Cyberspace and the Israel Defense Forces

Gadi Eizenkot

Over the past decade, the Israel Defense Forces (IDF) has made the greatest strides in the field of cyberspace. During this period, cyberspace became a pertinent issue and in the IDF it became an extensive field of activity of developing and applying knowledge. The IDF perceives cyberspace and cyber regulation as significant for several reasons: First, they relate to the public discourse on knowledge development and the regulation of relations between the state and the economic system on the issue of national cyberspace and its resilience and the strengthening of the state's ability to continuing functioning in any emergency and while under enemy attack; second, cyberspace has great importance also in the international context. The State of Israel sees itself as being at the global forefront in developing cyber knowledge and, as such, can meaningfully contribute to developing the defense of cyberspace in other nations as well.

The IDF deals intensively with cyberspace and allocates significant resources for that purpose. Work in this field consists of three main components: first and foremost is defending military cyberspace and helping to secure civilian cyberspace. The IDF invests vast resources in fortifying cyberspace security. The second component concerns the army's ability to gather intelligence in cyberspace. As a result of technological development, increasing amounts

Lt. Gen. Gadi Eizenkot is the chief of the General Staff of the Israel Defense Forces. This essay is based on Lt. Gen. Eizenkot's lecture on cyberspace in the IDF given on October 24, 2018 at the conference jointly sponsored by INSS and the Academic Center for Law and Science in Hod Hasharon to honor the launch of *Cyber Regulation*, written by Dr. Col. (res.) Gabi Siboni and Ido Sivan-Sevilla.

of critical intelligence information is digitalized. Consequently, many more attempts at technological intelligence gathering efforts take place in cyberspace. The third component is cyberattacks—that is, the ability to make real operational gains via activity in cyberspace. The IDF integrates all these activities in its extensive operations.

Cyberspace as Part of the Threat Circle

The IDF is a very technological army, certainly when compared to some of Israel's enemies, and defense is viewed as critical to its functional capability. Since the establishment of the state, the IDF has faced three central threat circles, to which a fourth has been added in recent years. The first is the conventional threat from states with militaries of varying capabilities, including armored corps, infantry, and artillery, all capable of ground maneuvers, and supported by aerial offensive forces, aerial defense forces to disrupt IDF activity, and even maritime forces. All of these were constructed primarily for offensive goals in order to seize parts of the State of Israel.

The second longstanding threat circle against Israel is the nonconventional threat, which consists primarily of attempts by various regional parties to develop offensive military nuclear capabilities. This is evidenced by the Iranian vision of developing nuclear arms and by the Syrian efforts, foiled in 2007, to do so. Other such attempts may come to light in the future. In addition to nuclear weapons, some of the nations surrounding Israel have the capacity to engage in chemical warfare. Syria, for example, clearly possessed that capacity and, although it was significantly reduced five years ago, chemical warfare has been used several times during the Syrian civil war.

The third threat circle that has greatly preoccupied the IDF in the last decade and will continue to do so in the foreseeable future is the sub-conventional threat posed by terrorist and guerilla organizations operating against Israel. This threat consists, inter alia, of high trajectory fire on a large scale, having greater impact and accuracy than ever before, and the development of subterranean capabilities, both for defensive purposes for survival and offensive ones for penetrating into Israel in order to carry out terrorist attacks against Israeli settlements. In addition, the IDF and the other security organizations face threats by jihadist organizations and the attacks by individuals. The terrorist threat exists in Israel's north, south, and in Judea and Samaria, as well as toward Israeli and Jewish targets abroad.

The fourth threat circle is the cyber one. Aimed primarily at Israel's functional capabilities, both military and civilian, this is a relatively recent threat, which has expanded exponentially over the last decade and is expected to grow significantly in the coming years. Over the years, the IDF focused on developing warfare capabilities in three dimensions—land, sea, and air. In recent years, it has also started to develop warfare capabilities in the fourth dimension—cyberspace—with the understanding that this dimension needs to be addressed broadly and comprehensively, with preparations made at both the national and security levels. In its process of developing its knowledge, the IDF examines how to secure military cyberspace as well as state cyberspace, in the understanding that the IDF is charged with the responsibility of protecting security infrastructures, critical installations, economic capabilities, hospitals, airports, the banking sector, and so on, while at the same time protecting its military capabilities so as to allow the army optimal functioning in operating its command-and-control systems. These capabilities obviously depend on the most advanced means, including weapons and intelligence systems and aerial and naval capabilities.

The IDF in Cyberspace

The IDF's intensive work in cyberspace began about a decade ago. In recent years, the army has conducted a thorough study of the most suitable approach to developing and organizing this field. The IDF is not the only military doing so. Other nations, too, are examining the issue; the US military held comprehensive inquiry of the cyberspace question, which subsequently led the United States and Israel to share knowledge about the optimal way to organize military activity in cyberspace. The discussion hinged primarily on the best way to organize the defensive/security capability, the intelligence gathering capability, and the attack/offensive capability.

The IDF's learning process began about four years ago, with the learning and work of the general staff continuing for about a year. The question raised was how to properly organize. Several options were examined. Some required quite a leap, such as organizing all the military's cyberspace capabilities under one command; other were more conservative. Given that the IDF continuously and intensively deals with a broad spectrum of threats, it was finally understood that it would be improper to engage in a move that would be considered a step forward, with much trial and error in

a truly critical sphere of operations, especially since the security situation could quickly escalate. Given this, it was decided to progress gradually, using a measured approach to cyber organization in the IDF. As a result, the Computer Service Directorate's authority was expanded and its name changed to the CC4I Directorate. The Cyber Defense Division, whose personnel have a background in offense, was formed within this framework. At the same time, it was decided to reorganize the Military Intelligence Directorate, while unifying its intelligence gathering capability with other capabilities, with the understanding that the infrastructure of Unit 8200 and other infrastructures required in cyberspace must operate in an integrative manner. We expect that the progress and experience in this will lead ultimately to defensive, intelligence gathering, and offensive capabilities all united under one command.

In the United States, too, the relevant authorities are deliberating on the right way to be prepared in cyberspace and are considering splitting USCYBERCOM and the National Security Agency (NSA). As noted, the shared dilemmas have led to sharing information between the IDF and various US cyberspace entities, and we can assume that the process will continue for many years during which the current split model of handling different cyberspace fields will still be in effect. Nonetheless, at a certain point down the road, conditions and capabilities will reach the point where it will be possible to unite the entire cyberspace sphere under one command. It can be assumed then too that the move will be done in a measured, deliberate way.

The IDF has made a significant change in selecting and training personnel, and in its digital infrastructures, force building, and software houses. The changes in these fields and the enhancement of the Computer and IT Directorate have generated real reforms and upgraded the IDF's defensive capabilities in the cybersphere. In this context, the enhancement of the IDF's telecommunications abilities as part of the Digital Ground Army project is remarkable; more than 10 billion NIS were invested in order to provide the IDF's ground forces with better functionality and optimization in concentrating information about the enemy, the IDF, and the combined use of IDF force. The reorganization carried out in the Military Intelligence Directorate led to a fundamental change within its systems aimed at optimization and reducing duplications. Significant changes and enhancements were also made to

inter-organizational integration and cooperation among the IDF, the General Security Service, and the Mossad, as well as to capabilities at the state level.

The IDF holds quite a few joint drills and training exercises within its own framework as well as with other organizations—including foreign militaries—to learn and share cyber information, having understood that this developing challenge requires the sharing and exchange of information. The IDF also actively participates in drills and capacity building in order to secure the state in emergencies conducted in close cooperation with the National Cyber Directorate. This aspect of the IDF's work stems from the fact that it views itself as an inseparable part of defending and protecting the national cyberspace in emergencies and wartime. To do this, it is necessary to continue developing knowledge and a common language among all the branches of the State of Israel, in addition to and beyond the great progress made in the field to date. The unknowns in this field still outnumber the knowns, and that is the way it ought to be.

Conclusion

The IDF has made tremendous strides in its Digital Ground Army plan, allowing modern commanders at all ranks to get more information and generate more up-to-date assessments of the enemy's location and the IDF's own forces in the field. This progress, however, is liable to cause an overload of information for the field ranks, which could cause greater harm than good. It should be remembered that too much information is not a guarantee for better command and control. The IDF has analyzed all of this, and it is important to be cognizant of this: "[If] in the past the tactical commander fought to get data about the location of his troop and the location of the enemy so that he could make decisions, today these data—as well as many other data—are presented to him. As a result, he now faces a new challenge: to sort the chaff from the wheat and find the relevant details of the information that will allow him to make better decisions and obtain a decisive victory in the fighting."[1]

Progress and transparency of information have other psychological implications on the way that commanders share information. As Clausewitz

1 Gabi Siboni and Moran Mayorchik, "The Curse of Abundance," *Ma'arakhot* 459 (February 2015): 19 [in Hebrew].

said, war is the realm of uncertainty and thus it will ever remain.[2] It is therefore important that transparency of information not confuse the various ranks during the decision-making process and that the ranks of command be maintained. The fact that the entire chain of command—the company commander, the battalion commander, the brigade commander, and the division commander—sees all the information at the same time should not cause a Tower of Babel situation; the advanced command-and-control systems, which enable everyone to see the same information, must not be allowed to lead to a situation in which a division commander or head of a command act as if they are at the level of company commander and think they understand the situation better and can therefore make better decisions than those who are actually in the field.

The IDF will continue to develop in cyberspace, build capabilities, organize the commands, and develop new technological tools. But in tandem with technological progress, which is a force multiplier for the IDF compared to its enemies, it is extremely important always to retain the fundamental principles and approaches of the command. These, based on thousands of years of human experience, are not merely conservative tenets; on the contrary, they do a better job of arranging the way in which the art of war is manifested on the battleground, the way decisions are made, and the processes of their implementation.

Military activity will continue to require difficult and demanding physical efforts. The days of sterile fighting with buttons alone still lies far ahead in the future if it should ever come. Therefore, even though the IDF is making tremendous efforts in developing its cyber capabilities, the need to maintain and develop its kinetic abilities has not changed, because the wars of the future will continue to be decided on the physical battlefield.

2 Roger Ashley Leonard, ed., *A Short Guide to Clausewitz on War* (Tel Aviv: Ministry of Defense, 1977), p. 79 [in Hebrew].