BESA PERSPECTIVES
THE BEGIN-SADAT CENTER FOR STRATEGIC STUDIES

Cyberspace, the Final Frontier

by Maj. Gen. (res.) Yaakov Amidror

BESA Center Perspectives Paper No. 360, August 30, 2016

EXECUTIVE SUMMARY: Israel's young cyber industry is proving to be a remarkable success story. Between the National Cyber Bureau and the budding Cyber Defense Agency, Israel can protect its critical infrastructure and continue cementing its position as a global cybersecurity powerhouse.

Sometimes dramatic advances are made in important fields far from the public eye, overshadowed by senseless media uproars over insignificant things. One of these leaps was made a month ago when Israel's cybersecurity legislation entered a new phase. After prolonged discussions, the Knesset voted in favor of a temporary provision laying the groundwork for Israel's civilian cyber defenses.

In 2012, following the recommendations of a committee headed by Maj. Gen. (res.) Isaac Ben-Israel, the National Cyber Bureau (NCB) was established at the Prime Minister's Office. The NCB has come a long way since then, and its framework of principles allows Israel to better protect its civilian cyber infrastructures.

This was a case in which the quality of the human capital involved in the government's efforts would have significant impact on the fate of the initiative. A high bar was set for those involved with the NCB. They would have to be top-notch individuals, ready and willing to dedicate their time, energy and skills to a project whose objectives are sometimes ambiguous.

Israel has had several breakthroughs in civilian cyber defense knowhow and organization. People now come here from all over the world to study the field so they can construct similar infrastructures and systems in their own countries.

The captains of the NCB held firm that the pursuit of cyber excellence should be multi-pronged. This meant bolstering the academic aspect of the field, encouraging private sector investment, and building the mechanisms necessary to protect current cyber infrastructure while constantly developing it further. The object was for Israel to capitalize on its achievements in the field by bolstering cybersecurity ties worldwide and boosting both its economy and its defensive capabilities.

The southern city of Beersheba, the "capital of the south" and home to Ben-Gurion University, was selected as the focus of government efforts in cyber defense. The decision to turn Beersheba into a hub of cyber excellence coincided with the decision to relocate the military's Communications Branch and Intelligence units to the Negev.

The nationally important greater Beersheba area can no longer be considered the "periphery," and global giants have recognized this. Encouraged by significant tax breaks, they are setting up research and development centers there, either moving them from other locations in Israel or establishing new ones. If this continues, Beersheba will soon be a household name within the international cyber community – an Israeli Silicon Valley, if you will.

Israel's young cyber industry is a remarkable success story. A few years ago, 200 Israeli startup companies were known in the field, and over 100 additional companies were anonymous. Today there are too many budding cyber startups to count. The more top-notch researchers our academies produce, the more their success will encourage others to follow their dreams, resulting in more capital being earmarked for cyber initiatives.

The scope of ideas in this field is endless, and the world is thirsty for them. In this respect, the biggest challenge Israel faces is building a truly robust cyber industry, rather than serving solely as an incubator for ideas that are to be sold off early in their development. The rush to run towards an “exit” is somewhat ingrained in Israeli culture – a culture that is also responsible for the wealth of ideas.

One of the most important aspects of Israel's cyber endeavor is the outlining of measures to protect the country's critical civilian infrastructure. These efforts have been quietly pursued by the Shin Bet security agency for years, but rapid changes in this sphere now require more comprehensive efforts.

In a democracy, it is best to divide responsibility for the protection of critical infrastructure between intelligence services and other organizations, devoid of intelligence interests, that are tasked with the technical aspects of the issue. It was

therefore decided that another state body, one removed from the Israeli intelligence community and with a technological outlook on the issue, would assume the mantle.

The newly created Cyber Defense Agency will act independently. This agency will determine the priority level of the defense of different bodies based on a scale of value to the state and monitor those bodies' compliance with cyber defense measures. In addition, it will compile a database on cyberattacks inside Israel while fostering relations with other countries in order to gain access to information on cyberattacks outside of Israel.

The Cyber Defense Agency will have to cooperate closely with its existing counterparts and government ministries so it can properly prioritize the defense needs of civilian, government and private organizations. This is no easy feat, as it entails government involvement in both public companies and private enterprises.

This is why it has to be made clear that the Cyber Defense Agency's only interest is the protection of Israel's cyber infrastructure. It does not seek to interfere in anyone's business. The fact that lawmakers have been able to hammer out the appropriate legislation to facilitate the Cyber Defense Agency's operation, even if only in the form of a temporary provision for now, proves that the NCB has been pursuing the right course of action.

While there is still much work to be done on this bill, and the final legislation will probably introduce changes to the letter of the law, the temporary provision is a step in the right direction.

In any event, Israel cannot wait to complete the entire legislative process. The enemy is at the gates, and Israel must come up with countermeasures without delay. The NCB and the budding Cyber Defense Agency deserve all praise for illustrating how Israel is gearing up to counter the threats that loom in cyberspace.

Maj. Gen. (res.) Yaakov Amidror is the Anne and Greg Rosshandler Senior Fellow at the Begin-Sadat Center for Strategic Studies. He is also a distinguished fellow at JINSA's Gemunder Center for Defense and Strategy.

This is an edited version of an article that appeared in Israel Hayom on August 19, 2016.

BESA Center Perspectives Papers are published through the generosity of the Greg Rosshandler Family