iNSS The Institute for National Security Studies
Strategic, Innovative, Policy-Oriented Research

INSS Insight No. 856, September 21, 2016

Structuring Israel's Cyber Defense

Shmuel Even, David Siman-Tov, and Gabi Siboni

April 2016 marked the official beginning of the National Cyber Defense Authority ("the Authority"). Its primary function is "to direct, operate, and execute as needed all defensive and operational efforts at the national level in cyberspace, based on a systemic approach, to allow a full and constant defensive response to cyberattacks, including the handling of cyberspace threats and cyber events in real time, formulation of a current situation assessment, gathering and research of intelligence, and work with the special institutions" (Government Decision No. 2444 of February 15, 2015). The director of the Authority is subordinate to the head of the National Cyber Staff, who is defined as the head of the national cyberspace operation.

The guiding rationale that informed the establishment of the Authority is that close cooperation among all parts of the civil sector is required to defend cyberspace, and hence the need to establish a civilian authority to focus solely on cyber security and, in the future, assume some of the work traditionally performed by the Israel Security Agency (ISA) to defend critical national infrastructures. Disagreements and tensions as to the division of responsibility among the various bodies accompanied the establishment of the Authority. On June 9, 2016, a memorandum of understanding between the Authority and the ISA was drafted in order to regulate activity, but the tension is inherent and will most likely persist in the future.

In tandem, the IDF has undergone conceptual and organizational changes. In June 2015, Chief of Staff Lt. Gen. Gadi Eisenkot decided to establish an independent cyber branch that would lead the IDF's defensive and offensive activity in cyberspace. As a preliminary stage, a Cyber Staff was established as part of the General Staff, a defensive brigade was set up in the Telecommunications Division, and organizational changes were made in the Intelligence Corps.

In August 2016, the Knesset Foreign Affairs and Defense Committee issued a report on "Division of Responsibility and Authority for Cyber Defense in Israel." The report represented the work of a subcommittee on cyberspace defense headed by MK Avi Dichter, former head of the ISA. The committee's objective was to "learn and supervise the state's preparations for cyberspace defense, and examine the significance of the government's decision to establish the Authority and its implementation." The report, which was distributed publicly, invites public scrutiny and debate.

According the committee report, "The working procedures, as presented to the committee, in practice render the subordination of the head of the Authority to the head of the national cyberspace operation redundant, because the head of the Authority is independent, working at the core of his professional commitment – cyberspace defense – and is not required to wait for authorization from the head of the department to make decisions and take action in the field." Furthermore, "the committee was not convinced of the need for two independent authoritative bodies in the Prime Minister's Office, both dealing with cyberspace." In other words, the committee felt it was necessary to examine the appropriate organizational placement of the National Cyber Staff, and marked this goal for further investigation.

Among the other conclusions reached by the committee:

- The Cyber Defense Authority should not be made into yet another intelligence gathering agency. It must base its work on information gathered by parties in the intelligence community and open data.
- The committee determined that the cyber law must be written with the cooperation and involvement of all relevant parties in the defense and civilian systems. The limits imposed on the ISA in terms of individual rights must likewise be imposed on the Authority.
- Given that the police capabilities in cyberspace are lacking, due to legislative limits and a lack of resources, the discussion of this issue should be expanded.
- In war time, it is important to confer responsibility for integrating and managing the cyberspace efforts on the entity at the forefront of the battle (the IDF or the ISA, depending on the nature of the conflict), while the Authority's defense forum would continue to operate and enable it to affect, directly and through its representation, the range of war efforts led by the IDF.
- The cyberspace arrangement should be reexamined periodically over the next five years, given the potency of the threat and the relatively little experience Israel has had in tackling it.

Implications and Recommendations

Fundamental concepts must be clarified, among them: "cyber," "cyber security," and "cyber defense." "Cyber" is a general term used for a large range of activities, phenomena, and outputs that create computerized and mechanized systems, social networks, communications, and others. Therefore, cyber companies include all telephony and computerization companies, internet providers, communications satellites, and companies whose business is cyber security and defense. "Cyber security" is a more limited field, though still sufficiently large, dealing with the stability and regular management of the national cyberspace, such as Israel's dependence on communications satellites, cellular companies, and so on. "Cyber defense" is one aspect of cyber security, and the sole responsibility of the Authority (except for defense of security institutions, institutions receiving instruction for the chief of security in the defense establishment, and other institutions that were excluded from the Authority's purview). Therefore, Israel needs a national cyber strategy in all aspects, including so as to improve cyber security and cyber defense. Formulating a national cyber strategy and a cyber security strategy should be the responsibility of the National Cyber Staff, whereupon it should be approved by the government cabinet and its main points disseminated to the public at large.

The term "cyber incident," which *is* mentioned in the February 2015 government decision, can be defined as an event that carries risk or causes damage in cyberspace for any reason whatsoever – a malfunction, fire, natural disaster, criminal act, or kinetic damage – rather than just the result of a logic-based cyberattack by an enemy. The possibilities are not clearly described either in the government decision or in the committee's report. If this definition of the concept is accepted, the new Authority would have to provide responses to all these eventualities and types of events.

Given the establishment of the Authority, the National Cyber Staff's center of gravity should gradually be shifted to issues related to the field of national cyberspace in general (developing the industry, encouraging R&D, building up human capital, expanding education and governance via cyber efforts, and so on) and specifically to issues related to national cyber security, such as the construction, stability, and survivability of the national cyberspace during routine times and in emergencies in those areas that lie outside the Authority's purview, areas that must be very clearly defined. After the Authority is well embedded in the Prime Minister's Office, its transfer to a more appropriate government ministry should be considered.

As for organizational changes, it is necessary to define the interfaces and the separate realms of responsibility and authority belonging to the Authority, the IDF, and the intelligence community. *T*he Authority*, for example,* is asked to analyze and research intelligence and gather it from sources in Israel's civilian system and elsewhere (information from the field, civilian companies, and colleagues abroad). *This* raises the question of how a unified intelligence assessment would be made in Israel if signs of an attack came to the knowledge of the Authority, which does not investigate most aspects of the enemy, while the information and knowledge explaining the signs of the attack (who is the attacker and what are its goals, and so on) came to the intelligence community. Therefore, the division of responsibility and cooperation among all bodies involved in cyber warfare in the contexts of intelligence, defense, offense, and integrated campaign management should be defined from a systemic point of view. For example, it is necessary to define who provides the intelligence assessment and early warnings, and who commands the cyber systems.

The IDF's function in defending cyberspace in emergencies and in wartime should be regulated, and the interfaces between the army and the Authority, and between the secret services and the police should be defined. Initial regulation has already been started, but has a long way to go. The committee's proposal that the IDF be responsible for leading the state's cyber defense in wartime is at odds with current reality, chiefly because anyone who is not deeply involved and working in the state-wide cyber realm on a day-to-day basis during routine times will be hard pressed to take effective responsibility for the task once the state transitions into emergency mode.

Finally, organizational changes, no matter how complex, are not necessarily evidence of capabilities or enhanced ability to defend cyberspace. Therefore, criteria and practical tests as to the *strength* of the cyber defense system should be instituted, to make it possible to assess the present situation and the added value of future action in the field.