Center for Cyber
& Homeland Security
THE GEORGE WASHINGTON UNIVERSITY

Trends in Technology and Digital Security

Israel: The Making of a Cyber Power Case Study

Issue Brief 5 in a Series
Based on Fall 2017 Symposium Proceedings

Featured Speaker
Dr. Eviatar Matania
Director General, Israel National Cyber Directorate
Prime Minister's Office

Panel Moderator
Frank J. Cilluffo

Panel Rapporteur
Sharon L. Cardash

This publication is the exclusive work product of the Center for Cyber & Homeland Security. It was made possible thanks to the financial support of Razor's Edge Ventures and Raytheon Company.

RAZOR'S EDGE

Raytheon

Center for Cyber
& Homeland Security

THE GEORGE WASHINGTON UNIVERSITY

Issue Brief Series on Trends in Technology and Digital Security
Israel: The Making of a Cyber Power (Case Study)

On September 14, 2017, CCHS convened a Symposium on Trends in Technology and Digital Security. Four panels addressed emerging threats and their implications for security policy, with a focus on digital infrastructure protection and anticipatory analysis. In a series of Issue Briefs, CCHS shares the findings and recommendations that emerged from the Symposium, primarily on a not-for-attribution basis. This fifth Brief in the series is a case study of the evolution of Israel as a cyber power.

The Role of Government in Technology and Innovation

Why is Israel so successful in the cyber domain? What ingredients make up that ecosystem? While it is tempting to talk about technology in reply, Dr. Eviatar Matania, the Director General of Israel National Cyber Directorate (INCD) within the Prime Minister's Office, spoke in-depth about government—specifically, how the Government of Israel approached the cyber challenge, and how it sought to mitigate the problems the country faced in this domain. What follows is a lightly adapted version of his remarks.

Before turning to cybersecurity, it is important to understand the unique role of a government in developing national capacities. While governments are often considered to be a negative factor in regards to innovation, Israel offers a few interesting examples for positive government involvement.

The first case study starts in 1992. Israel was a small economy (and still is), with a high percentage of its GDP attributable to exports/imports. At the beginning of the 1990's, Israeli imports amounted to more than 35% of the country's GDP, while exports were below 20% of GDP, which showed that Israel had a problem: the import-export gap.

During the 1950's and '60s, agriculture was the leading export branch of the Israeli economy. Step by step, the country entered into the industrial revolution and, in particular, into the hi-tech arena. At the beginning of the 1990's, everything was ready for a new economy: Israel had both experience and success with its technology-oriented defense industries. The country had very talented graduates of its military units. Many experienced engineers and managers returned to Israel from the corporate arena and the hi-tech economy of the United States. Israel also enjoyed skilled immigration from Russia, including a great deal of engineers. All of these elements were in place, but nothing happened. Yet there was a need, a real need, to have a new economy in Israel.

And then the Government stepped in with a pioneering program, called "YOZMA" (Hebrew for "Initiative"), that changed everything. It was a very small program, but with a regulator that did not think the way government regulators usually think. The question was: how to build a hi-tech economy in Israel? At the time, Israel had almost no venture capital funds (VCs) and the industry lacked reliable sources of investments. Therefore, the Government of Israel called investors to establish VCs in the country. The "YOZMA" program promised to investors to match their investments, through a very tempting mechanism: the Government would share the risk together with investors, but the upside would belong only to the investors—the Government would step out at that point.

The ten “YOZMA”-backed VCs in Israel were very small, about $20 million each. However, they were very successful and later grew into $50-100 million funds, while many other local and foreign VCs joined the community. All in all, several dozens of billions of dollars have been raised by the hi-tech sector in Israel since the introduction of “YOZMA.” Israel became what is now called “start-up nation” or “hi-tech nation.”

During the last decade, Israel exported much more than it imported, while 50% of Israel’s exports derive from the hi-tech industry. The Government of Israel knew when to enter the market, but also had the wisdom to get out—leaving the business community to do the rest.

The second successful case study was water. Israel was a thirsty country; it did not have enough water. The country needed water for drinking water, agriculture, industry, etc.; but had only very small sources of water. The first step was to build awareness through an educational campaign to "save each drop." Then, the Government decided to step in, with a program that encouraged the business community to build water desalination facilities, with a promise of 25-year contracts; and a program encouraging the use of recycled water in agriculture.

In recent years, Israel has, marvelously, become a country which has enough water; and not just for its own needs, but also for its friends and neighbors (Jordan, for example). Today, over 85% of the water in Israel is re-used—which makes Israel the leading country in the world in this regard, with a re-use percentage far higher than any other country. Over 50% of drinking water comes from desalination plants. In the past four years, Israel has suffered a severe drought; but this was hardly felt by Israeli citizens. Nevertheless, water is still a challenge, especially in regards to ecological concerns—in fact, Israel is now preparing to bring water back to the Sea of Galilee.

Building a Cyber Ecosystem in Israel

These cases were in my mind, as Director General of Israel National Cyber Directorate within the Prime Minister’s Office, when I was instructed by the Prime Minister in January 2012, to make Israel one of the leading cyber powers in the world. Israel was already in a great position, but the question was what should be the role of the Government in taking the country another step forward.

In addition to its more obvious role in building national security in and through the cyber domain, the Government of Israel also understood that Israel needed a strong and flourishing cybersecurity ecosystem in the country. To achieve this, the Government first had to consider existing strengths: in the country’s universities, there were a lot of researchers in computer sciences. Four of Israel’s faculties of computer science were included in the top-twenty leading in the world. The Hebrew University mathematics department was one of the three leading in the world. Israel was in a good position; however, there was not enough cyber research.

Next, we went to see what was happening with the industry. A lot of ideas, a lot of startups, and technology; but, industry said, we do not have enough people, we need more human capital.

At that point, the Government introduced a national program. First, as part of the strategy, Israel aimed (and continues to aim) to develop high quality human capital. Starting at the ages of 14 and 15, the state nurtures cyber skills. With the Israeli Defense Forces, which everyone goes through because of the country's compulsory service, Israel trains the best people to work in cybersecurity during their term of service; and then, to go out and be part of industry and academia. Together with its universities, Israel finds and screens the best students at the age of 15, to take them to preparatory study, to high school; and to study for the B.Sc. in computer science or technical engineering, with two more years before military service, to complete their degree and then go into the military service.

Second, the Government approached all of the country's universities, declaring the need for cyber research centers, because, if we want to be a cyber power, we need universities to step in. However, the universities demanded that the Government fully finance new cyber centers. The Government, on the other hand, was ready to match funds and be a partner: for each dollar the universities raised, the Government would match with another dollar. Eventually, most universities participated, and now Israel has six cyber research centers.

On the industry side, the Government also initiated national programs where there was a need; again, not to replace the business community, not to tell them what to do. The programs sought to do just one thing: initiate more startups, by sharing the risk in very risky research and development (R&D) projects. Together with some funds from the Minister of Economy, the Government presented some tools, where very risky R&D projects can come to the Government, and it will share 50% of the risk, for one to two years. At that point, the Government simply requires a return of the investment if that project succeeds. If you do not succeed, the Government shares the risk. That's all. And with very small funds (in government terms), some $25 million for two years, the program initiated a lot of risky projects, thus pushing the industry forward.

The current situation in the cyber arena in Israel is phenomenal: if you look at the hi-tech industry of Israel, it is the highest in the world per capita (e.g., the number of engineers and scientists—Israel is first in the world, relative to other nation-states). Israel's R&D, as a percentage of GDP, is first in the world. Largely thanks to the national programs, Israel is objectively (not just per capita) second in the world in cyber; second, of course, to the United States. The revenues of Israeli cybersecurity companies have almost doubled themselves in five years, from $2 billion in 2012 to nearly $4 billion in 2017, which is 10% of Israel's hi-tech exports. Israel has more cyber companies than the world combined, with the exception of the United States. Israel attracts almost 20% of the world's private investment. Yet Israel is just 0.01% of the world's population. While these statistics are a source of pride, Israel is doing what it does out of necessity, because of the country's security needs and economic needs. The Government tries to look for partners, adopting a humble mindset, that it is not the only entity with the "right" ideas.

Lessons Learned, Moving Forward

Looking at small- to medium-sized countries around the world, government has a role. Analyzing the success of the Government of Israel in the above cases yields four key pointers: first, the Government succeeded when there was a real need, a necessity (be it water, the economy, or cyber). Second, a national program succeeded when the Government tried to understand the whole ecosystem, and not just interfere where it should not be. Most of the time, the right thing for a government, is to understand where it does not have to be (for example, with cyber: Israel has almost no regulations). Third, the right framework: how to initiate, how to encourage the business community? Funding alone, in and of itself, will not work; the government must find the right way to harness the market through a national program. Fourth and finally, it cannot happen if there is no base: if the industry is not there, if the investors are not there, the government could not replace them. The government needs to examine what is missing, identify market failure, and explore ways to trigger the desirable actions.

To conclude, I would like to refer again to cyber. Cyber is one of the most important phenomena of this age—changing our economies, our way of life, and our national security—and it is just beginning. We are now at the point at which government may still have the possibility of shaping this new world, and harnessing cyber as a power for encouraging growth and welfare. To do so, government must act decisively, and formulate grand strategies to cope with this issue.

About Us

The Center for Cyber & Homeland Security (CCHS) at the George Washington University is a nonpartisan "think and do" tank whose mission is to carry out policy-relevant research and analysis on homeland security, counterterrorism, and cybersecurity issues.

Website http://cchs.gwu.edu **Email** cchs@email.gwu.edu **Twitter** @gwcchs