studies, "CSIS Commission on Cybersecurity for the 44th Presidency: Human Capital Crisis in Cybersecurity," (2010), p. VIII.

72 For example, virus activity was exposed by commercial companies specializing in the field, such as Kaspersky Lab and others.

73 Barak Obama, "Protecting US Innovation from Cyberthreat," *Wall Street Journal*, February 9, 2016, http://www.wsj.com/articles/protecting-u-s-innovation-from-cyberthreats-1455012003.

decision to increase spending by $19 billion on the development of these technologies.[74] President Obama's article represents the prevailing approach especially among decision makers in the United States and most likely in other countries; it relies on the assumption that the panacea for the growing difficulty of securing cyberspace and protecting critical national infrastructure and resources is to increase technological development and invest resources in it. Although Obama states in his article that senior defense establishment officials and military officers would apply the spatial organizational approach, it appears that this currently has not prevailed among US decision makers.

As noted above, studies in defense and international relations in recent years have dealt at length with the development of warfare in cyberspace, and the desirable state strategy.[75] It should therefore be asked: What is the significance of focusing on organizational and conceptual change instead of technological development? Specifically, what is the optimal way of organization in order to achieve a security advantage in cyberspace? What contribution does describing this process have on understanding and improving a country's capability in providing security for its citizens against cyber threats?

In the following discussion, the article presents an alternative to the latter, stressing the benefits of investing in organizational development and highlights the possible different consequences of the two choices. Although it is not based on a comparative research, this discussion has value for understanding the different level of dominance in the cyber domain achieved by other countries that decided to prioritize organizational and conceptual development over technological development. At the onset of the article, it was noted that the current focus should be on re-organizing the forces to provide security in cyberspace as did the American military., which regards cyberspace as a battlefield comparable to physical battlefields. I believe that the need for this focus lies in two complementary factors: 1) the growing threats posed by cyberspace and the changes that have occurred to those

74 Tobias Naegele, "7 Keys to President Obama's 19 Billion Cybersecurity Plan," *GOVTECH Works*, February 16, 2016, https://www.govtechworks.com/7-keys-to-obama-19-billion-cybersecurity-plan/#gs.iMSThHM.

75 See, for example, the discussion of the ability to defend against cyberattacks utilizing the Internet of Things (IoT) in Bruce Schneier, "Security and the Internet of Things," *Schneier on Security, February 1, 2017,* https://www.schneier.com/blog/archives/2017/02/security_and_th.html, and the discussion of deterrent capability in cyberspace in Nye, "Deterrence and Dissuasion in Cyberspace," pp. 44–71.

threats; and 2) the unique technological characteristics of the weapons in cyberspace.

In regard to the first factor of the change in the threat, the examples from the three periods described above highlight the organizational shifts that have occurred in the US defense establishment due to the growing comprehension of the depth and substance of the threat in cyberspace to the security policies in general and to the ability to use military force in particular. The source of the change lies in the transition of cyberspace as a system for transmitting information to an important omnipresent element in modern life. Cyber began as a threat posed by other countries or individuals to sensitive and covert state information—such as official state information, intelligence, and technological knowledge, all defined as part of the "information security"—to threatening the basic infrastructure and fundamental resources of a modern country that relies on computerized information, and can be defined as part of the defense of strategic infrastructure and sites (civil defense); finally, it has become a spatial threat (cyberspace), which interacts with and affects a large proportion of civilian and military operations in physical spaces. The latter can be described as a threat to a country's sovereignty and to interpersonal interactions—economic, political, and social—that is, a threat to the public security. The diverse human use of cyberspace means that it is no longer possible to focus on defense of state infrastructure solely by means of technological development (as indicated by President Obama's statement).

The second factor that contributed to the uniqueness of weapons in cyberspace, results from their rapid technological development and their growing availability in the private market, as evident from the daily need to update hardware and software at a quick pace in the home computer system. The development of computerized espionage and surveillance tools, easily obtainable in the private sector and simple to use,[76] has prevented countries from achieving a technological advantage through the national development of new weapons. A state cannot cope with the rate of development and the relatively low prices of similar weapons in the private market; therefore, development alone cannot be the only or even the principal means of achieving an advantage in the cyber domain. This unique characteristic leads to the conclusion that the ability to control and defend cyberspace cannot be based

76 The US administration has already recognized this problem. See, for example, "Securing the Nation's Critical Cyber Infrastructure," (2008). p. 3, Figure 1.

solely on technological development but must also include organization of force and the evolution of a doctrine that employs force in a way in which it will be well integrated with a country's other military actions. This approach is similar to the organization of force for creating security in physical space, such as organizing an air force to protect the national air space and to assist ground and maritime efforts. Comparing between the virtual space and the physical space—between a field perceived as new and revolutionary and the "old and conservative" mode of action—is part of the necessary solution.

The historical review presented above shows that the spatial organizational approach is the one being applied by the American security bureaucracy, especially the military. Its clearest practical expression is the formation of a designated, extensive, and solid security establishment in cyberspace, which includes a number of special personnel operating hierarchically from the level of a consultant office in the president's staff to military units and the United States Computer Emergency Readiness Team (US-CERT). Operations are also coordinated with policing units and divisions in the Department of Homeland Security, and with semi-governmental bodies that mediate between the public and private sectors.[77] This characteristic has also led to a change in the use of force in cyberspace: from targeting sensitive information and national infrastructures to effecting the adversary's internal legitimacy.

It is possible that the spatial organizational change is also one of the reasons for the hierarchy in the power relations between the various countries operating in cyberspace. This change is one of the special characteristics of great international powers (GPs) like the United States, which is the leading international security force in cyberspace, capable of allocating resources for organizing military action based on a spatial-like principle. This kind of change is expensive, requiring personnel, expertise, and organizational capabilities that are unique to states that are accustomed to large-scale security spending. In other words, asymmetric operations in cyberspace, such as terrorism, sabotage, theft of information, psychological warfare, and fake news-type communications can be executed by weak states and even non-state organizations. The ability to organize operations in cyberspace as regular military missions based on the spatial organizational approach is

77 (NCSC) National Computer Security Center; (NIAC) National Infrastructure Advisory Council including the business sector and higher education; (ISAC) Information Sharing and Analysis Center.

confined to global and regional powers and a few other countries possessing technologically advanced modern armies.

The question of whether we are witnessing an organizational competition between the Western style of organization of force in the cyber domain by forming official state military and security institutions—in which the United States is the leader—and the hybrid organizational concept of carrying out offensive cyber action using an "Ecosystem" that synchronizes state security institutions, universities, the private sector and/or criminal elements—led by countries like China and Russia—requires additional research that could be an important future contribution.

Given the changes in the organization of the cyber capabilities as part of military force, one could ask the question arises of whether it can be assessed using the same tools through which we measure force building in the physical space and whether we can compare the two. The answer is not unequivocal. On the one hand, from the perspective of cost-benefit calculations, it is clearly impossible to compare the cost of a new aerial platform, either monetarily or in terms of development resources and professional investment, and the development of operational cyber tools. On the other hand, in both cases, force building involves the need to develop the capacity of using the weapons in combination with existing weapons that are designed for warfare in a different space by means of procedures, doctrine, and technological tools that enable better command and control. Historical comparisons can also be made between the development of aerial and naval military combat systems, and the development of cyber combat systems as a result of technological advancements.[78] Such a comparison emphasizes the importance of both the organization of force around a spatial concept in the cyber domain as a way of achieving a national security.

Summary and Conclusion

The organizational change in the United States due to the emergence of the concept of "cyberspace" has led to transformations in three areas: in the

78 This question has begun to attract the attention of researchers in recent years. See, for example, Amit Shiniak, "The State Plan in the Online Border Zone: A Theoretical and Historical Comparison," *Bein Ha-qtavim*, (Dado Center for Interdisciplinary Military Studies), no. 3 (2014): 13–44 (in Hebrew); Florian Egloff, "Cybersecurity and the Age of Privateering: A Historical Analogy," Cyber Studies Programme, Working Paper Series No. 1, University of Oxford, March 2015.

range of cyber operations; in the characteristics of these operations; and in the conception of activity in cyberspace and its consequences for the United States' national security approach and its overall strategy. The development of the range of US security operations in cyberspace, which initially were limited, restricted, and aimed mainly at securing and protecting the national cyberspace (institutions and interests) and have culminated with US forces prepared to conduct offensive, defensive, and intelligence cyber operation, resulted mainly from an organizational change. This has led to the creation of units, agencies, and organizations with defined responsibilities and a national mechanism for coordinating the activity in cyberspace.

Despite this development, organizational change has not been sufficiently recognized in research nor professional frameworks, and important budget decisions, such as the one by the Obama administration, reflect the belief that investment in technological development alone will lead to a better security of the cyberspace. This approach contradicts the substantial development in the force organization in cyberspace, as described in this article, and jeopardizes its continuation. It is also the result of a bureaucratic attitude that tends to assess policy through quantitative (cost-benefit) measures, while ignoring qualitative aspects, such as conceptualization, organization, and doctrine creation, which are some of the qualitative elements that give an advantage to companies using weapons in every space, including cyberspace.

The final conclusion of this article is that in the framework of planning today's security strategy, it is worthwhile also to address the differences between states in their ability to organize defense operations in cyberspace, with an emphasis on regional powers and the world's leading military forces. The process of organizing and consolidating the spatial operating concept that characterizes current US military policy is part of the creation and consolidation of behavioral norms. These organizational norms are the subject of the current international discourse on cyberspace and are worthy of study and research and of becoming part of the assessment mechanism in the development of capabilities in this sphere. This article recommends an organizational approach based, to some extent, on equivalence between states conduct in cyberspace and in physical spaces, in order to make it possible to develop multi-dimensional control capabilities for managing an "integrated," synchronized physical and technological operations that might lead eventually to a national dominance in cyberspace.