Études de l'Ifri

ISRAELI CYBERPOWER

The Unfinished Development of the Start-up Nation?

Jean-Christophe NOËL

November 2020

ifri since 1979
French Institute of International Relations

Ifri is a research center and a forum for debate on major international political and economic issues. Headed by Thierry de Montbrial since its founding in 1979, Ifri is a non-governmental, non-profit organization. As an independent think tank, Ifri sets its own research agenda, publishing its findings regularly for a global audience.

Taking an interdisciplinary approach, Ifri brings together political and economic decision-makers, researchers and internationally renowned experts to animate its debate and research activities.

The opinions expressed in this text are the responsibility of the author alone.

ISBN: 979-10-373-0284-7

How to quote this document:

Jean-Christophe Noël, "Israeli Cyberpower: The Unfinished Development of the Start-up Nation?", *Études de l'Ifri*, Ifri, November 2020.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tel.: +33 (0)1 40 61 60 00 – Fax: +33 (0)1 40 61 60 60

Email: accueil@ifri.org

Website: Ifri.org

Author

Jean-Christophe Noël is a Research Fellow at Ifri's Security Studies Center. He was previously an officer in the French Air Force. After serving as fighter pilot, he held various positions on the General Staff, mainly dealing with policy or strategy issues.

He was also Deputy Chief of Staff of the French Air Chief of Staff from 2006 to 2009; a Military Fellow at the Center for Strategic and International Studies in Washington, DC, in 2009; as well as an expert on political and military affairs for five years at the Center of Analysis, Planning and Strategy (CAPS) in the Ministry of Foreign Affairs between 2012 and 2017.

Summary

Israel’s economic success in the cyber sector is undeniable. It is due to the development of an ecosystem encouraging the mastery of digital innovation. It is supported by proactive digital diplomacy and underpinned by unmatched military cybercapabilities in the region. However, its rapid growth exposes structural weaknesses from an economic point of view and raises questions about the role that Israeli democracy seeks to play on the world stage.

Table of Contents

Introduction

The sales representative finishes chatting with his client, carefully notes where they will meet and saves the large compressed digital file on a USB flash drive that he will hand deliver. Already late for their meeting, the sales representative hurries towards his car and connects to the Waze application to work out the quickest route. He is satisfied with the estimated arrival time and turns on the car radio. A journalist then discusses the latest Israeli cyberattack against the Iranian port of Bandar Abbas.

Without knowing it, our sales representative has just used different products or applications developed by Israeli engineers, such as Zip, Waze, online chat or the USB flash drive. He has also been made aware of the Israeli government's ability to conduct sophisticated cyberattacks. Both examples demonstrate Israel's digital power. Israel is a small country with only 9.2 million inhabitants that is smaller than Brittany. It was included for the first time in the top ten of the *Global Innovation Index* in 2019,[1] and is now commonly called the start-up nation.[2]

We will define Israeli digital power as Israeli actors' capability to exploit the opportunities provided by cyberspace, to help change the behavior of other actors on the international stage and achieve their own goals.[3] It is worth noting that a partner's change in behavior may be sought and does not necessarily result from constraint. The type of actors or purposes can also be quite varied. In this particular case, they will mainly be economic or security-related.

The aim of this paper is to characterize the drivers of this cyber power.[4] We will highlight the principles it is based on and set out the vision that drives it; identify the actors involved and clarify the respective roles of the State, private entrepreneurs, military personnel and academics; describe the potential it offers and examine how this cyberpower is exploited regionally and globally from an economic and military point of

[1] *Global Innovation Index 2019*, Ithaca: Cornell University Press, available at: www.wipo.int.

[2] A nickname given to Israel in an attempt to explain Israeli success in the digital sector. Cf. D. Senor and S. Singer, *Israël, La nation start-up*, Paris: Maxima Laurent du Mesnil, 2014 (2nd ed.).

[3] *Ibid.*, p. 11.

[4] The paper published by Ifri in 2018 on the concept of digital power will serve as a guide. Cf. J.-C. Noël, "Qu'est-ce que la puissance numérique?" [What is Digital Power?] Ifri, *Études de l'Ifri*, October 2019, p. 11, available at: www.ifri.org.

view; and finally assess its effects on Israeli society and on relations with its traditional allies.

In fact, Israel's economic success is due to the development of an ecosystem encouraging mastery of digital innovation (1). It is supported by proactive digital diplomacy and underpinned by unmatched military cybercapabilities in the region (2). However, its rapid growth exposes structural weaknesses from an economic point of view and raises questions about the role that Israeli democracy seeks to play on the world stage (3).

The Innovation Ecosystem

Background

The growth in Israeli cyberpower has been consistent with the choice by leaders to focus on a knowledge industry since the 1990s. 40% of Israeli-manufactured exports are now high-tech products compared to an Organisation for Economic Co-operation and Development (OECD) average of 16%, and 60% of exported services are IT-based compared to an OECD average of 30%.[5] The initial developments in this industry emerged in the agricultural and military sectors during the Cold War. Innovative solutions had to be found to develop the frequently barren land in order to feed the population. Irrigation techniques were refined and farmers were soon growing fruit and vegetables on arid soil.[6] France also provided Israel with most of its weapons in the 1950s and 1960s. This source suddenly dried up with the embargo imposed by General de Gaulle in 1967. The Israelis decided to turn to US suppliers and to develop their own military industry to reduce their dependence on other countries. Israeli engineers increased initiatives to adapt foreign equipment to local needs and modernized it to extend its lifecycle. The failure to develop the Lavi fighter jet in August 1987, resulted in the cancellation of large-scale programs and shaped the nature of the defense industry, that consequently invested in electronics and upgrading weapon systems.[7]

The end of the Cold War brought about new changes and a renewed framework for thinking and action. The triumph of economic liberalism[8] firstly resulted in the State's withdrawal that gave the private sector greater freedom. For instance, general deregulation of the telecommunications market was implemented, providing companies with new opportunities. Furthermore, the defense sector, although it remained crucial for Israel, took a more modest role. The era of inter-

[5] "Five Reasons Why Israel Has a Booming Start-Up and R&D Landscape", Consultancy-me.com, November 15, 2018, available at: www.consultancy-me.com.

[6] C. de Bonnaventure, "Comment Israël a transformé le désert du Néguev en immense laboratoire high-tech", *Géo*, November 15, 2019, available at: www.geo.fr.

[7] The domestic market was too small and the Americans pressurized the Israelis into dropping the project that they partly financed to reduce export competition against their own aircraft.

[8] J. Bendelac, "Du dirigisme militaro-industriel au libéralisme civil : l'économie israélienne dans tous ses états", *Politique étrangère*, Vol. 78, No. 1, 2013, pp. 37-49.

state wars ended and discussions for peace plans guided the strategic agenda. The number of employees in the defense industry was cut in half between 1985 and 1997.[9] Many of them moved into civilian industry and joined a highly-skilled foreign workforce. Israeli engineers, who contributed to Silicon Valley's success, returned from the United States, familiar with the rules of how startups and technology clusters operate.[10] Furthermore, one million former citizens of the Soviet Union, including approximately 100,000 scientists or engineers, emigrated to Israel between 1990 and 2009.

Therefore, political leaders seized the opportunity. Structurally, the country lacks natural resources and has a small domestic market. Its trade balance is therefore negative, with imports accounting for 35% of the gross domestic product (GDP) compared with 20% for exports. Saving the Israeli economy would thus come about through greater involvement in international trade. Its comparative advantage would be in the quality of a workforce ready to innovate and that is now flourishing.[11]

The decision was made to focus on the digital sector. Firstly, Israeli leaders foresaw the security issues that would arise with the development of IT at that time. Furthermore, a cyberindustry can start up quickly without having to rely on heavy industrial infrastructure.[12] The start-up model was adopted. Nonetheless, the model called for a focus on horizontal organizations, willingness to take risks, valuing knowledge-sharing and attention to market needs.

Although the vision and the political will existed, everything else, however, had to be implemented. It is within this context that the Israeli government acted as a catalyst to build an ecosystem for cyberindustry. It has played a decisive role in ensuring interaction between digital actors, financial investments and development of the cybersecurity industry.

[9] *Ibid.*, p. 29.

[10] *Ibid.*, p. 34.

[11] The politicians are taking up the reasoning that the military has been using since the 1950s. According to them, the best way to ensure Israel's survival is to focus on the quality of its soldiers given the much larger Arab armies. Cf. L. Norden, *Fighters Over Israel*, London: Greenhill Books, 1990, p. 29.

[12] The example of the autonomous car now proves this. The age-old corporate culture of car-manufacturers counts for less when the cars of the future will require the writing of 10,000 million lines of code to operate. Manufacturers have to turn to engineers who know how to write, improve and protect these lines of code.

Building human capital

Two categories of actors are particularly important in the development of digital hi-tech. The first is made up of academics. The academic sector has been supported since the 1950s to help with the country's development.[13] Investments made since then have achieved results, since Israel has the highest number of researchers per employed person in the OECD countries[14] and more engineers per capita than the United States and Germany.[15] The universities have cybercenters where the results of applied research can be used by entrepreneurs who are sometimes from the academic sector themselves. The Yissum program, developed by the Hebrew University of Jerusalem, has led to ten new company start-ups per year.[16] A share of the profits generated by these companies reverts to the university which in turn can fund new research.

The other significant category is the military. Most innovation originates from specific military requirements or applications developed in the defense industry.[17] They are often new and are regularly outsourced to the civilian sector. The need to store or protect data sparked the research that led to the development of the USB flash drive or firewalls that nowadays ensure the success of cybersecurity companies such as Check Point.[18]

Furthermore, many military personnel – conscripts or professionals – who move to the private sector can count on high-quality training. They have an extensive network of supportive former colleagues who have shared the same challenges. They maintain this network during reserve duty when they learn about the military's needs. The statistics confirm these trends, showing that 36% of start-up employees had been members of an army technical specialist unit and 32% of a combat

[13] D. Rosenberg, *Israel's Technology Economy: Origins and Impact*, New York: Palgrave Macmillan, 2018, p. 25.

[14] 17.4/1,000 in Israel compared to 7.8/1,000 in other OECD countries. Source: OECD.

[15] "Five Reasons Why Israel Has a Booming Start-Up and R&D Landscape", *art. cit.*

[16] É. Brasi, É. Laurençon and P. Nouma Anaba, *Israël, le 6^{e} GAFAM? Une stratégie de puissance au travers des nouvelles technologies*, Paris: VA Press, 2019, p. 101.

[17] The Israeli military innovation process has two specific facets. The first is that the process must address specific needs, such as the requirement to have a well-defined capability. The Iron Dome system evolved from the need to defend the country against short-range missiles. The Merkava tank was initially manufactured to protect the crew by placing the engine at the front of the vehicle. It is not about creating the weapons system of the future, but about performing a specific function. The second facet is related to the closeness of the military and manufacturers. Manufacturers often have access to battlefields and can see at first hand what does not work or requires improvement. This is how the innovation cycle quickly evolves.

[18] *Ibid.*, p. 100.

unit.[19] More than 1,000 start-ups have been founded by former members of Unit 8200, a renowned intelligence unit, that accounts for 25% of cybersecurity actors.[20]

Also, the military instills a culture in young conscripts that is well suited to working in start-ups.[21] It boosts short feedback loop environments, group loyalty and risk-taking. It emphasizes practical solutions to address specific problems rather than resorting to rigid concepts. Finally, the lack of respect for rules and hierarchy, a certain honesty, a bit of aggression, and lots of chutzpah complete the picture of the perfect soldier and Israeli citizen.[22] Therefore, the army is the primary incubator of the knowledge industry.[23]

The government's strength is knowing how to mix all these digital actors in clusters to make them work together. They are concentrated in the same places. As soon as an original and promising idea emerges, it is more easily taken up by a large number of experts to exploit its full potential. The entrepreneurial ecosystem first developed around Tel Aviv and Haifa, close to the best scientific universities. And although 77% of companies are currently located in the Israeli capital, the development of the CyberPark in Beer Sheva, in an economically poor area, contributes to the region's development. Military personnel, academics and researchers from private companies need to be able to mix every day and combine their expertise. Their interactions are all the more productive as the feeling of insecurity regarding the regional political situation is widespread in Israeli society. By helping to develop original solutions, each individual feels they are actively involved in the country's defense.

[19] D. Rosenberg, *Israel's Technology Economy, op. cit.,* p. 146.

[20] É. Brasi, É. Laurençon and P. Nouma Anaba, *Israël, le 6ᵉ GAFAM?*, *op. cit.*, p. 101. Unit 8200 is, more or less, the equivalent of the US National Security Agency (NSA). Nowadays, it is an elite unit where the very best young Israeli computer scientists perform their military service. It is the heir to the Shin Mem2 unit, that intercepted British or Arab telephone calls to the advantage of Jewish militias in the 1930s. It has been constantly modernizing since then and has regularly adopted state-of-the-art IT solutions that it helped to develop.

[21] Can the influence of the Jewish religion on economic behavior also be considered? The Jewish religion is a religion of the Book and all of the questions – and sometimes the answers – that arise from reading the Old Testament, can help to foster the curiosity and critical sense of its readers or believers. For general problems related to economic development and the influence of religion, cf. M. Weber, *L'Éthique protestante et l'esprit du capitalisme*, Paris: Gallimard, 2004.

[22] D. Rosenberg, *Israel's Technology Economy*, *op. cit.*, pp. 143-163; B. Linehan, "What Will Israel's Start-Up Nation Look Like in 2020", *Irish Tech News*, January 8, 2020, available at: https://irishtechnews.ie.

[23] B. Linehan, "What Will Israel's Start-Up Nation Look Like in 2020", *op. cit.*

Attracting financial investment

The government also implements public policies that are crucial for the development of innovation, making the necessary efforts to ensure macroeconomic stability[24] and to promote research. Public investment in R&D[25] amounted to 4.95% of GDP over the 2010–2018 period and is the highest in the OECD area.[26]

The government also compensates for market failures by trying to reduce the risks and uncertainties related to the development of new technology. The Office of the Chief Scientist, founded in 1969, is a state body that manages research and development funding and is responsible for this task.[27]

An incubator program was launched in 1991 to mainly help Russian migrants start their own businesses.[28] The aim is to offer support at the start of a project to keep entrepreneurs motivated and overcome the obstacles they encounter. Access to funding is guaranteed and material or intellectual support is provided. The government may commit money to the project, but does not get rich from it. Public funds are lost if the start-up fails. If it succeeds, the only requirement is for the initial funds to be repaid. Therefore, the government remains economically neutral.

Programs were also introduced at the same time to attract private and foreign venture capital. The aim was to create investment funds to address the critical lack of investment capacity. The most famous of them is Yozma, the high-risk investment fund,[29] supported by the government since 1992. The government invested US $ 100 million and proved its commitment by sharing the risks. Its success was immediate and this played a decisive role in the cyberindustry's launch.[30] Now, the proportion of foreign venture capital accounts for 65% of business conducted.[31] And while a dollar of

[24] D. Getz and I. Goldberg, "Best Practices and Lessons Learned in ICT Sector Innovation: A Case Study of Israel", *World Development Report 2016 Digital Dividends*, World Bank, 2016, p. 15, available at: http://pubdocs.worldbank.org.

[25] Research and development.

[26] "World Development Indicators: Science and Technology", World Bank, available at: http://wdi.worldbank.org.

[27] The Office of the Chief Scientist became the National Authority for Innovation (NAI) on June 21, 2015, and is a name that states its purpose clearly.

[28] S. Perez, *Iran-Israël : une guerre technologique*, Paris: Éditions François Bourrin, 2015, p. 73.

[29] "Initiative" in Hebrew.

[30] É. Brasi, É. Laurençon and P. Nouma Anaba, *Israël, le 6e GAFAM?*, *op. cit.*, pp. 72-73.

[31] "Five Reasons Why Israel Has a Booming Start-Up and R&D Landscape", *art. cit.* Approximately US $ 21.9 billion of venture capital was raised in Israel between 2006 and 2015. Although this sum is very high, it needs to also be put into context. Approximately US $ 333.5 billion of venture capital was raised in the United States during the same period.

public money attracted a dollar from private investors in the 1990s, it now attracts three times more.

Both states and foreign companies are also investing in Israel. Consequently, preferred partnerships are consolidated with some countries through binational foundations or funds. These organizations are generally involved in joint R&D programs.[32] Meanwhile, multinational corporations (MNC) use two types of strategy to take advantage of Israeli entrepreneurs' unique expertise.[33] The first is to establish R&D centers locally. For instance, Microsoft and Cisco have chosen to set up their first research centers outside the United States in Israel. The country now has 300 multinational corporations' R&D centers[34], sometimes employing up to 8,000 people.[35] The other strategy adopted by the MNCs is to purchase the most promising start-ups to exploit their ideas, their staff and to get a head start on the competition. Between 2016 and 2018, 716 start-ups were bought by large companies, most of which let Israeli engineers continue working in situ.[36]

Currently, Israel is estimated to have 8,000 start-ups and 356 incubators.[37] The Israeli government has managed to create a climate of confidence for foreign investors by offering them high dividends for measured risk-taking. In terms of power, it has succeeded in creating close ties with the world's leading digital actors who depend on local R&D to continually improve their products. Israel has managed to make itself indispensable in the global digital innovation process.

Prioritizing cybersecurity

In the end, the government's role is decisive in selecting which technologies are supported. Of course, disruptive technology, ensuring a leading position in state-of-the-art fields, is prioritized. For instance, projects developed in the incubators are selected according to the government's industrial and strategic priorities. The artificial intelligence sector accounts for 40.7% of Tel-Aviv-based start-ups'

[32] Examples include the BIRD Foundation for Israel and the United States, the SIIRD with Singapore, BRITECH with Great Britain or KORIL with South Korea. Other agreements are in place with Germany, France or China, that allow Israeli companies participating in these programs to receive OCS funding. Cf. *Best Practices and Lessons Learned in ICT Sector Innovation: A Case Study of Israel, op. cit.*, p. 32.

[33] *Ibid.*, p. 26.

[34] N. Falevich, "Start-Up Nation Central: Finder Insights Series/Israel's Cybersecurity Industry in 2018", *Start-Up Nation Central*, 2019, available at: http://mlp.startupnationcentral.org.

[35] P. Thouverez, "Israël: un tissu numérique de pointe dans un environnement unique au monde", *Cvstene*, available at: www.cvstene.fr. Information about the presence of French companies in Israel.

[36] É. Brasi, É. Laurençon and P. Nouma Anaba, *Israël, le 6e GAFAM?*, *op. cit.*, p. 73.

[37] IVC Research Center, August 14, 2020, available at: http://compassvgg.com.

activity. Companies working on Big Data or cloud management account for 38.1%.[38] Research in quantum information technology, 5G, human behavior in cyberspace and homomorphic encryption is also very advanced.[39] On the other hand, activity related to the development of digital consumer products, media and entertainment is not very widespread, as they often require significant investment to start up that Israeli companies cannot obtain.[40]

Cybersecurity is the sector most prioritized by government policies. Since the invention of the Internet, the Israeli government has been aware of defense issues related to cyberspace and acts to maintain its sovereignty. In 2002,[41] the National Information Security Agency (NISA) was established, under the leadership of Shin Bet,[42] to focus on the protection of both critical public and private systems.[43] The concept of shared responsibility is set out between regulators and users, with the latter expected to assume an active role in protecting their digital facilities and data. A reorganization was carried out in 2011 to pre-empt future threats, as most systems that did not come under the "critical systems" category became too vulnerable. The National Cyber Bureau (NCB) was founded under the Prime Minister's leadership. As a think tank, it is responsible for developing national capability and building an ecosystem that continually adapts to new challenges. After several years of considerable tension between the various security agencies and civilian companies, a National Cyber Directorate (NCD) was established in 2017. This political organization's role is to ensure the defense of civilian infrastructure – just like the French National Cybersecurity Agency (ANSSI) – and to maintain Israeli commercial leadership.

The initiatives taken by the NCB significantly boosted the cybersecurity sector. Some projects, such as "Kidma" or "Masad" have been launched with the OCS and the Ministry of Defense to develop R&D and local entrepreneurship.[44] Above all, the NCB is pushing to improve education in digital science.[45] The education budget increased

[38] Available at: https://startupgenome.com.

[39] "Cyber and Innovation in Israel: Cigref Learning Expedition in November 2018", *CIGREF*, 2019, p. 6, available at: www.cigref.fr.

[40] D. Rosenberg, *Israel's Technology Economy*, *op. cit.*, p. 84.

[41] ANSSI was established in 2009.

[42] Shin Bet, the Israeli domestic security agency, had experience in this field with responsibility for protecting embassies and national companies.

[43] Nineteen such systems were identified.

[44] "Ghavim" program. Cf. O. Danino, "L'économie de la cybersécurité en Israël", *Chaire de cybersécurité & cyberdéfense Saint-Cyr, Sogeti, Thalès*, March 2017, p. 4, available at: www.chaire-cyber.fr.

[45] G. Press, "6 Reasons Israel Became A Cybersecurity Powerhouse Leading the $82 Billion Industry", *Forbes*, July 18, 2017, available at: www.forbes.com.

from US $ 6.9 billion in 2010 to US $ 11.8 billion in 2019. Cybersecurity-related sectors benefited from public initiatives. Six university research centers are specifically focused on this subject. Interdisciplinarity is favored over mere technical education with regular participation by social science experts.

The NCB plays a key role in expanding the pool of young Israelis who can move into cyberindustry.[46] The teaching of computer science and programming starts from high school in the most advantaged areas. Final secondary school examinations offer options in these subjects. Inter-school hacking tournaments are even organized. Recruiters also travel to disadvantaged areas to identify potential talent that could join military units. Generally, young people with specific skills are supervised and receive appropriate education in computer science or cybersecurity depending on their ability.[47]

The initiatives undertaken by the NCB, and then the NCD, have achieved convincing results, since 20% of Israeli high-tech companies are now focused on cybersecurity. Their development has been continuous. There were 20 companies in the sector in 1996, 250 in 2006 and up to 350 in 2018.[48] These companies' performance is impressive. Out of the leading 150 cybersecurity firms in the world, 18 are Israeli.[49] In 2014, their export volume reached US $ 6 billion and exceeded that of the arms industry.[50] It is estimated that a dollar invested in this sector generates between five and eight dollars for the Israeli economy.[51] The future need to establish firewalls to protect applications in the artificial intelligence (AI) or Internet of Things (IoT) sectors to prevent any attempt to take control remotely, suggests the markets will remain both strong and profitable.[52]

The cybersecurity example shows how the Israeli government has managed to build a digital ecosystem that creates an economic virtuous circle. Beginning with a military need or a new technical application, Israeli entrepreneurs develop a practical and innovative solution based on their culture and closeness to other actors. The initial development is

[46] *Ibid.*

[47] "Magshimim" and "Ghavim" program. Cf. O. Danino, "L'économie de la cybersécurité en Israël", *op. cit.*, p. 6.

[48] "Cybertech 2018 – un point sur la cyber-sécurité vue d'Israël", *Direction générale du trésor*, February 9, 2018, available at: www.tresor.economie.gouv.fr.

[49] Or 12% of companies worldwide. French companies do not appear in this ranking. Cf. "Hot 150 Cyber Security Companies 2020", *Cybercrime Magazine*, available at: https://cybersecurityventures.com.

[50] D. Rosenberg, *Israel's Technology Economy*, *op. cit.*, p. 85.

[51] "Cyber and Innovation Israel: Cigref Learning Expedition in November 2018", *art. cit.*

[52] N. Falevich, "Start-Up Nation Central: Finder Insights Series/Israel's Cybersecurity Industry in 2018", *art. cit.*

funded by venture capital and the product is offered for export, bringing in money that pays back the investors. The success of a start-up attracts MNCs which then purchase it. In turn, the MNCs invest in further research.[53] Consequently, Israel's economic power is due to this constant ability to be at the forefront of innovation. Its success also lies in its ability to closely coordinate economic power with its national sovereignty.

[53] The entrepreneurial example provided by Ami Moyal is symbolic from this point of view. With a team made up of linguists or engineers in the start-up he founded at Ben-Gurion University, Ami Moyal managed to develop software capable of isolating a spoken conversation in a very noisy environment. The need probably came from the intelligence services, that supported Moyal in his research. After achieving his goal, Moyal was able to export his product to other foreign intelligence agencies, particularly the NSA and hoped to be able to develop civil applications to attract other clients. Cf. J. Benillouche, "Ami Moyal, le chercheur par qui le scandale des écoutes de la NSA est arrivé", June 20, 2015, available at: www.slate.fr.

A Global Stance

Although digital resources are primarily used in Israel in the private sector to achieve economic objectives, the adage "cyberspace serves, first and foremost, to wage war" is also true.[54] Israeli cyberpower is extensively utilized in diplomatic and military fields that are places of constant conflict.

Becoming a global player using cyberdiplomacy

Israel needs to expand its cyberindustry abroad to ensure a sufficient level of exports to keep the virtuous circle of its innovation system running. To this effect, the Israeli authorities are seeking to epitomize the excellence of their high tech by organizing annual cyberspace events.[55] The oldest event is Cyber Week, whose last session brought together 400 contributors and 9,000 participants coming from more than 80 countries.[56] Leading figures and actors from the digital world come to speak there. In 2014, the Israeli authorities launched Cyber Tech, where participants have the opportunity to present their cybersecurity products. In 2020, Cyber Tech brought together more than 18,000 participants, 200 companies and 160 delegations.[57] CyberTech has now become a brand that can be exported to other capitals where this type of exhibition is organized. A source of prestige and a preferred meeting place, these two types of events are a showcase for the Israeli digital ecosystem and appropriate places to spread the watchwords of Israeli politics.

The message is often the same. Israeli cyberactors already have the solutions to your problems; if not, they will find them for you. Forming closer ties with them, is working towards significantly improving your own situation. In his annual address to the United Nations in 2016, Benyamin Netanyahu also insisted that "governments are changing their attitude towards Israel, because they know that Israel can help them protect their

[54] F. Douzet and A. Gery, "Le cyberespace, ça sert d'abord à faire la guerre. Prolifération, sécurité et stabilité du cyberespace", *Hérodote*, Vol. 177-178, No. 2020/2, pp. 329-350.

[55] D. Amsellem, "Le cyberespace israélien, un enjeu de puissance", *Hérodote*, Vol. 177-178, No. 2020/2, pp. 281-296.

[56] More information available at: https://cyberweek.tau.ac.il.

[57] More information available at: www.cybertechisrael.com.

people, can help them feed them, and can help them better their lives".[58] In a more security-oriented vein, in 2018 Y. Unna, a Director of the NCD, invited countries lagging behind in the cybersecurity field to open their doors to Israeli companies. He explained that governments "that cannot contain the rapidly evolving threat in cyberspace on their own, should encourage and support more partnerships between and with (Israeli) companies to establish operational domination in cyberspace".[59]

The scope of Israel's links with companies or foreign countries extends beyond the economic sphere. The partnerships are a diplomatic asset. Israel is forging closer relations with partners that were previously inhibited by the Israeli-Palestinian conflict.[60] It can break its diplomatic isolation and gradually build new partnerships. The extent of its diplomacy is increasing significantly and extending to African and Asian countries. However, its partners can get involved with some peace of mind. The Israelis are exporting ideas and innovative processes that are intangible products. Cooperation is not based on developing technical facilities with factories or manufacturing plant. The physical footprint is minimal. Israel primarily exports components that restrict the scope of possible calls for boycott.

In actual fact, Israel is gradually going out into the world. Israel has moved closer to giants on the international stage such as India and China.[61] Admittedly, in the case of India, trade between both countries is primarily concentrated in the arms sector.[62] However, many programs initiated by the Indian government, such as "Digital India", "Make in India" or "Startup India" require improved innovation capacity and access to the most up-to-date technology. The explosion of the mobile Internet also requires new solutions in a country that must make up for a significant delay. In this respect, the Indian prime minister, Narendra Modi, urged his countrymen to work more closely with Israeli companies in water management, agriculture and digital technology. He emphasized that a people's determination counts more than a country's size. India does not deny its

[58] O. Danino, "L'économie de la cybersécurité en Israël", *art. cit.*

[59] "Cybertech 2018 – un point sur la cyber-sécurité vue d'Israël", *art. cit.*

[60] Although the fight against Iran is a key factor in explaining the agreement to normalize diplomatic relations between Israel and the United Arab Emirates, access to Israeli companies – already well established in defense matters – also influenced Abu Dhabi's choice. It should help maintain economic development.

[61] D. Rosenberg, "How Israel Is Turning Its High-Tech into Global Political Power", *Fathom*, November 2018, available at: https://fathomjournal.org.

[62] For relations between India and Israel, see N. Blarel, *The Evolution of India's Israel Policy: Continuity, Change, and Compromise since 1922*, Oxford: Oxford University Press, 2015.

support for the Palestinian cause – it condemned the relocation of the US embassy from Tel Aviv to Jerusalem in a United Nations vote, that is a legacy of Third World solidarity, while developing technical partnerships with Israel. It states its admiration for Israel without any qualms.

Bilateral relations with Beijing have taken on a scale that would have been inconceivable at the end of the Cold War. Israel offers attractive opportunities for two Chinese projects. Its geographical position, at the crossroads of Europe, Africa and Asia, makes it an ideal back door for promoting the development of the Belt and Road Initiative (BRI) to the West. Furthermore, its innovation capacity is attractive to Chinese officials, who are determined to make the "Made in China 2025" project succeed amid technical decoupling from the United States.[63] In return, Israeli enthusiasm is obvious. Benyamin Netanyahu stated during an official visit to China in 2017 that Israel and China were the perfect partners to technically ensure continuous improvement in products and services.[64]

The exact extent of relations between the two countries is difficult to estimate. It is sometimes inhibited by the culture shock between Israeli and Chinese entrepreneurs. The Israelis favor boldness while the Chinese uphold their ideology. A report in 2018 stated that Chinese investments in the Israeli high-tech sector had only increased 2.4 times between 2013 and 2017. Fewer start-ups had been purchased, with the notable exception of Playtika in 2016 for US $ 4.4 billion. Nevertheless, it appears that the figures are significantly higher.[65]

On the other hand, the cultural barriers seem insignificant in trade relations between Russians and Israelis. President Vladimir Putin even considers Israel as a Russian-speaking state.[66] Trade between the two countries has particularly developed during the last decade, increasing by 70%,[67] and microeconomic relations between Israeli entrepreneurs of Soviet origin and their Russian counterparts remain extremely strong. The Israelis regularly join forces with the Russians if they are looking for skilled labor. However, these relations are currently thwarted by Moscow's support for Tehran, although the contacts remain very open and often successful at the highest level.

[63] E. Shira, K. Schwindt and E. Haskel, *Chinese Investment in Israeli Technology and Infrastructure: Security Implications for Israel and the United States*, Santa Monica: RAND Corporation, 2020, pp. 17-20, available at: www.rand.org.

[64] D. Rosenberg, "How Israel Is Turning Its High-Tech into Global Political Power", *art. cit.*

[65] *Ibid.*

[66] "Putin Says He Considers Israel a Russian-Speaking Country", *The Times of Israel*, September 19, 2019, available at: www.timesofisrael.com.

[67] D. R. Edmunds, "Russia-Israel Trade Exceeds $5 Billion for Second Year Running", *The Jerusalem Post*, January 28, 2020, available at: www.jpost.com.

Asserting its power regionally

Israeli military officials officially recognize cyberspace as a hostile environment.[68] Israel has to deal with a continuous onslaught of cyberattacks from state and non-state actors. The vast majority of attacks are low level and take the form of website hacking or denial of service attacks. They are often the work of isolated activists. However, the boundaries between cybercrime and cyberwar are blurred, with teams of hackers sometimes attacking certain targets for both financial and political reasons.[69]

The greatest concerns come from attacks by structured or state organizations. Although Hamas does not have as sophisticated resources as Israel, it is becoming increasingly aggressive in this field. Hamas specializes in spying on soldiers or high-value targets by penetrating social media or hacking into mobile phones.[70]

Cyberwar against Hezbollah has been ongoing for years.[71] The Shiite organization seems to be particularly involved in using information to create fake news and shape the general public's perception. It is allegedly training many agents to manipulate digital photos, manage fake accounts on social media, or create engaging videos. It has set up groups of IT operators that could be mobilized in Lebanon or Iraq if needed. The aim is to promote the organization's political agenda and to raise regional or international public opinion in its favor, particularly in the event of a crisis with Israel.[72]

Iran is undoubtedly the most formidable opponent, even though it is admitted that its capabilities do not yet reach the level of those of

[68] Threats against the state of Israel are symbolized by four circles. The first corresponds to conventional threats from hostile states, that would use their armies to fight. The second consists of unconventional threats, with attempts by regional states to develop nuclear weapons or a chemical arsenal. The third refers to the challenges posed by terrorist movements and irregular warfare. Finally, the fourth and last circle represents cyberspace. It was recently added to take into account the dangers impacting the functioning of Israeli society and institutions. Cf. G. Eizenkot, "Cyberspace and the Israel Defense Forces", *Cyber, Intelligence, and Security*, Vol. 2, No. 3, December 2018, pp. 99-104, available at: www.inss.org.il.

[69] N. Falevich, "Start-Up Nation Central: Finder Insights Series/Israel's Cybersecurity Industry in 2018", *art. cit.*, p. 3.

[70] O. Dostri, "Hamas' Cyber Activity Against Israel", *The Jerusalem Institute for Strategy and Security*, October 15, 2018, available at: https://jiss.org.il.

[71] H. M. Al-Rizzo, "The Undeclared Cyberspace War between Hezbollah and Israel", *Contemporary Arab Affairs*, Vol. 1, No. 3, July 2008, pp. 391-405.

[72] W. Crisp and S. al Sahly, "Exclusive: Inside Hizbollah's Fake News Training Camps Sowing Instability across the Middle East" *The Daily Telegraph*, August 2, 2020.

Israel.[73] It takes advantage of the ambiguity related to cyberattacks to conduct many covert operations, by adopting a strategy closely aligned with the regional situation. Its cyberactivity is often a response to events affecting Iranian policies. This cyberactivity can even go so far as destroying its targets, by digitally sabotaging their modes of operation.

There is no official Israeli cyberpolicy to respond to these threats.[74] However, Israeli cyberwar fits perfectly into a more comprehensive strategy.[75] The Israeli military consider that the space of general conflict around them, cannot be defined by clear and pronounced geographic, political, economic, military or social boundaries. It is shifting, indeterminate, and dependent upon the changing strategies of all the actors in the area. The role of the Israeli Defense Forces (IDF) is to constantly operate in all of this space.[76] Therefore, Israel lives in a state of latent war. And although the period of great victories, such as the Six Day War, is over, it must, as in the past, deter opponents from engaging in conventional warfare to avoid costly conflicts in human and financial terms. This state of latent war is therefore regularly marked by short but sudden military operations intended to limit opponents' capabilities and willingness to engage.[77] A mix of deterrence through denial and retaliation should help prevent action by its enemies.[78]

[73] G. Siboni, L. Abramski and G. Sapir, "Iran's Activity in Cyberspace: Identifying Patterns and Understanding the Strategy", *Cyber, Intelligence, and Security*, Vol. 4, No. 1. March 2020, available at: www.inss.org.il; J. Lewis, "Iran and Cyber Power", *CSIS*, June 25, 2019, available at: www.csis.org.

[74] From an organizational point of view, there is also no independent Cyber Command in Israel, as in the United States. Despite the wish of General G. Eisenkott, the former IDF Chief of Staff, who advocated for this solution, it was decided to proceed gradually by initially giving greater authority to the departments handling cyberaffairs. Their independence would come about later. The Military Intelligence Directorate, which includes Unit 8200, is responsible for intelligence, while another more operational one, called C4I Directorate, is responsible for managing and defending the IDF's networks. It can undertake offensive military operations. Cf. "Cyberspace and the Israel Defense Forces", *art. cit.*; M. Raska, "Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy", *Policy Report*, S. Rajaratnam School of International Studies (RSiS), January 2015, available at: www.michaelraska.de; "Israel Defence Forces Will Not Create Cyber Command, But Will Strengthen Military Cyber Defences", *spacewatch.global*, available at: https://spacewatch.global.

[75] Broadly speaking, the Israeli strategy consists of emphasizing preparation and information because of the lack of strategic depth, having qualitative superiority to compensate for the lack of soldiers, allying itself with a superpower and finally having the means of ultimate deterrence as a last resort.

[76] T. Libel, "Explaining the Security Paradigm Shift: Strategic Culture, Epistemic Communities, and Israel's Changing National Security Policy", *Defence Studies*, Vol. 16, No. 2, 2016, p. 151.

[77] More specifically, repeated low-level military operations must be carried out to teach the opponent the Israeli rules of the game, to impress them and leave a psychological mark. If the opponent begins to break the rules, a larger-scale operation is conducted, not to achieve a great victory, but to reduce the opponents' military capability, restore the principle of deterrence and ensure a period where the level of conflict will be lower. Cf. D. Adamsky, "From Israel with Deterrence: Strategic Culture, Intra-war Coercion and Brute Force", *Security Studies*, Vol. 26, No. 1, 2017, pp. 157-184.

[78] Deterrence by denial aims to prevent the enemy from achieving their objectives in the event of aggression through effective defense. Punitive deterrence involves severely striking the opponent in the event of attack, enforcing greater costs on them than the gains they hope to achieve.

Israel conducts both defensive and offensive cyberoperations based on these principles. From a defensive point of view, Unit 8200 seeks to infiltrate enemy organizations to pre-empt their operations. Robustness and resilience are emphasized for the defense of networks.[79] But the Israeli operators' main advantage is their responsiveness and mastery of innovation. They are constantly developing new algorithms, firewalls and tactics to resist cyberattacks. Attacks by the Syrian Electronic Army, Korean hackers in 2019, or Palestinian sympathizers during military operations against Hamas have not crippled the country.[80] Israel is primarily deterring by denial, managing – for the time being – to reduce the effect of the most severe attacks on its territory through effective defense.

From an offensive point of view, the Israelis tend to prefer pragmatism. They do not hesitate to use all the resources available in cyberspace to advance their interests, ranging from espionage to sabotage,[81] from supporting military operations to destroying cyber targets. In 2007, the Israelis launched an air attack on facilities suspected of containing a Syrian nuclear reactor, and digitally penetrated the local anti-aircraft defense networks and neutralized them. In 2010, they sabotaged the operation of Iranian atomic centrifuges with the help of the Americans, delaying the Iranian nuclear program by two years.[82] They spied on the Iranians with the Flame or Duqu viruses in the 2010s. Meanwhile, they extended the fight in cyberspace to the physical world, by bombing a Hamas building in May 2019 where a cyberattack was being planned.[83] The most recently publicized action was triggered after an Iranian attack on the Israeli water distribution system's infrastructure on April 24 and 25, 2020.[84] It was reportedly carried out by the Revolutionary Guards' offensive cyberunits. Tel Aviv retaliated by bringing down the computers managing the port of Bandar Abbas in southern Iran. The flows of boats, trucks and merchandise were severely disrupted, resulting in the port's temporary closure.

[79] G. Press, "6 Reasons Israel Became A Cybersecurity Powerhouse Leading the $82 Billion Industry", *art. cit.*

[80] D. Amsellem, "Le cyberespace israélien, un enjeu de puissance", *art. cit.*, p. 291.

[81] T. Rid, *Cyber War Will Not Take Place,* New York/London: Oxford University Press/Hurst, 2013.

[82] The effect of successful aerial bombardment would have been similar. Cf. S. Perez, *Iran-Israël: une guerre technologique*, *op. cit.*, pp. 7-9.

[83] Z. Doffman, "Israel Responds to Cyber Attack with Air Strike on Cyber Attackers in World First", *Forbes*, May 6, 2019, available at: www.forbes.com.

[84] D. Siman-Tov and S. Even, "A New Level in the Cyber War between Israel and Iran", *INSS Insight*, No. 1328, June 3 2020, available at: www.inss.org.il.

In this case, like during the May 2019 bombardment, the Israeli initiatives are in keeping with the thinking that dominates the cycle of Israeli operations. By regularly raising the rhetoric and suddenly increasing the intensity of operations, Israel is reminding its enemies of its determination; emphasizing its technical and military superiority to inflict severe damage; and trying to deter by retaliation.

Additionally, the last operation could have been conducted clandestinely. In fact, the Iranians could have already attacked the Israeli water infrastructure twice, without the nature of the retaliation having been revealed. This "naming and shaming" contributes to the posture of deterrence, mainly sending the signal that Tel Aviv takes responsibility for its actions. It is also part of the new approach that the Israelis are giving to their cyberspace operations, not hesitating to use transparency to defeat the information war waged by its opponents.

They also willingly adopt the codes and specific language of social media to attract and convince an ever-increasing share of young Internet users. Pop culture references are also carefully chosen. Following Israeli retaliation on the Iranian port, the Director of the NCD, Y. Unna said that, "the cyberwinter [was] coming", quoting the successful television series Game of Thrones. His message was widely reported.[85]

By having the digital tools to assert its security interests and by developing an ambitious digital diplomacy, Israel has the main attributes of cyberpower. It remains to be seen whether this cyberpower is built on stable foundations or whether some weaknesses could threaten its survival.

[85] Cf. M. Srivastava, N. Bozorgmehr and K. Manson, "Israel-Iran Attacks: 'Cyber Winter Is Coming'", *Financial Times*, May 31, 2020, available at: www.ft.com; D. Amsellem, "Le cyberespace israélien, un enjeu de puissance", *art. cit.*, pp. 293-295.

Foundations to Be Consolidated

However, the rise of Israeli cyberpower shows some weaknesses in the economic and diplomatic fields, where it has rapidly asserted itself. From an economic point of view, it is above all structural weaknesses and the specificity of its model that raise questions.

Bottlenecks

The first problem, which is surprising in a country that places so much value on initiative, is the excessive bureaucracy.[86] Israel is only 35th in the global ranking of countries that have a business-friendly environment. It is 28th in the ranking of countries conducive to business start-ups. The OECD ranks Israel in 69th place for countries where excessive bureaucracy is under control.[87] The regulations are often onerous and complicated, and can hinder the growth of young companies that do not benefit from state assistance. The high-tech sector also suffers from rising rents and cost-of-living, particularly in Tel Aviv. The development of public transportation is slow and many traffic jams hinder the smooth flow of both people and goods.[88]

Above all, the development of the digital industry is not taking the rest of the economy with it.[89] The Israeli economy has a double structure, with a sector immersed in the knowledge industry and another, isolated and inward-looking, which is evolving in a protected and uncompetitive environment. The productivity of this sector is very low compared to that of other developed countries. It does not even benefit from high-tech innovation, since the rate of adopting new technology is lower in Israel than in other OECD countries.[90] This lack of connectedness in the local economy means that digital start-ups' contribution to Israeli economic power is limited.

[86] N. Bosma, S. Hill, A. Ionescu-Somers *et al.*, *Global Report 2019-2020*, London: Global Entrepreneurship Monitor, 2020, pp. 124-125.

[87] K. Schwab, "The Global Competitiveness Report 2019", *World Economic Forum*, 2019, p. 33, available at: www3.weforum.org.

[88] B. Linehan, "What Will Israel's Start-Up Nation Look Like in 2020?", *art. cit.*

[89] "L'économie israélienne", *Direction générale du Trésor*, available at: www.tresor.economie.gouv.fr.

[90] K. Schwab, "The Global Competitiveness Report 2019 ", *art. cit.*

Only a homogeneous elite, representing 8% of the working population and generally coming from the leading universities or certain military units, benefit from the development of high tech in the end. Jewish men aged under 45 years and non-Orthodox, represent 67% of this elite. Wealth hardly trickles through to other social categories. Israeli society has one of the highest poverty rates in the OECD zone.[91]

Furthermore, high investment by the state in education is failing to deliver the expected results. Israeli students obtain average scores compared to students in other OECD countries.[92] However, the two population categories with the highest birth rate, namely Israelis of Arab origin and ultra-orthodox Jews, face great difficulty in their scientific studies and seem to be excluded from the Israeli miracle. The first group suffers from studying in poorly-funded schools. The teaching takes place in Arabic and their adjustment is more difficult when they have access to university. The second group initially studies traditional religious texts and struggles to achieve the level required for scientific studies.[93] The fact that both of them do not generally undertake military service exacerbates the problem.

Yet, the Israeli knowledge industry now desperately lacks engineers and developers. Approximately 18,000 specialists are needed to satisfy market demand.[94] Certainly, the brain drain maintains this shortfall, with 11% of doctoral graduates living abroad for at least three years.[95] But the professionals regret not being able to draw on all of the country's communities and believe their better integration in the high-tech sector could make the difference.[96] They are also calling for the government, in conjunction with companies, to fund training and coaching for potential employees.

Israel's cyberpower is concentrated and leaves out parts of the population that could help it meet the increasing demand. Questions are also being asked about its growth model.

[91] "Taux de pauvreté", OECD data, available at: https://data.oecd.org.

[92] 2018 PISA results, OECD, pp. 3-4, available at www.oecd.org.

[93] The number of ultra-Orthodox working in the high-tech sector has been increasing since 2014, but they only represent 3% of the people in this industry. Cf. T. Heruti-Sover, "Number of ultra-Orthodox in Israeli High-tech Soared in Past Years, Study Shows", *Haaretz*, July 28, 2020, available at: www.haaretz.com.

[94] "L'économie israélienne", *art. cit.*

[95] É. Brasi, É. Laurençon and P. Nouma Anaba, *Israël, le 6e GAFAM? Une stratégie de puissance au travers des nouvelles technologies*, *op. cit.*, p. 12.

[96] NoCamels Team, "Israeli Tech Industry Grows But Employee Shortage Climbs to 18,500 – Report", *Nocamels*, February 26, 2020, available at: https://nocamels.com.

A set model?

The Israeli digital sector does not have large companies that would belong to the GAFAM club[97] and dominate their market.[98] Indeed, start-ups rarely succeed in becoming larger entities that would require the employment of sales, accounting or legal staff to operate and grow. They fail to exploit their innovation.

Two main explanations can be put forward. The first is that the current Israeli model is self-sustaining.[99] Inventors can get rich quickly by selling their companies and are satisfied with this. Demand is not weakening either, with MNCs significantly improving their performances by purchasing the most dynamic start-ups. The products created by the Israeli digital industry are in fact the companies themselves.[100]

A second reason is that the local culture that fosters the emergence of the start-ups is very poorly adapted to the following stages of development. Israeli entrepreneurs lack the discipline and rigor needed to carefully and correctly organize the various functions of a very large international company. This managerial and logistical knowledge is very difficult to find in Israel.[101] The lack of large national companies that could train experts or serve as an example compounds the problem.

Solutions are being proposed for the high-tech sector to move beyond the scale-up stage. The development of medium-sized companies employing up to 500 people, as in Germany, would serve as a learning experience for entrepreneurs and would allow a decisive step to be subsequently taken. Building the factories of the future in Israel, using sophisticated algorithms and electronic sensors generating lower manufacturing costs, could also give Israel a head start in the industrialization process of the digital era. Other avenues will certainly need to be explored to diversify the sector's resources and not make it dependent on a single development model.

[97] GAFAM is the acronym for Google, Apple, Facebook, Amazon and Microsoft.

[98] The largest Israeli company is Teva Pharmaceutical Industries, that has the 496th place in the Forbes 500 ranking. In addition, the country only had three unicorns in 2018 and only 1% of Israeli high-tech companies were listed on the US Stock Exchange in 2017. Cf. É. Brasi, É. Laurençon and P. Nouma Anaba, *Israël, le 6e GAFAM?*, *op. cit.*, p. 24.

[99] The average lifetime of an Israeli start-up prior to its purchase was 3.95 years in 2014, as opposed to 6.41 years for a British start-up, 6.66 for a French one and 9.03 for a Swedish one. Cf. "Israel's Technology Economy", *op. cit.*, p. 108.

[100] *Ibid.*, p. 83.

[101] *Ibid.*, p. 38.

Are the entrepreneurs… too enterprising?

At the same time, the competition to win foreign markets has become increasingly difficult. The importance of digital technology in everyday life is now well understood by economic actors worldwide. There is an increasing supply to win new markets and this sometimes tends to saturate them. The strong microeconomic dynamism in the Israeli cybersecurity sector appears to be waning somewhat. Only 40 new Israeli start-ups were founded in 2019 compared to 60 in 2016.[102]

Since maintaining market opportunities is essential to sustaining the Israeli model, the government is responding to this challenge by partly reducing its regulation of digital exports. Initially, regulation of arms exports was used to control the cybersecurity sector.[103] However, statements at the highest level of state show that companies are encouraged to be bold in their quest for clients. Benyamin Netanyahu also states that, "anything that is not specifically forbidden is authorized", in the area of digital exports. He recently said that, "we have to take risks and it's a considerable risk to regulate less in order to grow more".[104]

This perceived loosening of rules is worrying for many observers. The decision to be less particular about the choice of clients makes it more likely that hackers or non-state actors will acquire high-performance software. The spread of these products is to be feared. The fact that they are sold to authoritarian states also worries many non-governmental organizations (NGOs). The United Nations' Special Rapporteur on Freedom of Opinion and Expression, D. Kaye, reflects this concern when he says that the Israeli control process is shrouded in a "veil of mystery", while sales should be conditional upon human rights compliance criteria.[105]

Investigations by journalists or NGOs proved that these concerns were justified. The newspaper, *Haaretz*, also found that Israel is the leading exporter of algorithms designed to spy on the civilian population.

[102] Cisomag, "Cyber Startup Hub in Israel Declines as Global Competition Rises: Elron VP", February 7, 2020, available at: https://cisomag.eccouncil.org.

[103] "L'économie de la cybersécurité en Israël", *art. cit.*

[104] T. Cohen and A. Rabinovitch, "Israel Eases Rules on Cyber Weapons Exports Despite Criticism", *Reuters*, August 22, 2019, available at: https://fr.reuters.com. Now, for example, lead times in decision-making processes on the sale of cybersecurity products to an allied country are reduced from 12 to 4 months to improve the position of Israeli companies during tender process. Cf. N. Lindsey, "Concerns Mounts as Israel Eases Rules on Cyber Weapons for Cyber Espionage", *CPO Magazine*, September 2, 2019, available at: www.cpomagazine.com.

[105] *Ibid.*

Many Israeli companies are involved in this market.[106] Citizen Lab published a report showing that the Israeli company, NSO, had supplied cell phone hacking software to the Mexican, Saudi and Emirati governments, so they could spy on political opponents or overly curious journalists.[107] Israeli technology would subsequently be the source of authoritarian countries' domestic cyberpower.[108]

The scandals do not only affect Israeli companies. People, whose status swings between privateer and hacker, publicly provide IT solutions for spying. T. Dillian, a former Intelligence Office, was arrested in Cyprus[109] for promoting his commercial vehicle in an astonishing video[110] and having toured the country. This vehicle contained US $ 9 million worth of equipment to listen to individual conversations within a radius of 500 meters.

The impression left by this type of business is that the Israeli ecosystem is very mixed. An entire range of actors exist side by side, ranging from the military and classic entrepreneur through to the privateer or hacker, that can play their own role. They blur the image that Israel wants to project on the international stage[111]. However, they do not deny their origin and can contribute to their country's security when needed.

[106] H. Shezaf and J. Jacobson, "Revealed: Israel's Cyber-Spy Industry Helps World Dictators Hunt Dissidents and Gays", *Haaretz*, October 20, 2018.

[107] Telephone conversations of well-known people, such as A. Mansoor, J. Khashoggi or J. Bezos were reportedly listened to. Qatar, Mozambique, Morocco, Yemen, Hungary, Nigeria or Bahrain are also reported to be NSO's clients. Cf. B. Marczak, J. Scott-Railton, S. McKune, B. Abdul Razzak and R. Deibert, "Hide And Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries", *The Citizen Lab*, September 18, 2018, available at: https://tspace.library.utoronto.ca.

[108] Although NSO has asserted its right to do so and democratic intentions, NGOs have taken legal action to ban exports of surveillance software. They were unsuccessful. At the same time, the sale of spyware to Middle Eastern states by British companies was made public, also drawing criticism from NGOs. Competition between cybersecurity companies continues to rage. Cf. T. McMullan, "Israel's Silent Cyberpower Is Reshaping the Middle East", *OneZero*, April 16, 2019, available at: https://onezero.medium.com ; "Israel Court Refuses to Stop Spyware Exports to 'Rights Abusers'", *Middle East Monitor*, July 14, 2020, available at: www.middleeastmonitor.com.

[109] T. Staff, "Israeli Spy-Tech CEO Wanted for Questioning by Cypriot Police", *The Times of Israel*, December 23, 2019, available at: www.timesofisrael.com.

[110] "Multimillionaire Surveillance Dealer and His $9 Million WhatsApp Hacking Van", *Forbes*, available at: www.youtube.com.

[111] The police novel by D. Alfon, a former correspondent for *Haaretz* in Paris, called *Unit 8200* is a fictional account of this. Cf. D. Alfon, *Unité 8200 [Unit 8200]*, Paris: Liana Levi, 2019.

A difficult double role

Israel's international role does not just worry the NGOs. The United States is also worried by Tel Aviv and Beijing's rapprochement[112] and, to a lesser extent, with Moscow. They are surprised by the Israeli prime minister's office's high level of commitment on this issue and wonder about the effects of Chinese lobbying. Furthermore, they are aware of the close links between companies and the Chinese government and know that the opportunities to spy on US interests locally will be taken. The companies, ZTE or Huawei, that embody this closeness between the public and private sectors, have been increasingly investing in Israel.[113]

Above all, Washington fears that its policy of decoupling from China will be seriously weakened.[114] The aim is to prevent Beijing from benefiting from American innovation in the high-tech sector by minimizing relations between the two countries' companies as much as possible. The relatively lax export control policy could be a problem, allowing technology transfer, particularly in the dual technology sector.[115] Chinese companies could catch up more easily.

President Donald Trump explained that the security relationship between Washington and Tel Aviv could be weakened if links with Beijing increased. The Secretary of State, Mike Pompeo, also emphasized the risks that this policy poses to intelligence-sharing between the two countries.[116]

Tel Aviv may try to push for further cooperation with Beijing, but it will never jeopardize its alliance with the United States. It is aware of the value of this alliance.[117] The United States is Israel's main trading partner. It supports the IDF financially and contributes approximately 3% to Israel's budget. It argues Israel's case in major international institutions

[112] "Chinese Investment in Israeli Technology and Infrastructure: Security Implications for Israel and the United States", *op. cit.*

[113] *Ibid.*, pp. 69-73. The port infrastructure of Haifa or Ashdod where American ships participating in sensitive military ballistic defense exercises dock, are also repaired by Chinese companies, that can easily exploit this advantageous position to penetrate the IT networks of US ships.

[114] M. Schuman, "Think It's Too Hard to Decouple From China? Think Again", *Bloomberg*, July 15, 2020, available at: www.bloomberg.com.

[115] Chinese Investment in Israeli Technology and Infrastructure: Security Implications for Israel and the United State, *op. cit.*, pp. 23-33.

[116] *Ibid.*, p. 23.

[117] É. Brasi, É. Laurençon and P. Nouma Anaba, *Israël, le 6^e GAFAM?*, *op. cit.*, pp. 16-23. Both countries also signed a cooperation agreement in 2016 in the field of cyberdefense, in particular the cyberdefense of critical infrastructure and the development of partnerships in the private sector. Cf. Israel Ministry of Foreign Affairs, *Israel and the US Sign Operative Cyber Defense Cooperation Agreement*, June 21, 2016, available at: https://mfa.gov.il.

like the United Nations (UN). Israel would not be able to regain support from this power on the international stage.

The choice of operators, scheduled for September 2020, for the roll-out of the 5G network could serve as an initial test. Chinese companies are not likely to be selected.[118] Israeli telecommunication networks do not currently have any Chinese components and this is expected to be maintained. This decision should significantly help to address American concerns.

The opportunities provided by the success of Israel's digital industry, are reshuffling the cards of its traditional diplomacy, that has to accommodate negative externalities in terms of prestige or alliance. Depending on its exports, Tel Aviv will have to find and then tread a fine line between economic performance and diplomatic stability. This is the price it pays to be able to maintain the integrity of its power.

The future: the effects of the Coronavirus crisis

The long-term effects of the COVID crisis are still difficult to estimate. The shock was initially severe for the Israeli economy. Growth in GDP fell by 7.1% in the first quarter of 2020 and the unemployment rate exceeded 25% in April.[119] Young start-ups were particularly affected.[120] An opinion poll found that 65% of them thought that they would be bankrupt in the next six months. They are having difficulty in raising money or concluding contracts.[121]

However, due to its strengths, the sector is showing its dynamism. Employees continue to work from home and the virus is creating high demand for e-medicine solutions. Cybersecurity companies are asked to deal with attacks, and Check Point is continuing with its recruitment.[122]

Benefiting from financial investors' confidence, start-ups are finally raising more capital in the second quarter of 2020 than in 2019 in the same period.[123] The government also states that it is releasing US $ 13 million for

[118] H. Segev, "The 5G Tender in Israel and the Global Struggle Against Huawei", *INSS Insight*, No. 1347, July 14, 2020, available at: www.inss.org.il.

[119] Or the sharpest decline in 20 years. Cf. "Économie israélienne", *op. cit.*

[120] La Tribune with AFP, "Dans la "Startup Nation", 65% des petites start-ups pourraient sombrer suite à la crise du COVID-19", *La Tribune*, June 1st, 2020, available at: www.latribune.fr.

[121] P. Quinebeche, "L'impact du COVID-19 sur l'économie israélienne. Point de situation au 30 avril", *Direction générale du Trésor*, April 30, 2020, available at: www.tresor.economie.gouv.fr.

[122] *Ibid.*

[123] D. Rosenberg, "Israel Can Cure Mass Coronavirus Unemployment", *Haaretz*, August 4, 2020, available at: www.haaretz.com.

R&D[124] and US $ 190 million will be granted as initial assistance to small and medium enterprises.[125] Finally, US $ 12.5 million in assistance is being granted to companies seeking solutions to stem the epidemic.[126] In the long run, the sector could become even stronger as a result of the crisis.

[124] G. Press, "Israeli Startups Joins the Fight Against Coronavirus", *Forbes*, March 18, 2020, available at: www.forbes.com.

[125] More information available at: https://startupgenome.com.

[126] "Économie israélienne", *art. cit.*

Conclusion

Israel wages war and is made by war. The importance of this military fact in the foundation and life of this state is such that it has left its mark on several generations of Israelis. With varying degrees of success depending on the conflict, the Israelis have managed to show ingenuity in the face of their opponents, take risks and utilize the latest technology by drawing on an advanced university network to compensate for their low numbers and maintain an innovation culture.

Israeli leaders have harnessed this energy and built an ecosystem to master cyberspace, an artificial environment that permeates the life of all inhabitants in the developed world. They have managed to attract foreign capital, keen to benefit from the local innovative mindset that has become a high point of cyberspace. Entrepreneurs have set out to conquer new markets, exported their solutions, often sold their companies and made money that sustains a virtuous circle that the COVID-19 crisis could further stimulate.

However, Israeli cyberpower is undergoing a growth crisis that makes sense given its rapid growth. New challenges lie ahead. It needs to learn to spread the benefits to other sectors of society and to explore other development models. Israeli cyberpower must also succeed in growing without encroaching upon the power of its traditional allies or challenging the values it is founded on, or it risks seeing its already very diverse identity, being diluted even further. It must also know its limits, so as to not exceed them or to reinvent itself.

The development of Israeli cyberpower recalls, in broad terms, the beginnings of English naval power. In the 16th century, England was a minor actor compared to Spain and Portugal, that had already set out to conquer the world. However, it supported semiprivate, semistate actors, like Francis Drake, to develop its navy and set out to conquer the world. The ability of its sailors to master technical changes and tactics ensured their military superiority of the oceans. Soon, it had much control over coastlines around the world that ensured its fortune. Israel's destiny will certainly be different. However, its new power could also take it very far from its original territory.

since
1979

French Institute
of International
Relations