Flash Report

Repression Diplomacy: The Israeli Cyber Industry

June 2021

EXECUTIVE SUMMARY

A major surveillance exporter, Israel is a key player in the fast growing global market for cybersecurity products. In 2020, Israeli cyber firms received approximately 31% of global investment in the sector, acquisitions of Israeli cyber companies generated some US$4.7 billion, and Israeli cyber exports stood at US$6.85 billion.[1]

The Israeli cyber industry is characterized by strong reciprocal ties between industry, military, academia and government. Through the military and state-owned military industries, public research and academic institutions and various government arms, the state assumes much of the cost of human capital development.

The Israeli government funnels hundreds of millions of dollars into supporting, funding and coordinating industrial and academic research and development (R&D) and promoting the Israeli cyber industry internationally. In recent years, Israel has signed cooperation agreements in the field of cyber with over 90 states and international organizations.[2] Through research partnerships, Israeli universities play a major role in facilitating connections between the Israeli industry and the rest of the world. Israeli scientists and companies participate in EU Framework Programmes projects such as FP7, Horizon 2020 and Horizon Europe. Under FP7 (2007-2013) alone, Israeli entities received over US$1.06 billion in grants and gained over US$2.4 billion in value of knowledge (IP).[3]

Unit 8200, the Israeli military's signal intelligence unit, is the main body responsible for Israeli cyber offense. According to 8200 veterans, the unit's intelligence is used for political persecution and to create divisions within Palestinian society in the occupied Palestinian territory (oPt).[4] But Unit 8200 also functions as a conveyer belt for the Israeli high-tech industry, which benefits from the commercialization of military knowledge, sanitized of its origins in Israel's ongoing colonial domination of the Palestinian people. Over the years, 8200 veterans have founded over 1,000 companies, including Checkpoint Software Technologies, NICE Systems, Palo Alto Networks, and Cyber Ark.[5]

Cyber exports are the latest chapter in Israel's long and lethal history of exporting repressive technologies to authoritarian regimes for economic and diplomatic gains. Business and economic ties reinforce, and at times pave the way for diplomatic relations and international cooperation, as can be seen in the recent normalization of political and economic relations between Israel and the United Arab Emirates (UAE).

According to journalists, researchers and human rights activists, Israeli cyber products have been used by repressive governments to track and detain activists, persecute LGBT people and silence political dissent. Though Israel formally adheres to export controls on dual-use items regulated under the Wassenaar Arrangement, it does not publicly disclose information on export licenses to specific companies or general licensing policies,

1 The Israeli cyber industry continues to grow: record fundraising in 2020, Israel National Cyber Directorate, 21 January 2021. Accessed 10 May 2021.

2 Annual report 2019-2020, (Hebrew) Israel National Cyber Directorate, 27 October 2020. Accessed 10 May 2021.

3 Goldschmidt, R., Participation of the State of Israel in the Research and Development Framework Programme of the European Union, (Hebrew) The Knesset Research and Information Center, 6 February 2014.

4 Israeli intelligence veterans' letter to Netanyahu and military chiefs - in full, *The Guardian,* 12 September 2014.

5 Shezaf, H. and Jackobson, J., Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays, *Haaretz*, 20 October 2018.

undercutting prospects of accountability.[6]

INTRODUCTION

Israel's cybersecurity industry is part of a booming global industry that pledges to "secure your everything," as one industry leader put it.[7] Cyber technologies increasingly saturate practically all spheres of economic and social activity. Whereas many industries were hard hit by the Covid-19 pandemic, the global cybersecurity industry saw a rise in demand as individuals, businesses, and public agencies shifted their activities to the digital sphere. Broadly speaking, the market for the industry has expanded significantly in recent years; rising from US$71 billion in 2014[8] to US$126 billion in 2020[9]. It is projected to continue to grow substantially in the coming years, exceeding US$207 billion by 2024.[10]

Governments worldwide are also increasingly preoccupied with developing their cyber capabilities. As cyber warfare becomes an integral part of, and occasional substitute for traditional warfare, states are engaging in an ever-intensifying cyber arms race. Cyber technologies such as computer interference, phone hacking, and network surveillance are also increasingly utilized by repressive regimes to monitor and surveil their own populations, target political dissidents, and suppress popular mobilizations. Such surveillance has been shown to lead to arbitrary detention, torture, and possibly to extrajudicial killings.[11]

It is within this context that Israel, a major surveillance and security exporter and close ally of the United States, has positioned itself as a key player. Israel considers cyber to not only be an important driver of economic growth, but also a key trade commodity that can be leveraged to achieve political objectives, and to secure and advance its international position.

Leveraging trade for political ends is not unique to Israel, nor to cyber products. This has historically been the case with Israeli exports of agricultural technology to Central American dictatorships,[12] and remains powerfully so for Israel's extensive global arms exports.[13] However, the meteoric rise of the Israeli cyber industry over the past decade has made it one of the top trade commodities through which Israel builds its global power. The combined value of Israeli defensive and offensive cyber exports is estimated at US$10 billion a year, exceeding the total value of Israeli military exports.[14] The ubiquity of cyber in the digital age, and the ease with which it can be used by those in power for targeted and mass surveillance makes it strategically valuable to states while posing a major threat to individuals and communities.

As this report shows, the rise of Israel's cyber

6 UN Human Rights Council, Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 28 May 2019, A/HRC/41/35.
7 Check Point Software Technologies Form 20-F for the fiscal year ended December 31, 2019 , p. 20.
8 Tsipori, T., Israeli cybersecurity grabs 8% global market share, *Globes*, 4 April 2016.
9 Mena-Kalil, A. and Barel Handeli, A., An investment guide to cyber: Which companies should be included, (Hebrew) *Globes*, 7 January 2021.
10 Forecast: Information Security and Risk Management, Worldwide, 2018-2024, 2Q20 Update, Gartner Research, 28 July 2020.
11 UN Human Rights Council, Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 28 May 2019, A/HRC/41/35.
12 Rubenberg, Cheryl A., "Israeli foreign policy in Central America," Third World Quarterly 8.3 (1986): 896-915.
13 Halper, J., (2015) *War against the People: Israel, the Palestinians and Global Pacification*. London: Pluto Press.
14 Limor, Y., Cyber King: The next generation of defense of the land, (Hebrew) *Israel Hayom*, 10 September 2020.

industry is not the product of the invisible hand of the market. Characterized by strong reciprocal ties between industry, military, academia and government, the cyber sector has been shaped by Israel's development as a settler colonial project and an occupying military power. The private sector benefits, not only from extensive government support, foreign investment, and state funded military and academic R&D, but also from the commercialization of military knowledge developed in the context of a prolonged and belligerent military occupation. Moreover, it benefits from the market value generated by Israel's reputation for military and security know-how, sanitized of the ongoing colonial domination of the Palestinian people.

The state benefits from the commercial success of the Israeli cyber industry in economic terms[15] through the creation of high-paying jobs and taxation on company exits in the form of Initial Public Offerings (IPO) and Mergers and Acquisitions (M&A). It also benefits in political terms, as business and economic ties reinforce, and at times pave the way for diplomatic relations and international cooperation. The recent normalization of political and economic relations between Israel and the UAE provides an instructive case study for examining the role of cyber within broader economic and political dynamics.

In the sections that follow, Who Profits sheds light on Israel's cybersecurity industry, including the role of the military and military industries, government agencies and academic institutions in the production and marketing of cyber technologies, and examines the ways cyber is mobilized by the state to enhance Israel's political power, focusing on the UAE as a case study.

The report is based on the collection and analysis of information from various public sources, such as publications by state authorities (including Israeli government ministries), industry reports, company publications and newspapers and other media sources.

THE ISRAELI CYBERSECURITY INDUSTRY

The high-tech industry is one of the main growth engines of the Israeli economy. In 2020, it attracted US$10.2 billion worth of investment through 607 deals[16] and accounted for 43% of all Israeli exports.[17] On average, high-tech contributes to around 12% of Israel's GDP.[18] As of the end of 2019, some 321,000 workers, representing about 9.2% of all Israeli employees, were employed in high-tech.[19]

It is a highly globalized industry, dominated by foreign investors and the strong presence of multinationals. In 2020, there were 387 active multinational corporations operating in Israel with a workforce of approximately 68,000 people.[20] The majority of multina-

15 It should be noted that high-tech is a major driver of inequality within Israeli society and that economic benefits do not trickle down to the general population. For a critical discussion of Israeli high tech see: Getzoff, Joseph F. Start-up nationalism: The rationalities of neoliberal Zionism. *Environment and Planning D: Society and Space* 38.5 (2020): 811-828.

16 The Israeli Tech Review 2020. IVC Research Center and Meitar Law Offices, January 2021.

17 Israeli innovation globally, (Hebrew) Israel Innovation Authority. Accessed 10 May 2021.

18 Getz, D., Buchnik, Z. and Zatcovetsky, I., Metrics for science, technology and innovation in Israel: Data infrastructure. Final report - Year II, (Hebrew) Samuel Neaman Institute for National Policy Research. November 2018.

19 2019 High-Tech Human Capital Report, Israel Innovation Authority, 26 February 2020. Accessed 10 May 2021.

20 Multinational Corporations Contribution to the Israeli Tech Ecosystem, Review by IVC Research Center. IVC Research Center and Israel Advanced Tech-

tionals are US-based (60%), followed by Germany, the UK, China, and Japan.[21] Venture Capital (VC) is the main source of capital for Israeli tech, accounting for 88% of all capital raised by the industry in 2020.[22] VC investors are overwhelmingly foreign, making up 85% of all VC investment. A breakdown of all capital investments in Israeli high-tech between 2013 and 2018 by region showed that most capital came from the US (35%), followed by Israel (30%), China (4%), Germany (3%), the UK (3%), and Canada (2%).[23] US buyers also dominate the M&A of Israeli companies; with a total value of US$7 billion in high-tech M&A compared with US$480 million by Israeli acquirers in 2020.[24]

Foreign funding also plays an important part in supporting Israeli technological innovation. In 2011, 47% of gross domestic expenditure on R&D (GERD) in Israel was financed from abroad, compared with 28% in 2007.[25] Expenditure on R&D in multinational companies in Israel in terms of percentage of yields stands at 17%, compared with 1.7% in the US.[26] In 2012, 37% of patents on Israeli innovation were foreign-owned.[27]

Within the Israeli high-tech industry, cybersecurity is a prominent sub-field, accounting for 30% of all capital raised by the industry in 2020.[28] According to a 2019 report by the IVC Research Center, there are some 421 active cyber companies in Israel, 15% of whom are engaged in information protection, 9% in network security and 7% in cyber intelligence, a comparatively high figure.[29] At the end of 2018 about 20,500 workers were employed in the Israeli cyber sector, approximately half of them in start-up companies, 4,500 in foreign R&D centers and 5,900 in the public sector.[30]

> The number of cyber companies operating in Israel more than doubled between 2010 and 2019 and the amount of private capital raised by the industry increased by 2,300%. In 2020, Israeli cyber companies received approximately 31% of global investment in the sector and exports stood at US$6.85 billion.

The value of gross domestic product from Israeli employees working in the cyber R&D centers of multinationals located in Israel amounted to US$900 million in 2017.[31]

The cyber industry has expanded dramatically since 2010. The number of cyber companies operating in Israel more than doubled between 2010 and 2019, the amount of private capital raised by the industry increased by 2,300%, and cyber companies accounted for

nology Industry, December 2020. Accessed 10 May 2021.

21 Multinational Corporations Contribution to the Israeli Tech Ecosystem, Review by IVC Research Center. December 2020, IVC Research Center and Israel Advanced Technology Industry. Accessed 10 May 2021.

22 The Israeli Tech Review 2020. IVC Research Center and Meitar Law Offices, January 2021.

23 Foreign High-Tech Activity in Israel: Facts & Figures 2018, IVC Research Center, November 2018.

24 The Israeli Tech Review 2020. IVC Research Center and Meitar Law Offices, January 2021.

25 Tabansky, L. and Ben Israel, I. *Cybersecurity in Israel*. Vol. 598. New York: Springer, 2015.

26 High Tech in Israel.

27 High Tech in Israel.

28 Ziv, A., 2020 was a record year for Israeli cyber - and 2021 may break it, (Hebrew) *TheMarker*, 21 January 2021.

29 A new report: the Israeli cyber industry jumps - raised 4 billion dollars in the last five years, (Hebrew) Israel National Cyber Directorate. 23 June 2019. Accessed 10 May 2021.

30 Ibid.

31 Ibid.

15% of all Israeli high-tech acquisitions, totaling US$10 billion.[32] Between 2011 and 2019, cyber exports increased by 600%, reaching US$6.5 billion in 2019.[33]

The industry continued to experience record breaking growth in 2020. Israeli cyber companies received approximately 31% of global investment in the sector, compared with 22% the previous year.[34] Cyber exports stood at US$6.85 billion, accounting for approximately 11% of all global cyber sales.[35] Israeli cyber companies raised US$2.9 billion through over 100 deals, a 70% increase compared to 2019.[36] Over 20 acquisitions of Israeli cyber companies were made at an estimated US$4.7 billion. These included the acquisition of Checkmarx by Hellman & Friedman for US$1.15 billion, Armis by CapitalG for US$1.1 billion, and CyberX by Microsoft for US$165 million.[37]

THE PUBLIC PILLARS OF PRIVATE INDUSTRY

Israel's emergence as a leading global purveyor of cyber technologies is not the result of invisible market forces, but is rather the outcome of Israel's particular development as a settler colonial project, and an occupying military power.

The Israeli state actively supports the high-tech industry, and cyber tech in particular, through tax exemptions, grants, subsidies, and liberalized export and licensing policies. Through the Israel Innovation Authority, it invests about NIS 1.5 billion annually in high-tech companies in the form of grants and exempts them from taxes through the Law for the Encouragement of Capital Investments.[38]

Moreover, through the military and state-owned military industries, public research and academic institutions and various government arms, the state assumes much of the cost of human capital development and R&D. In particular, Israel's prolific cyber industry owes much of its existence to the role played by the military sector in shaping the Israeli high-tech sector and incubating tech entrepreneurship. Academia and government also promote the industry through joint research collaborations and international partnerships.

> While the so-called "Israeli experience" of deploying security technologies looms large in the corporate and state marketing of Israeli cyber, the political realities in which it is grounded are obscured.

32 2019 in the cyber industry - Summary of the year and the decade, (Hebrew) Israel National Cyber Directorate, 27 January 2020. Accessed 10 May 2021.
33 Ibid.
34 Ibid. The Israeli cyber industry continues to grow: record fundraising in 2020, Israel National Cyber Directorate, 21 January 2021. Accessed 10 May 2021.
35 Ziv, A. 2020 was a record year for Israeli cyber - and 2021 may break it, (Hebrew) *TheMarker*, 21 January 2021.
36 The Israeli cyber industry continues to grow: record fundraising in 2020, Israel National Cyber Directorate, 21 January 2021. Accessed 10 May 2021.
37 The Israeli Tech Review 2020. IVC Research Center and Meitar Law Offices, January 2021.

38 Naftali, Y., High tech is the growth engine of the economy - but there are no compartments attached, (Hebrew) *TheMarker*. 16 September 2018.

REVOLVING DOORS: Military Intelligence and Cyber Innovation

A central pillar of Israeli cyber innovation is the Israeli military, portrayed in the promotional literature of Israeli cyber companies and government officials as an incubator for cybersecurity talent, an unfailing source of eager young minds equipped with hands-on experience, networking skills, and technical know-how. As Joseph Getzoff recently observed, in the discourse on Israeli tech, "military service is hardly about military endeavors at all, but instead serves as a training course for aspiring start-up entrepreneurs."[39] While the so-called "Israeli experience"[40] of deploying security technologies looms large in the corporate and state marketing of Israeli cyber, the political realities in which it is grounded are obscured. Conspicuously absent are those on the receiving end of Israel's military-industrial complex, the Palestinians living under Israel's prolonged military occupation and siege.

The Israeli military operates in the cyber domain through two units: C4I Directorate and Unit 8200. C4I, which operates under the military's Computer Service Directorate, is responsible for network security within the Israeli military, as well as for the development of ICT systems infrastructure, software, and cryptographic foundations for the military.[41] Unit 8200, the Military Intelligence Directorate's signal intelligence collection and code decryption unit, carries out offensive cyber operations.[42] According to international sources, the unit participated in major cyberattacks involving espionage and sabotage of industrial facilities, the best known of which is Stuxnet, a digital malware developed jointly with the US National Security Agency (NSA) which targeted Iranian nuclear facilities.[43] Stuxnet is considered by some to be the world's first cyber weapon.[44]

Israeli military intelligence has long played a major role in maintaining military and political control over the occupied Palestinian population. In a 2014 open letter to the Israeli Prime Minister and military chiefs, intelligence veterans stated that Palestinians in the oPt are "completely exposed" to Israeli surveillance, and that intelligence gathered by Unit 8200 is used "for political persecution and to create divisions within Palestinian society by recruiting collaborators and driving parts of Palestinian society against itself."[45] The unit also has its own combat division, which is involved in military operations in the oPt and the occupied Syrian Golan. Combat intelligence soldiers were reportedly involved in a third of the mass arrests carried out by the Israeli military in the occupied West Bank during the summer of 2014.[46] Unit 8200 accounts for

39 Getzoff, Joseph F. Start-up nationalism: The rationalities of neoliberal Zionism. *Environment and Planning D: Society and Space* 38.5 (2020): 811-828.

40 See Gordon, N. The Political Economy of Israel's Homeland Security. 2009.

41 Tabansky, L. Israel Defense Forces and National Cyber Defense. *Connections* 19.1 (2020): 45-62.

42 Cordey, S., The Israeli Unit 8200–An OSINT-based study: Trend Analysis, ETH Zurich, 2019.

43 Frei, J., Israel's National Cybersecurity and Cyberdefense Posture: Policy and Organizations, ETH Zurich, 2020. Tabansky, L. Israel Defense Forces and National Cyber Defense. *Connections* 19.1 (2020): 45-62. Other suspected Israeli military cyber operations include Flame, a cyberespionage malware with targets in Israel, the oPt and Iran, and Duqu, which targeted industrial systems in a dozen countries.

44 Franceschi-Bicchierai, L., The History of Stuxnet: The World's First True Cyberweapon, *Motherboard: Tech by Vice*, 9 August 2016.

45 Israeli intelligence veterans' letter to Netanyahu and military chiefs - in full, *The Guardian*, 12 September 2014.

46 Ofer, Y., 8200 combatants reveal: This is how we assassinated terrorists in Pillar of Defense, (Hebrew) *Makor Rishon*, 8 October 2014.

> Unit 8200 also functions as a training ground and conveyer belt for the Israeli tech industry. Over the years, 8200 veterans have founded over 1,000 companies, including Checkpoint Software Technologies, NICE Systems, Palo Alto Networks, and Cyber Ark.

some 90% of all intelligence material collected in Israel, meaning it is involved in virtually all major operations of the Mossad and the Shin Bet.[47]

The significance of Unit 8200, however, is not limited to its role in military operations. The unit also functions as a training ground and conveyer belt for the Israeli tech industry.[48] With at least 5,000 soldiers on active duty, 8200 is the largest unit in the Israeli military. An average service time of four years ensures a continuous flow of veterans who are both highly skilled and in high demand by the private sector. Over the years, 8200 veterans have founded over 1,000 companies, including Checkpoint Software Technologies, NICE Systems, Palo Alto Networks, and Cyber Ark.[49] One study found that of 2,300 Israelis who founded 700 Israeli cyber firms, 80% were graduates of Unit 8200.[50]

Other technological units of the Israeli military also funnel human capital and military know-how into the private sector. For instance, veterans of Lotem, a C4I unit responsible for introducing advanced technology into the Israeli military's combat operations, made over NIS3 billion in exits over a period of five years.[51]

Unit 8200 also acts as an incubator for tech entrepreneurship, investing in projects developed by soldiers in the unit. Such is the case of former 8200 captain Barak Perelman, founder of the cybersecurity start-up Indegy, which specializes in critical infrastructure protection. According to Forbes, in order to retain Perelman in the unit, his superiors agreed to invest manpower in an innovation project he developed, a situation Perelman referred to as "'a win-win'".[52] Perelman's Indegy was later sold to the US-based company Tenable, which opened an Israeli office based on that acquisition.[53]

The Israeli Ministry of Defense, the Directorate for Defense R&D (DDR&D), and the air and ground forces of the Israeli military, together with iHLS Startup Accelerator also launched INNOFENSE – a start-up accelerator for dual-use technological projects in the civilian and military sectors.[54]

Since intelligence veterans, like all Israeli veterans, continue to serve as reserve soldiers into their early forties; they maintain continual privileged access to technological developments within the military, as well as to new

47 Behar, R., Inside Israel's Secret Startup Machine, *Forbes*, 11 May 2016.
48 Gordon, N. The Political Economy of Israel's Homeland Security. 2009.
49 The hi-tech industry in Israel, Invest in Israel, Israeli Ministry of Economy and Industry, 2017, p. 23. Choudhury, S. R., Former cyber-intelligence sleuths for Israel now work to uncover malicious hackers, *CNBC*, 11 May 2017.
50 Shezaf, H. and Jackobson, J., Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays, *Haaretz*, 20 October 2018.
51 Five facts about Lotem Unit, Israel Defense Forces [sic]. Accessed 10 May 2021.
52 Behar, R., Inside Israel's Secret Startup Machine, *Forbes*, 11 May 2016.
53 Zerachovit, O., US co Tenable buys Israeli cybersecurity startup Indegy, *Globes*, 3 December 2019.
54 iHLS INNOFENSE, iHLS Startups Accelerator. Accessed 10 May 2021.

talent for recruitment. Some are retained in their units as technicians or developers, becoming conduits between the private sector, the military and academia.[55]

IN THE PURSUIT OF KNOWLEDGE: The Role of Academia and Civilian R&D

Israeli public research universities are also deeply involved in the militarized character of Israel's human capital development through the Academic Reserves (*Atuda*) and *Talpiot* programs. The Academic Reserves track enables high school students to complete a university degree before enlisting in the military. Graduates then serve in positions that utilize their academic training, typically extending their compulsory service by three to five years while receiving a full salary and benefits.[56] *Talpiot* is an elite 40-month training program run by the DDR&D.[57] Both programs have a considerable spillover effect over Israel's cyber industry, with hundreds of trained engineers, scientists and programmers entering the workforce each year.

Additionally, state military R&D, which is estimated at 1.5% of Israel's GDP, is frequently carried out in civilian research facilities. Israeli academic institutions are involved in military R&D projects coordinated by the DDR&D, alongside the military and military industries.[58]

Through their international research partnerships and cooperation agreements, Israeli universities also facilitate connections between Israeli industry and the rest of the world. In 2011, the Technion – Israel Institute of Technology and Cornell University consortium won an international competition to establish an applied science campus in New York City.[59] Tel Aviv University and Tsinghua University in Beijing signed an agreement to invest US$300 million in a joint nanotechnologies research project through a newly established center.[60] The Technion also developed a technological school in China with the Guangdong Province Government, the Shantou Municipal Government and Shantou University.[61]

In 1996, Israel joined the European Framework Programme for Research and Technological Development as the only non-European member. Israel regards this partnership as the "flagship of Israel-EU relations,"[62] enabling Israeli entities to establish research and business ties with European institutions,

> Israeli public research universities are deeply involved in the militarized character of Israel's human capital development through the Academic Reserves (Atuda) and Talpiot programs. Through their international research partnerships and cooperation agreements, they also facilitate connections between Israeli industry and the rest of the world.

55 Tabansky, L. and Ben Israel, I. *Cybersecurity in Israel*. Vol. 598. New York: Springer, 2015.
56 Ibid.
57 Ibid.
58 Ibid.
59 Cornell wins NYC Tech Campus bid, *Cornell Chronicle*, 19 December 2011. The proposal included a strong industry component, including legal support for start-ups, pre-seed financing programs, and an on-site tech transfer office structured to facilitate start-up formation and technology licensing.
60 Tabansky, L. and Ben Israel, I. *Cybersecurity in Israel.* Vol. 598. New York: Springer, 2015.
61 Ibid.
62 Innovation in Israel: A snapshot, (Hebrew) Israel Innovation Authority (formerly Office of the Chief Scientist). 2015, p. 34.

companies and clients. The Israel-Europe Research & Innovation Directorate (ISERD), an inter-ministerial directorate operated through the Israel Innovation Authority, is the National Contact Point for Israeli participation in the Framework Programme. It is also responsible for promoting Israeli participation in bilateral and multilateral research collaborations with European states.

As part of the EU's FP7, Israeli bodies participated in projects with an overall budget of US$12 billion, and the estimated value of knowledge (IP) gained by the Israeli industry through its participation in FP7 projects exceeds US$2.4 billion.

As part of the EU's Seventh Framework Programme (FP7), which lasted from 2007 to 2013, Israeli entities received over US$1.06 billion in grants, 63% more than Israel invested in FP7.[63] Israeli bodies participated in projects with an overall budget of US$12 billion, and the estimated value of knowledge (IP) gained by the Israeli industry through its participation in FP7 projects exceeds US$2.4 billion.[64] In 2014, Israel joined Horizon 2020, the EU program that succeeded FP7. Between 2014 and the first half of 2017, Israeli participants were awarded US$597 million in grants.[65]

Israeli cyber researchers and companies are among the beneficiaries of such international funding programs. The Cyber Division of ELTA Systems, a subsidiary of the state owned Israel Aerospace Industries (IAI), is the only non-European member of the Hermeneut consortium, a Horizon 2020 cyber risk assessment project.[66] Israeli cyber firm Odix was awarded a US$2.4 million grant in 2019 in the framework of Horizon 2020.[67] Incidentally, Odix was founded by two Israeli military veterans, Oren Eitan, former commander of the Center of Encryption and Information Security (*Matzov*) and Dudu Geva, former commander of the C4I's School of Communications, ICT and Cyber (*Bahad 7*).[68] Another example is the state-owned Israel Electric Company (IEC), which participated in several international projects on cybersecurity and Industrial Controls Systems (ICS) security under the framework of FP7 and Horizon 2020.[69]

63 Israel, Annexation, and the EU's Research and Development Program "Horizon", Mitvim – The Israeli Institute for Regional Foreign Policies, July 2020. Accessed 10 May 2021.

64 Goldschmidt, R., Participation of the State of Israel in the Research and Development Framework Programme of the European Union, (Hebrew) The Knesset Research and Information Center, 6 February 2014.

65 Honoring Israeli companies that won Horizon 2020 grants, Israeli Ministry of Science and Technology, 22 March 2018. Accessed 10 May 2021.

66 Hermeneut – Horizon 2020 Consortium Cyber Risk Assessment for Intangible Assets, Israel Aerospace Industries. Accessed 10 May 2021.

67 Orbach, M. Former Matzov commander's Odix raised $2.1 million, (Hebrew) Calcalist, 4 March 2020.

68 Ibid.

69 Israel Electric Company reveals cyber activity data in anticipation of cybertech international cyber conference, (Hebrew) 22 March 2015. Accessed 10 May 2021.

A PORTAL FOR THE INDUSTRY: Government Support

Through the Israel National Cyber Directorate (INCD), the Israel Innovation Authority, the Israeli Ministry of Economy and Industry, the Cyber Unit of the Israel Export Institute, and Israeli embassies worldwide, the Israeli government funnels hundreds of millions of dollars into what it terms "capacity building" in cyber – building the technological and scientific backbone of its cyber power through supporting, funding and coordinating industrial and academic R&D and promoting the Israeli cyber industry internationally.

Formed from a 2017 merger between the National Cyber Security Authority and the Israel National Cyber Bureau,[70] the INCD is the chief governmental organ tasked with organizing cybersecurity in Israeli civilian cyberspace. It is one of only four bodies directly under the Prime Minister's Office, the other three being the Israel Security Agency (Shin Bet), the Institute for Intelligence and Special Operations (Mossad) and the Atomic Energy Committee. [71]The INCD developed out of the Shin Bet division for the protection of critical infrastructure and its current head, Yigal Una, is a former Shin Bet operative.[72]

The INCD serves as a "portal for the Israeli industry vis-à-vis international clients," marketing a "complete package of knowledge and strategic, regulatory and operational experience, together with technological and industrial solutions."[73] It operates a number of digital platforms for the industry to showcase its products and share knowledge, including *Cybernet*, an anonymous secure information exchange platform for sharing cyber threats; [74] *Showroom*, a risk exposure evaluation tool for organizations and recommends ways to minimize exposure; Marketplace, a platform launched specifically in response to the Covid-19 pandemic as a tool for Israeli cybersecurity vendors to present products and services,[75] and *Corona.net*, a system developed by Elta Systems based on *Cybernet*, which was presented by Israeli Prime Minister Binyamin Netanyahu during an international video conference on the second wave of the pandemic.[76]

Through the INCD, Israel has signed cooperation agreements in the field of cyber with over 90 states and international organizations.[77] These include a partnership with the Inter-American Development Bank (2016), trilateral and bilateral agreements with Greece and Cyprus (2018 and 2020), a memorandum of cooperation with Japan (2018), Memorandums of Understanding with Australia, Brazil, Croatia and Romania (2019), and operational cooperation agreements with India (2018 and 2020).[78] Agreements are frequently accom-

70 Government Resolution 3720, (Hebrew) Israeli Prime Minister's Office, 17 December 2017.

71 Frei, J., Israel's National Cybersecurity and Cyberdefense Posture: Policy and Organizations, ETH Zurich, 2020.

72 Limor, Y., Cyber King: The next generation of defense of the land, (Hebrew) *Israel Hayom*, 10 September 2020.

73 Annual report 2019-2020, (Hebrew) Israel National Cyber Directorate, 27 October 2020.

74 Cybernet - the world's first social network for information exchange on cyber-attacks, Israel National Cyber Directorate, 16 January 2020. Accessed 10 May 2021.

75 Participation in a 'Marketplace' of Cybersecurity Solutions for the Coronavirus Crisis, Israel National Cyber Directorate, 8 April 2020. Accessed 10 May 2021.

76 CoronaNet – a platform for sharing information between countries on the fight against the virus, Israel National Cyber Directorate, 12 November 2020. Accessed 10 May 2021.

77 Annual report 2019-2020, (Hebrew) Israel National Cyber Directorate, 27 October 2020. Israel National Cyber Directorate, 12 November 2020. Accessed 10 May 2021.

78 For the first time, cyber cooperation agreement in the Greece-Cyprus-Israel trilateral summit,

panied by commercial collaborations such as industry fairs,[79] business presentations[80] and private sector delegations organized by the Israeli Ministry of Economy and Industry.[81]

> Through the INCD, Israel has signed cooperation agreements in the field of cyber with over 90 states and international organizations. CyberSpark, Israel's flagship project for public-private cybersecurity collaboration, is home to several multinational companies, including Oracle, Lockheed Martin, IBM, Dell, and Deutsche Telekom.

The CyberSpark cyber innovation arena, an industrial park launched in 2014, is Israel's flagship project for public-private cybersecurity collaboration. Located in the city of Bir al-Saba (Beer Sheva) in the Naqab (Negev) region, it is home to the national Computer Emergency Response Team (CERT-IL), built by an industrial consortium led by the state-owned military corporation Rafael Advanced Defense Systems,[82] as well as to several sectoral CERTs (e.g. finance, telecommunications and energy). Several multinational companies, including Oracle, Lockheed Martin, IBM, Dell, and Deutsche Telekom have also established a presence in CyberSpark.[83]

The state encourages industry participation through initiatives such as government financed innovation arenas and laboratories,[84]

(Hebrew) Israel National Cyber Directorate, 20 December 2018. Accessed 10 May 2021. Joint statement on cybersecurity signed between Greece and Israel, Israel National Cyber Directorate, 16 June 2020. Israel National Cyber Directorate, 20 December 2018. Accessed 10 May 2021. For the first time, cooperation agreement for information exchanges and R&D collaborations in the field of cyber between Israel and Japan, Israel National Cyber Directorate, 29 November 2018. Accessed 10 May 2021. Israeli-Australian cooperation in the fields of cyber, Israel National Cyber Directorate, 29 January 2019. Accessed 10 May 2021. Schneider, T., Brazil and Israel signed a series of cooperation agreements today, (Hebrew) *Globes*, 31 March 2019. Memorandum of understanding for cooperation in the field of cyberdefense between Israel and Croatia, (Hebrew) Israel National Cyber Directorate, 12 September 2019. Accessed 10 May 2021. Memorandum of understanding for cooperation in the field of cyberdefense between Israel and Romania, (Hebrew) Israel National Cyber Directorate, 6 June 2019. Accessed 10 May 2021. India and Israel to expand cooperation in cyber, (Hebrew) Israel National Cyber Directorate, 27 October 2020. Accessed 10 May 2021.

79 For the first time, cyber cooperation agreement in the Greece-Cyprus-Israel trilateral summit, (Hebrew) Israel National Cyber Directorate, 20 December 2018. Accessed 10 May 2021.

80 Memorandum of understanding for cooperation in the field of cyberdefense between Israel and Romania, (Hebrew) Israel National Cyber Directorate, 6 June 2019. Accessed 10 May 2021.

81 Zened, L., Israel's cyber warriors enter Japan, (Hebrew). Ynet, 1 December 2017. For the first time: An Israeli cyber delegation visited India, (Hebrew) Israeli Ministry of Economy and Industry, 23 December 2019. Accessed 10 May 2021.

82 Tabansky, L., Israel Defense Forces and National Cyber Defense. *Connections* 19.1 (2020): 45-62.

83 Frei, J., Israel's National Cybersecurity and Cyberdefense Posture: Policy and Organizations, ETH Zurich, 2020. PayPal closed its office in Beer Sheva in 2017. Perlov, N. and Cohen, H., Case study: Gav Yam Negev High Tech Park, (Hebrew) Maoz Knowledge and Strategy Center, 4 November 2019.

84 CyberSpark includes a laboratory for testing industrial control systems, established by the INCD and Israeli Ministry of Energy, a cyber innovation arena for transportation to be built by the INCD and the Israeli Ministry of Transportation for NIS 18 million, and a fintech cyber laboratory to be built by a private consortium owned by MasterCard and Enel X with financing from the INCD, Israel Innovation Authority, and the Ministry of Finance for a concession period of 3 years. Fintech lab to be established in Beer Sheva, (Hebrew) Israel National Cyber Directorate, 4 May 2020. Accessed 10 May 2021. Innovation arena for cyberdefense in transport to be established in the Beer Sheva area, (Hebrew) Israel National Cyber Directorate, 20 December 2018. Accessed 10 May 2021. Melnitcki, G. A new cyber lab in Beer Sheva will test threats to

a cyber incubator supported by the Israel Innovation Authority, a tax incentivized R&D hub[85] and annual grants of NIS 13 to 20 million to incentivize employment in cyber in Bir al-Saba.[86] In 2019, the INCD hosted over 150 foreign delegations in the national CERT in CyberSpark.[87] The project is also meant to benefit from the planned relocation of the Israeli military intelligence and technological units to Bir al-Saba, set to be complete in 2026.[88]

REPRESSION DIPLOMACY: Israel's Global Cyber Ties

Israel has a long and lethal history of exporting repressive technologies to regimes guaranteed to put them to their worst possible use, reaping both economic and diplomatic profits in the process. Cyber exports are the latest chapter in this history.

Relying on 100 sources from 15 countries, a 2018 investigation by the Israeli newspaper Haaretz found that private Israeli firms sold cyber intelligence and espionage technologies to a long list of countries with human rights records that are patchy at best, including: Bahrain, Indonesia, Angola, Mozambique, the Dominican Republic, Azerbaijan, Swaziland, Botswana, Bangladesh, El Salvador, Panama, Nicaragua, Malaysia, Vietnam, Mexico, Uzbekistan, Kazakhstan, Ethiopia, South Sudan, Honduras, Trinidad and Tobago, Peru, Colombia, Uganda, Nigeria, Ecuador, and the UAE.[89] Some of the buyers were countries that do not have official diplomatic relations with Israel. According to testimonies, Israeli products enabled governments to track and detain activists, persecute LGBT people and silence political dissent.[90] Even when abuses were publicly revealed, Israeli companies did not halt the sale of espionage products.[91]

Human rights attorney Eitay Mack has argued that Israeli cyber firms should be seen as implementing state policy, and not merely following their private economic interests.[92] According to Mack; "Israel has so much military sensitivity" that cyberweapon sales are effectively "military agreements between governments."[93]

The United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression noted in a 2019 report that although Israel formally adheres to export controls on dual-use items regulated under the Wassenaar Arrangement, its enforcement of these controls is "shrouded in secrecy."[94] As Israel's Defense Export Controls Agency (DECA) does not publicly disclose information on export licenses granted to specific companies or on its general licensing policies, there is no real possibility of accountability.[95]

industrial control systems, (Hebrew) *TheMarker*, 9 January 2020.

85 Who we are, (Hebrew) Cyberspark Israeli Innovation Arena. Accessed 10 May 2021.

86 Annual report 2019-2020, (Hebrew) Israel National Cyber Directorate, 27 October 2020.

87 Annual report 2019-2020, (Hebrew) Israel National Cyber Directorate, 27 October 2020.

88 Gross, J. A., Mega-builder Shikun & Binui gets tender to build IDF intel complex in south, *Times of Israel*, 13 July 2020.

89 Shezaf, H. and Jackobson, J., Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays, *Haaretz*, 20 October 2018.

90 Ibid.

91 Ibid.

92 Barshad, A., Inside Israel's lucrative — and secretive —cybersurveillance industry, *Rest of the World*, 9 March 2021.

93 Ibid.

94 UN Human Rights Council, Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 28 May 2019, A/HRC/41/35.

95 Amnesty International, Amnesty International Affidavit in Support of Israeli Petition, 13 May 2019. ACT 10/0332/2019.

However, weak controls are the mechanism that enables Israeli global exports of cyber repression, not its raison d'être. Israel's disproportionate share in supplying authoritarian governments is best understood as rooted in and stemming from its interests as a settler colonial state. Israel's decades-old oppression of the Palestinian people, military occupation, apartheid policies, and denial of the right of return of Palestinian refugees have given it a vested interest in global repression; both to normalize its own regime and to rally international support for, or at least tacit acceptance of, its ongoing policies of repression.

THE NEW NORMAL: Cybersecurity and Israel-UAE Normalization

The Trump-brokered normalization agreements signed between Israel, the UAE, and Bahrain in September 2020 marked the culmination of a process of regional normalization several years in the making.[96] Revolutionary and counterrevolutionary processes unfolding in the Middle East and North Africa (MENA) region since the 2011 Arab uprisings, including the intensifying Saudi/UAE conflict with Iran, have led to a realignment of regional power that was previously unthinkable.[97]

The export of Israeli cyber intelligence and espionage technologies has been an important channel in this growing rapprochement. Rori Donaghy, founder of the Emirates Centre for Human Rights, told The Intercept in 2016 that the UAE considers Israelis to be "simply the best in this market, the most intrusive, the most secretive."[98] Donaghy claimed the UAE bought Israeli security products to the tune of hundreds of millions of US dollars. Hacked data from Cellebrite shared with Motherboard contained messages from the UAE's

> According to testimonies, Israeli products enabled governments to track and detain activists, persecute LGBT people and silence political dissent.

Other political motivations are more immediate and context-dependent. At the regional level, Israel's ongoing conflict with Iran has pushed it to form new strategic alliances in which cyber has been a key commodity. The recent normalization of political and economic relations between Israel and the UAE as discussed in the following section, provides an instructive case study for situating cyber within broader economic and political dynamics.

96 US Department of State, Bureau of Near Eastern Affairs, The Abraham Accords Declaration, 15 September 2020.

97 Hanieh, A. *Money, markets, and monarchies: The Gulf Cooperation Council and the political economy of the contemporary Middle East*. Vol. 4. Cambridge University Press, 2018.

98 Kane, A., How Israel Became a Hub for Surveillance Technology, *The Intercept*, 17 October 2016.

> Israel's disproportionate share in supplying authoritarian governments is best understood as rooted in its decades-old oppression of the Palestinian people, which has given it a vested interest in global repression to normalize its repressive policies and rally international support for them.

Ministry of Interior dated 2011.[99] In 2016, The Intercept reported that Cellebrite's UFED technology was used by Bahraini authorities in 2013 to crack the phone of tortured political dissident Mohammed al-Singace. The phone's contents, extracted using Cellebrite's software, were entered as evidence in al-Singace's trial.[100] According to Citizen Lab, NSO Group's iPhone zero-days was used against the UAE-based human rights defender Ahmed Mansoor.[101] In 2016, the Swiss-registered company Asia Global Technologies (AGT), owned by Israeli businessman Mati Kochavi, participated in installing Abu Dhabi's mass-surveillance system Falcon Eye, which was developed by ATG's Israeli subsidiary Logic Industries.[102]

Not only may Israeli technologies have been present in the Gulf for quite some time, but also Israeli human resources, in the form of intelligence veterans turned tech workers. Media sources revealed that the Abu Dhabi-based cyber company Dark Matter has been recruiting Unit 8200 veterans and employing them in Cyprus well before diplomatic relations were established.[103] Former Israeli military intelligence personnel were reportedly tied to a messaging app used by the UAE to monitor and surveil users. [104]

99 Cox, J., Cellebrite Sold Phone Hacking Tech to Repressive Regimes, Data Suggests, *Motherboard Tech by Vice*, 12 January 2017. According to Motherboard, "Cellebrite declined a request for comment, and did not answer an emailed set of questions about the company's vetting of customers, nor the absence of any human rights clauses from the EULA."

100 Biddle, S. and Desmukh, F., Phone-Cracking Cellebrite Software Used to Prosecute Tortured Dissident, *The Intercept*, 8 December 2016. The Intercept contacted Cellebrite co-CEO Yossi Carmil, who referred the authors to Cellebrite's CMO Jeremy Nazarian. "Nazarian told The Intercept that the use of Cellebrite technology to torture a Bahraini human rights activist 'doesn't ring a bell,' and 'as a general policy we don't discuss anything having to do with field operations.'" The following day, a PR firm representing the company told The Intercept Cellebrite declined to comment any further.

101 Marczak, B. and Scott-Railton, J., The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender, Citizen Lab, 24 August 2016. Brewster, T., Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones with a Single Text, *Forbes*, 25 August 2016. According to Forbes, "NSO Group sent a statement to FORBES via email in which it said its mission was to make the world a safer place 'by providing authorized governments with technology that helps them combat terror and crime'. 'The company sells only to authorized governmental agencies, and fully complies with strict export control laws and regulations. Moreover, the company does NOT operate any of its systems; it is strictly a technology company,' the statement continued. 'The agreements signed with the company's customers require that the company's products only be used in a lawful manner. Specifically, the products may only be used for the prevention and investigation of crimes. The company has no knowledge of and cannot confirm the specific cases mentioned in your inquiry.'" For more on the activities of NSO Group, see: Who Profits, NSO Group: Technologies of Control, May 2020.

102 Ferzeiger, J. and Waldman, P. How Do Israel's Tech Firms Do Business in Saudi Arabia? Very Quietly, *Bloomberg*, 2 February 2017. According to Bloomberg, Kochavi through his spokesperson declined to comment on the allegations.

103 Mazzetti, M., Goldman, A., Bergman, R., and Perlroth, N. A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments, *New York Times*, 21 March 2019. According to the NYT, the company did not respond to a request to comment.

104 TOI Staff, Former IDF intelligence personnel likely tied to UAE spy app, report says, *Times of Israel*,

Following the establishment of formal economic and political relations in September 2020, such business dealings and recruitment efforts have been taking place openly, and their volume has increased dramatically. According to the Israel Export Institute, Israeli exports to the UAE surpassed US$500 million in the first six months since the normalization agreement was signed and are expected to reach a billion US dollars within a year.[105]

> The export of Israeli cyber intelligence and espionage technologies has been an important channel in the growing rapprochement between Israel and the UAE.

Shortly after the agreements were signed, the head of the INCD and his Emirati counterpart spoke in a joint public forum organized by Tel Aviv University's cyber research center, affirming the strategic partnership between the two states.[106] The UAE Head of Cyber Security went as far as to propose joint Israeli-UAE cyber exercises.[107] Israeli cyber companies participated in a high-tech delegation to the UAE organized by Jerusalem Venture Partners Fund.[108] In October 2020, Cellebrite announced a US$3 million deal with a government agency in Abu Dhabi.[109] A source told Israeli newspaper Globes that the deal was brokered by a former Mossad executive.[110] Israeli cyber company, Waterfall Security, opened a subsidiary in Abu Dhabi in March 2021,[111] while an Israeli consortium led by Rafael participated in (and reportedly lost) an international bid to establish a national cybersecurity command center in Dubai in February 2021.[112]

The coming together of shared geopolitical interests, Emirati capital and Israeli surveillance expertise was encapsulated in the Cybertech Global international conference and exhibition held in Dubai in April 2021. This was the first time since its inception in 2013 that Cybertech Global took place outside of Tel Aviv. According to media reports, it was the biggest conference for the cyber industry outside of the US, and its main exhibit appeared to be the newly public and rapidly expanding cyber ties between the founding and host countries, Israel and the UAE.[113]

The conference program included sessions on cyber in aviation, maritime and logistics, crit-

23 December 2019.

105 Desoukie, O and Duer, P., Israel y Emiratos, medio año de relaciones más comerciales que diplomáticas, (Spanish) *SWI swissinfo.ch*, 15 March 2021.

106 Head of UAE cyber directorate: We share information and it helps us with deterrence, (Hebrew) Israel National Cyber Directorate, 24 September 2020. Accessed 10 May 2021.

107 Kogosowski, M., Head of UAE cyber directorate calls for joint cyber exercises with Israel, (Hebrew) Israel Defense, 6 April 2021.

108 Solomon, S., Food, cybersecurity firms leave for UAE in bid to forge tech ties, *Times of Israel*, 25 October 2020.

109 Berkovitz, U., Israeli cyber intelligence co Cellebrite signs deal in UAE, *Globes*, 22 October 2020.

110 Ibid.

111 Israeli industrial cyber firm Waterfall established a subsidiary in the UAE, (Hebrew) *TechTime Electronics & Technology News*, 29 March 2021.

112 Melman, Y., Stinging Blow for Israel in Major Dubai Cyber Bid, *Haaretz*, 28 February 2021. Emirati official denied that Rafael lost the bid and told Haaretz the tender is currently undergoing structural changes. Ben Yaakov, O. Israel and the UAE share information on Hezbolla's cyber activties, (Hebrew) *Haaretz*, 7 April 2021.

113 Israel-UAE cybersecurity ties the focus of attention at Cybertech conference in Dubai, *CTech*, 7 April 2020.

ical infrastructures and smart cities, fintech, national intelligence and policing, and in the post-Covid-19 world. On the Emirati side, there were speakers and sponsors from the Dubai International Financial Center, London Stock Exchange Group, the National Bank of Fujairah and the government owned Emirates NBD, as well as major public and private enterprises. [114]

On the Israeli side, high ranking intelligence officers turned tech entrepreneurs dominated the list of participants. Those included Nadav Zafrir, the former commander of Unit 8200 and current Managing Partner of Team8, Tamir Pardo, the former Head of the Mossad and current Chairman of XM Cyber, and Nir Lempert, the CEO of Israeli surveillance firm Mer Group and Chairman of the Unit 8200 Alumni Association.[115] An invitation-only special session invited conference attendees to unlock the "Secrets of Unit 8200 – incubator forging entrepreneurs and innovators."[116]

The forms of political, economic and scientific cooperation facilitated by the recent UAE-Israeli normalization are part of a growing trend whereby Israel's booming surveillance industry is utilized to shape and advance political ends, generating enormous profits in the process.

114 Agenda, Cybertech Global Dubai. Accessed 10 May 2021.
115 Ibid.
116 Ibid.