



## An overview of Israeli efforts in the cybernetics field

*Olivier Danino. Researcher for the French Institute for Strategic Analysis (IFAS)  
Member of the Circle of Middle East Researchers (CCMO)*

*March 2015, Article III.21*

For several years, the Israeli State has been trying to become a world leader in the cybernetics field. Though the Israeli strategy hasn't yet been the subject of an official policy document, on which the *Israel National Cyber Bureau* (INCB) has been working since its creation (11 July 2011), the fact remains that the Netanyahu government is taking several initiatives which clearly translate Israel's vision. The efforts are focused on youth training, the security industry of information systems, private and public research and the defensive and offensive capacities of the army <sup>1</sup>.

### 1 - Youth

Youth training is a major stake which should enable Israel to have over time a pool of people with high level technical skills in the cybernetics field. This sector is massively recruiting but is having difficulty in finding qualified personnel. The same applies to the army where the needs of some of the units are rapidly increasing. This is why the State is developing specialised programs for 15 to 18-year olds. The Israeli bachelor-level diploma is made up of a common base for all students which is complemented by options allowing for the specialisation of the diploma. The cyber options are not new. Programming, for example, has been taught for several years. On the other hand, the implementation of programs tailored to meet the recruiting needs of the army is more recent.

Thus, end of 2012 – early 2013, the Israeli government launched in collaboration with Tsahal, security services, the Tsahi Foundation, the Ministry of Education and the *Israel National Cyber Bureau*, a national program for first and second year high-school pupils named *Magshimim* <sup>2</sup> in Hebrew. This program is addressed to the people living in the periphery of the country (some coastal towns especially) and first focuses on acquiring the basics in computer science (computer languages, the operation of the Internet and networks). The students who integrate this program therefore increase their chances of serving later with a cybernetics unit in the army. The Israeli press describes it as a high-level “*cyber-warfare program*”. After the conflict which took place between Hamas and Israel during the summer of 2014, several students enrolled in this program asked to leave it in order to integrate combat units.

<sup>1</sup> For analysis of the Israeli cybernetics strategy see Olivier DANINO, *The cyber-strategy of the Israeli State*, Global Security, n°24, 2013/2, p15-24.

<sup>2</sup> For more information on this program see the site <https://www.magshimim.net/Default.aspx?KPages=492> (source in Hebrew).

This initiative is one of many. One in particular which dates back to exactly the same period. This is the program *Gvahim* <sup>3</sup>. Backed by the same institutional players as *Magshimim*, *Gvahim* is only addressed to students in the centre of the country and was implanted only in ten Israeli high schools. One year after the launching of this program, a competition sponsored by Unit 8200 was carried out in these ten schools. The target for the participants was to neutralise servers while protecting theirs from being attacked. The point of this competition was twofold: strengthen the emulation between students and make it possible for the army to identify the best students.

## 2 – The industry specialised in the system security information (SSI)

The second pillar, after youth training, is one of support to the SSI industry. The Israeli government does indeed invest large sums of money in this field as it is perceived by politicians as creating jobs and economic growth. The sums allocated by the State are mostly used by the Research & Development departments of these industries specialised in the security of the information systems. In 2013, near half a million shekels (125 million dollars) were allocated to them, in order to support their efforts in R&D. This decision is consistent with the recommendations made in 2011 by the national Board for Research & Development following the order made by Prime Minister Netanyahu in 2010 for a report on cyber-stakes in Israel <sup>4</sup>.

By supporting the SSI companies, the Israeli government is also trying to satisfy its own needs. The idea being to guarantee military, governmental institutions and the country's critical infrastructures efficient tools such as the software *Telepath* developed by Hybrid Security. It is a support which is not exclusively dedicated to the State, since it is available to all, but which is used by several national infrastructures in Israel. *Telepath* is capable of detecting suspect behaviours on the Internet and on the Intranets. More recently, in February 2015, Rafael, who notably manages the defence tools for the information system "Iron Dome", announced that it would develop its commercial offer by aiming to supply solutions for the protection of SCADA systems <sup>5</sup>. Some offers can however be more exclusive. Thus in June 2012, Elbit System implemented a simulator for the training purposes of civilian and military agencies who are responsible for the defence of the Israeli cyber-space.

Nonetheless, the wish of the Israeli government is to deploy throughout the world. It will therefore not be satisfied with supplying products to the Israeli market, but wants to obtain international market shares. This is why Israel is forging partnerships with several states such as Italy, Japan and India. The Israeli SSI companies are major players in these cyber-defence agreements. The collaborations between Israel and foreign countries also apply to Research & Development such as the centre opened in Singapore in February 2014. The Israeli space agency, IAI, participates in this project, whose purpose is to develop solutions for the detection of a current threat in cyberspace before it becomes effective. R&D is not the only field in question; the SSI companies also offer solutions for securing the information systems of foreign organisations. In November 2014, the security division of the MER Group signed a contract with the government pension fund of Mexico. The project runs over several years, during which time MER Security will notably supply the necessary tools for the protection of the information systems of the pension fund.

<sup>3</sup> The Israeli press (notably Haaretz and Times of Israel) echoed those initiatives in several articles the great majority of which is accessible in English.

<sup>4</sup> For a summary of the recommendations made by the national Board for research and development, see Lior Tabansky, *Cyberdefense Policy of Israel: Evolving Threats and Responses*, available online on the website of the cyber-defence and cyber-security Chair, [http://www.chaire-cyber.fr/IMG/pdf/article\\_3\\_12\\_-\\_chaire\\_cyberdefense.pdf](http://www.chaire-cyber.fr/IMG/pdf/article_3_12_-_chaire_cyberdefense.pdf)

<sup>5</sup> The SCADA systems (*Supervisory Control And Data Acquisition*) are automatic systems organising certain infrastructures, notably in the fields of water, electricity and transport.

It is important to underline that industrial research is not the only field supported by the Israeli government, which also pays special attention to university research. As early as in 2012, the INCB joined the Technology and Science Ministry in order to support it. Near 50 million shekels (around 13 million dollars) were thus committed to provide study and research grants in several universities around the country. The fields in question are not only technical. One of the particularities of Israel is that the cyber-stakes are not limited to engineering or computer studies. In the university of Tel-Aviv, for example, students work on the psychology of hackers, in order to better understand their mechanisms of action (individual or group).

### 3 - Tsahal

The Israeli army has defensive and offensive know-how across several specialised units, the most famous one being unit 8200. This unit has several units under its orders, such as the *Hatzav* which collects open source intelligence, or an elite commando unit which specialises in direct field operations. The *Computer Service Directorate* (CSD), in Hebrew called *Agav atikshouv*, is another structure in the Israeli military arrangement. The CSD involves three different branches, namely unit C4I, an operational brigade, and unit *Lotem*, specialised in telecommunication and information technology, and further divided into several specialised units <sup>6</sup>.

Nevertheless, the Israeli military structure is in constant evolution. In 2009, a sort of cyber-military staff was created within Unit 8200, whose role is to coordinate and lead the activities of the army in cyber-space. The soldiers of this organisation belong to Unit 8200 as well as to the CSD. In January 2012, seeking organisation and efficiency, the Israeli Defence ministry created a central organisation in order to better monitor the partnerships between the army, the Israeli security services and the private companies of SSI.

The cybernetics tool is not however limited to specialised units. For example, the *Yahalom* unit, which belongs to Military Engineering, uses sophisticated robots during its operations, such as the "EyeDrive", a cross-country robot <sup>7</sup>. One of the missions of unit *Yahalom* is to search for hidden arms and tunnels. It notably intervened with "EyeDrive" during the operation lead by Tsahal on the Gaza strip during the summer of 2014. In the end, the Israeli army aims to broadcast this cybernetics know-how to all of its units.

Since the middle of the year 2012, the senior officers, mostly those from the infantry, artillery and armoured brigades, must follow training in order for the cybernetics dimension to be taken into account in their command. It is the CSD, through unit C4I, which is in charge of this training. In February 2014, the army set up a second training module intended for senior officers who already have operational experience in cyber-defence in order to increase their awareness about the stakes and risks of the cyber-dimension.

The Israeli army is therefore in constant evolution. The strategic reflection conducted throughout Tsahal is as much about the distribution of responsibilities in the army's general organisation as it is about the acquisition of new technical skills, defensive as well as offensive, but not only. The military staff also wishes for all of the units of the army to integrate the cybernetics tools in their operations and for the officers to be trained in cyber-issues even if they are not directly concerned by this field of activity.

<sup>6</sup> Strategic Affaires Section (Olivier Danino), "The strategic use of cybernetics in the Middle East", Ministry of Defence, May 2013, <http://www.defense.gouv.fr/das/la-delegation/evenements/restitution-etude-utilisation-strategique-du-cyber-au-moyen-orient-22-avril-2013/restitution-etude-utilisation-cyber-au-moyen-orient-22-avril-2013>

## 4 – The creation of “Cyber Spark”

The creation of “Cyber Spark” is a perfect reflection of Israel’s ambitions which does not wish to merely separately support the industrial, military, research and education fields, but in reality to create a symbiosis among these different worlds. The aim being of course the sharing of experience, emulation and the pooling of each of these fields own know-how, in order to avoid dispersing and losing information.

Influenced by his experience in the United States when he was a student there, the Israeli Prime minister decided to create in Beer-Shev’a, a complex dedicated to cyber-matters in order to create this symbiosis: “Cyber Spark”<sup>8</sup>. The project, announced in January 2014 and estimated by the press at 9 billion dollars, should bring together on the same site Israeli and foreign manufacturers, university studies, private and public research centres, public institutions and all of the cybernetics units of Tsahal.

The site chosen for the constuction of “Cyber Spark” is quite close to the Ben-Gurion University, which is linked by railway to the Tel-Aviv University. These two universities are for Israel two major institutions in the field of cybernetics research and analysis. Several companies have already announced their participation in this project such as Microsoft, Deutsche Telekom or Lockheed Martin. In April 2014, the INCB, the Ben-Gurion University and Tsahal signed an agreement for 8.5 million dollars in order to establish a research centre within “Cyber Spark”. Lastly, the first CERT in Israel, created in November 2014 within the INCB, and therefore based in Tel-Aviv , will move its offices to the Beer-Shev’a in the course of the year 2015 or at the beginning of the year 2016. The project is therefore underway and seems to be well received by all of the players in the cyber-field in Israel, be they local or international.

## Conclusion

This quick overview of Israeli efforts in cybernetics matters shows that the Netanyahu government has made this field of activity a strategic priority. Israel is not only focused on the capacities of its army but also on those of its industries and of its private and public research, knowing that the targets that have been set can’t be attained without qualified and competent human resources, which explains the emphasis put on training youth. The lessons offered to the 16 to 18-year-old students are not only specialised but also clearly address the needs of the army, making higher quality recruitment possible for the army. At the end of their military service, at the age of 20 for women and 21 for the men, these young people have a very high-level practical and theoretical background considering their age, which they put toward the service of either the State or private companies specialised in the security of information systems. This is one of the strengths of the Israeli educational model.

<sup>7</sup> The Israeli army devoted an entire article to this unit in the French version of their website:<http://tsahal.fr/2012/04/17/yahalom-lunite-delite-qui-fait-face-au-terrorisme-a-laide-dune-technologie-de-pointe/>

<sup>8</sup> See official communication from the Ministry of Foreign Affairs, PM Netanyahu opens Cybertech 2014, announces creation of CyberSpark in Beer Sheba, 27 janvier 2014, <http://mfa.gov.il/MFA/PressRoom/2014/Pages/PM-Netanyahu-to-open-Cybertech-2014-.aspx>