INSS Insight No. 719, July 8, 2015

Establishing an IDF Cyber Command

Meir Elran and Gabi Siboni

On June 15, 2015, the IDF Spokesperson announced that in light of the substantial challenges facing the IDF in the cyber realm, the Chief of Staff decided to establish a cyber command to lead the operational activities in this emerging field. The cyber command will be established within two years, in the first stage both within the Military Intelligence Directorate (DMI) and the C4I Telecommunications Directorate of the IDF. The decision to establish a cyber command was taken following the recommendation of a multi-branch team appointed by the Chief of Staff when he assumed office, led by the head of DMI, to examine ways to enhance the military operational effectiveness in the cyber realm. According to the Chief of Staff, "establishing this arm will enable the IDF to perform better on the [cyber] fronts…and will utilize the technological and human advantages already existing in Israel."

The new reorganization should come as no surprise. It reflects an increasing understanding within the IDF of the growing centrality of cyber activity as a major component of military operations on both offensive and defensive levels, and awareness that the updated integration of this realm within the General Staff and subordinate levels is long overdue. Until now, the defensive cyber missions were under the responsibility of the C4I Directorate, with the intelligence collection and offensive missions under DMI's 8200 signal intelligence unit. However, this organizational split has come to be seen as inadequate for the dynamic operational needs of the force in a rapidly changing environment, particularly since the field demands long range planning and synchronic execution with exceptionally high levels of precision, speed, and imagination.

This is the backdrop to the call for the creation of a new command within the IDF, which will provide an adequate setting for a tightly knit, integrative, and robust cyber system, be able to compete for the necessary resources within and outside the military, and ensure the system's long term development, in accordance with the needs and technological opportunities of the cyber world.

The IDF is currently facing a number of challenges as to the cyber-related reorganization, and will need to choose between several options:

a. It has already been decided that the IDF cyber command will be directly subordinate to the Chief of Staff; this arm will be the fifth such branch within the General Staff. Among the four existing branches, the air force, navy, and intelligence are responsible for both the buildup and operational deployment of their respective forces, while the ground forces command is responsible solely for the buildup of its force, with the operational deployment carried out by the territorial commands. The cyber command will apparently be charged with both the buildup and the operational missions of the force.
b. One of the most significant questions relates to the future role of DMI. In recent years, DMI has been engaged with cyber collection and offensive missions, while keeping its supreme national responsibility for traditional intelligence missions: collection, evaluation and analysis, and strategic and operational intelligence activities. Some might suggest that the addition of the cyber field to DMI's responsibility is too much of a burden, hampering its capacity to fulfill its traditional – and already widespread – missions. At the same time, the organizational split between the offensive and defensive theaters of the cyber operations has not contributed to overall operational effectiveness.
c. The establishment of the cyber command will require the strengthened and institutionalized synergy between DMI's intelligence gathering and offensive setup on the one hand, and the new command on the other. Such robust links already exist in the relationship between the various cyber units. However, experience indicates that there is room for improving the interconnectedness between the different functions. The decision to integrate the system on the one hand, while keeping the actual functions of the offensive and defensive missions organizationally separated, will represent a severe challenge for the future design, which will need to find ways to maximize the connectivity of the force.
d. Assigning the overall responsibility for the cyber realm to the new command will require strict organizational and professional restructuring, which would best utilize the assets of DMI as an "operational contractor." This has long been a routine mode of operation regarding intelligence data gathering and dissemination for other branches (air, naval, and ground, as well as agencies outside the IDF). Reciprocal data sharing is also common – and highly successful – among intelligence gathering contractors and platforms, such as those operated by the air force or navy. Similar circular working relations, adapted to the specific needs of the cyber world, can likewise be constructed with the new command.
e. Hence, a major imperative in coherently implementing the decision to set up a cyber command within the IDF will be the attainment of maximal operational cooperation between the new command and other IDF forces and units. This imperative may seem trivial, but its realization in practice, under the circumstances of operating an emerging, relatively new system that is less

familiar to many of the IDF units, will require special, long range professional efforts and resources.

f. It is important to consider the new command's position in the organizational structure, not only on the strategic General Staff level, but also on the operational and tactical levels. The IDF's cyber command will ultimately be widely engaged in offensive and defensive operations, in close association with the field units, primarily countering enemy command and control systems and other operational components heavily based on information technologies.

g. The IDF is not alone in the cyber arena. A large number of important, relevant civilian agencies, such as the National Cyber Bureau and the Cyber Authority, as well as security agencies such as the GSS and the Mossad are also active in the field. All are committed to maintaining direct and effective organizational and operational links with the IDF, which for its part must build its capability vis-à-vis and in cooperation with them. Past experience indicates that this will be a highly challenging task.

Future decisions with regard to the reorganization of cyber activity and construction of the new command must contribute directly to the overall capacities of the IDF cyber potential. This will not be an easy undertaking. A particularly important challenge will be the attainment of the adequate combination of long range planning and precise execution capabilities on the different levels, together with an optimal degree of operational flexibility in the defensive and offensive theater, in order to maximize the high potential of the cyber realm. An improved, innovative cyber system will serve to expand Israel's spectrum of security capabilities, as long as it is based on and integrated with an updated general security doctrine that is responsive to Israel's rapidly changing needs.