CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Deborah Housen-Couriel

National Cyber Security Organisation: ISRAEL

Tallinn 2017

www.ccdcoe.org
publications@ccdcoe.org

About NATO CCD COE

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is a NATO-accredited knowledge hub, research institution, and training and exercise facility. The Tallinn-based international military organisation focuses on interdisciplinary applied research, as well as consultations, trainings and exercises in the field of cyber security.

The heart of the Centre is a diverse group of international experts, including legal scholars, policy and strategy specialists who join forces with technology researchers, all from military, government and industry backgrounds.

Membership of the Centre is open to all Allies. As of October 2016, Belgium, the Czech Republic, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, Turkey, the United Kingdom and the United States have signed on as Sponsoring Nations (SNs) of the Centre. Austria and Finland have become Contributing Participants (CPs) – the status available for non-NATO nations.

For more information on NATO CCD COE, visit the Centre's website at http://www.ccdcoe.org.

About this study

The NATO CCD COE series of reports on national organisational models for ensuring cyber security summarise national cyber security strategy objectives and outline the division of cyber security tasks and responsibilities between agencies. In particular, the reports give an overview of the mandate, tasks and competences of the relevant organisations and the coordination between them. The scope of the reports encompasses the mandates of political and strategic cyber security governance; national cyber incident management coordination; military cyber defence; and cyber aspects of crisis prevention and crisis management.

Reports in this series

National Cyber Security Organisation in Czech Republic

National Cyber Security Organisation in Estonia

National Cyber Security Organisation in France

National Cyber Security Organisation in Hungary

National Cyber Security Organisation in Italy

National Cyber Security Organisation in Lithuania

National Cyber Security Organisation in the Netherlands

National Cyber Security Organisation in Slovakia

National Cyber Security Organisation in Spain

National Cyber Security Organisation in the United Kingdom

National Cyber Security Organisation in the USA

Non-NATO nations

China: China and Cyber: Attitudes, Strategies, Organisation

National Cyber Security Organisation: Israel

Series editor: Kadri Kaska (Researcher, NATO CCD COE)

Information in this study was checked for accuracy as of March 2017.

ISRAEL

By Deborah Housen-Couriel, B.A., LL.M.
Attorney (Israel Bar)
Research Fellow at Tel Aviv University Interdisciplinary Cyber Research Center, the Minerva Center for the Rule of Law at Haifa University and the International Institute for Counterterrorism at the Herzliya IDC

Table of Contents

1. Digital society context in the State of Israel

1.1. Internet infrastructure availability and take-up

Israel has been at the forefront of hi-tech and internet infrastructure and services development for the past decade, consistently ranking among those countries leading the OECD rankings for research and development spending as a percentage of national GDP. In 2014, Israel ranked second of all OECD countries for this parameter, with national expenditure on civilian R&D amounting to NIS 44.8 billion (ca 10.4 billion EUR), or 4.1% of its GDP.[1] Likewise, the estimated value of the ICT sector in Israel for 2014 is 129 million NIS (ca 30 million EUR),[2] constituting more than 18% of total national output.[3] Foreign investment in the sector grew 20% between 2014 and 2015, and stands at approximately USD 540 million.[4] In 2014, the total Israeli share of the global cybersecurity market stood at approximately 8%.[5]

In keeping with the country's emphasis on technological and scientific innovation, the installation of advanced communications infrastructures and the public's uptake of internet services have been characterised by relatively early adoption and wide utilisation.[6] The ITU's 2016 State of Broadband Report estimates the percentage of the population using the internet in 2015 at 78.89%, ranking Israel 33rd globally.[7] The percentage of Israel's population above the age of 20 utilising computers to access the Internet is 74.2%, with a relatively small gender gap (76.4% of men and 72.1% of women).[8]

Broadband became available in 2000, and within a decade approximately 82% of Israeli households were connected at an average speed of above 35 Mbps.[9] Fixed broadband penetration reaches 27.44% of the population,

[1] OECD, 'Gross domestic spending on R&D (indicator)', 2016, <https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm>; Central Bureau of Statistics (CBS), <http://www.cbs.gov.il/www/hodaot2015n/12_15_227e.pdf>. The statistics for Israel follow the CBS and OECD criteria for population, businesses and the industries surveyed, <http://www.cbs.gov.il/www/shnaton61/st_eng02.pdf>; World Bank Group, 'World Development Report 2016: Digital Dividends', 2016, p. 231.

[2] CBS, <http://www.cbs.gov.il/hodaot2015n/29_15_212t1.pdf>.

[3] CBS, <http://www.cbs.gov.il/shnaton66/diag/18_04.pdf>, 20 October 2015. The gross added value of the ICT sector for 2014 is 73 million NIS (ca 17 million €), <http://www.cbs.gov.il/hodaot2015n/29_15_212t1.pdf>. See also http://www.cbs.gov.il/shnaton67/diag/18_04.pdf (Hebrew). See also Getz, Daphne and Goldberg, Itzhak, 'Best Practices and Lessons Learned in ICT Sector Innovation: A Case Study of Israel', World Development Report Background Paper, 2016.

[4] Reuters, 'Israeli firms have record year in cyber, raise $540 mln – report', 24 January 2016, <http://www.reuters.com/article/israel-cyber-idUSL8N158044>. See also Opall-Rome, Barbara, 'Israeli Cyber Exports Double in a Year', DefenseNews, 3 June 2015. Early reports of 2016 figures show an increase in growth (Solomon, Shoshanna, 'Speed, agility seen as Israel's edge in cyber war', The Times of Israel, January 30, 2017.

[5] Figures are according to the Israel National Cyber Bureau, as cited in Tsipori, Tali, 'Israeli cybersecurity grabs 8% global market share', Globes, 4 April 2016, <http://www.globes.co.il/en/article-israeli-cyber-industry-hits-the-big-time-1001114669>; See also Start-Up Nation Central, 'Israel's Cybersecurity Industry in 2016', February 2017, which indicates that these figures have increased for 2016.

[6] One example is Israel having been ranked first among OECD countries in the use of selected geo-location services (spurred by the Israeli start-up company *Waze*), OECD, 'Digital Economy Outlook 2015', Fig.3.16, p. 146; See also Bezeq, 'Life in the Digital Age', 2017, (Hebrew), <http://www.bezeq.co.il/media/PDF/internetreport_2016.pdf>.

[7] ITU and UNESCO, 'The State of Broadband 2016', 2016, p. 96. <http://www.broadbandcommission.org/Documents/reports/bb-annualreport2016.pdf>,.

[8] CBS, 'Statistical Abstract of Israel 2015', <http://www.cbs.gov.il/reader/shnaton/templ_shnaton_e.html?num_tab=st09_07&CYear=2015> (statistics are updated to 2013); See also Israeli Internet Association, Statistics Database (Hebrew), <http://en.isoc.org.il/tech_eng/sts_eng.html>.

[9] Ministry of Communications, 'Telecommunications in Israel 2013', <http://www.moc.gov.il/sip_storage/FILES/5/605.pdf>; One of the major suppliers, Bezeq Ltd., reports an average broadband speed per subscriber of 36.7 Mbps for the final quarter of 2015, <http://phx.corporate-ir.net/External.File?item=UGFyZW50SUQ9MzEzOTY1fENoaWxkSUQ9LTF8VHlwZT0z&t=1&cb=635835135360505783>.

with broadband services presently provided by the fixed telephone and cable infrastructures of two companies.[10] A third competitor has been licensed to provide customers with a 1 Gbps connection over fibre-optic cables and the national electric grid. In February 2015, the Ministry of Communication introduced a reform allowing operators to purchase internet infrastructure from these companies (i.e. broadband access and fixed lines) at wholesale prices, thereby opening up these markets to greater competition.[11]

Cellphone operators introduced wireless Internet in 2001, and the uptake of mobile telephony has exceeded 100% of the population since 2004.[12] There is presently an overall penetration rate of 122% for mobile telephony,[13] with mobile broadband penetration standing at 56.06%;[14] and presently accounting for over 40% of the total revenue of Israel's ICT digital economy.[15]

Israel has relatively few land-contiguous internet connections.[16] In addition to its satellite connectivity, three undersea cables connect Israel to points abroad.[17] The Israel Internet eXchange (IIX), one of the early hubs for Israeli ISPs, provides some domestic connectivity in addition to some direct connections in place among ISPs. The exchange is supported by the **Israel Internet Association (ISOC-IL)**, a not-for-profit organization that, *inter alia,* manages domain names, promotes internet use and provides the public with information regarding online safety.[18]

Israel was ranked 21st globally by the World Economic Forum's Networked Readiness Index in 2016.[19]

1.2. Availability and use of e-government and e-commerce

The e-government platform, *Tehila*, was established in 1997 in order to provide government offices and authorities with a secure and protected platform for connection to the internet, intra-governmental activity, government-to-citizen and citizen-to-government fora, and the infrastructure for provision of services to the public. The platform has evolved into the present, expanded *gov.il* portal, now under the aegis of the governmental ICT Authority,

[10] ITU and UNESCO, (n 7) . The OECD 2015 estimate for Israel's fixed broadband penetration rate stands at 25.9% per capita, ranked 28th among OECD countries. 'OECD Broadband Portal', <http://www.oecd.org/sti/broadband/broadband-statistics-update.htm>. This relatively low rate is partially offset by the relatively large household size in Israel.
[11] Ministry of Communications, Press Release, 'The Wholesale Market Reform – Increased Competition in Broadband Internet', 2 August 2015, <http://www.moc.gov.il/sip_storage/FILES/5/4425.pdf>.
[12] Ministry of Communications, 'Telecommunications in Israel 2006', p. 6, (population for 2004 was 6.8 million), <http://www.moc.gov.il/new/documents/broch_1.11.06.pdf>.
[13] OECD, 'Key ICT Indicators 2016', 2b, <https://docs.google.com/viewer?url=http%3A%2F%2Fwww.oecd.org%2Fsti%2Fieconomy%2FICT-Key-Indic_2_Mobile.xlsx>
[14] Ministry of Communications, (n 11). The OECD 2015 estimate for Israel's fixed broadband penetration rate stands at 25.9% per capita, ranked 28th among OECD countries (OECD Broadband Portal', <http://www.oecd.org/sti/broadband/broadband-statistics-update.htm>.
[15] OECD, 'Digital Economy Outlook Tables 2015', Tables 2.24 and 2.11, <http://www.oecd.org/sti/deo-tables-2015.htm>. The Israeli Ministry of Communications estimated mobile cellphone penetration at 132% in 2013, <http://www.moc.gov.il/sip_storage/FILES/5/605.pdf>.
[16] See Israel's peace agreements with Egypt, Jordan and the Palestinian Authority for specific provisions regarding telecommunications connectivity and spectrum coordination. These are, respectively, the Peace Treaty between Israel and Egypt, 26 March 1979 (Annex III, art. 6), <http://www.mfa.gov.il/mfa/foreignpolicy/peace/guide/pages/israel-egypt%20peace%20treaty.aspx>; the Peace Treaty between Israel and Jordan, 26 October 1994 (art. 16), <http://www.mfa.gov.il/mfa/foreignpolicy/peace/guide/pages/israel-jordan%20peace%20treaty.aspx>; and the Israeli-Palestinian Interim Agreement, 28 September 1995 (Annex III, Appendix 1, art. 36) <http://www.mfa.gov.il/MFA/ForeignPolicy/Peace/Guide/Pages/THE%20ISRAELI-PALESTINIAN%20INTERIM%20AGREEMENT%20-%20Annex%20III.aspx>.
[17] The three undersea cables are MedNautilus (owned by Telecom Italia), the Tamares Telecom cable, and The Bezeq International Optical System.
[18] The Israel Internet Association supports the IIX hub for the approximately 70 licensed ISP's (3 are the major providers). See <http://www.isoc.org.il/iix/2x.html>.
[19] World Economic Forum, 'The Global Information Technology Report 2016', <http://reports.weforum.org/global-information-technology-report-2016/networked-readiness-index/>.

established in 2011.[20] The portal supports a wide range of online services and guidance in Hebrew, Arabic and English on topics such as health insurance, employment, foreign investment, and childcare. Local and municipal government services are supplied through the *gov.il* portal and the *Shoham* payment system, through which tax payments can be made. Specific examples of dedicated e-government applications include an electronic 'smart card' for government employees and businesses that permits safe transfer of documents and electronic signatures, e-access to the national Judicial Authority's electronic system, the tax authority portal, electronic government tenders, the *Magna* system for reporting to the Securities Authority, the government's *Merkava* Enterprise Resource Planning (ERP) infrastructure, and an electronic identity card (currently under development). In 2016, a UN survey ranked Israel 17th among the world's countries for its level of e-government services (1st in the Western Asia category).[21]

In 2009, the **Knesset** enacted the Biometric Database Law,[22] establishing the arrangements for securely including biometric data in official identification documents such as ID cards and passports, and established the Biometric Database Management Authority.[23] The onboarding period for transition to biometric documentation began in 2013, and the law was amended in early 2017 with respect to, *inter alia,* finalization of the transition period.[24] These initiatives have been supplemented since 2013 by the government's 'Digital Israel' programme, which aims to reduce digital gaps within Israel through the construction of a national optical fibre grid allowing for Internet speeds of up to 1 Gbps, providing advanced digital services to the entire population and setting out a long-term national digital strategy.[25] In 2014, Israel joined the UK-sponsored Digital 5 initiative as a charter member.[26]

As for private sector e-commerce and e-business, a 2015 survey conducted on behalf of eBay noted that two-thirds of Israeli businesses sell goods and services online, and that 91% of the Israelis surveyed had made at least one online purchase over the previous year.[27] Since July 2014, Israelis have been able to open bank accounts online.[28]

2. Strategic national cyber security objectives

2.1. National cyber security foundation and objectives

Israel's establishment of national cyber security measures and institutions came about relatively early and continues to develop in the face of a challenging environment of military and civilian threats. Israeli banks, financial

[20] Government Resolution 3058, 27 March 2011, <http://www.pmo.gov.il/Secretary/GovDecisions/2011/Pages/des3058.aspx>; Government Resolution 2097, 10 October 2014,<http://www.pmo.gov.il/Secretary/GovDecisions/2014/Pages/dec2097.aspx>; Getz and Goldberg, (n 3), pp. 58-59.
[21] United Nations, 'E-Government Survey 2016', <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016>.
[22] Inclusion of Biometric Means of Identification in Identity Documents and in an Information Database Law of 2009, <http://smartid.gov.il/SiteCollectionDocuments/bio_law.pdf> (Hebrew).
[23] Population And Immigration Authority, 'Questions And Answers', <http://smartid.gov.il/english/GeneralInformation/Pages/FAQ.aspx>.
[24] The pilot programme had also been extended in March 2016 , see <http://www.jpost.com/Israel-News/Knesset-approves-extension-of-biometric-database-pilot-449639>. The amendment to the 2009 law of 27 February 2017 is available in Hebrew at: <https://www.law.co.il/media/computer-law/biometric_law_amendment_2017.pdf>.
[25] Government Resolution 1046, 15 December 2013, <http://www.pmo.gov.il/Secretary/GovDecisions/2013/Pages/dec1046.aspx>.
[26] D5 Charter, 9 December 2014, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386290/D5Charter_signed.pdf>.
[27] Press Release, Stern-Ariely, 12 October 2015, <http://data.isoc.org.il/data/632>; Israel Internet Association, (n 8).
[28] Bank of Israel, Supervisor of Banks, Proper Conduct of Banking Business Directive 418, 'Opening of Accounts *via* the Internet', 15 July 2014, <http://www.boi.org.il/he/BankingSupervision/LettersAndCircularsSupervisorOfBanks/HozSup/2427.pdf>.

institutions, utility companies and other critical infrastructures are among those most frequently subjected to hostile cyber events globally.[29]

Cyber security became an explicit national objective in November 2010,[30] with the Prime Minister's launch of a '*National Cyber Initiative*' under the auspices of the National Council on Research and Development within the Ministry of Science. This *ad hoc* multi-disciplinary task force was headed by the chair of the National Council for Research and Development, and composed of approximately eighty specialists from the military, government ministries, academia and the private sector.[31] The 'Initiative' task force was charged by the Prime Minister with recommending measures to promote Israeli leadership in cyber security at the global level. Its twelve final recommendations, presented to the government after six months of intensive work[32], were incorporated into Government Resolution 3611 in August 2011, entitled '*Advancing National Cyberspace Capabilities*'.[33] The Resolution also established the **National Cyber Bureau** (INCB) as the first national advisory and consolidating body for cyber security.

As of late 2016, the INCB has not yet published a unified document setting out its national cyber policy, although its approach is incorporated into the regulatory and other activities described below. Government Resolution 3611, the basis upon which the eventual policy document will most likely rely, indicates four national priorities in the realm of cyberspace: (1) advancing national capabilities and improving the management of current and future cyberspace challenges; (2) improving 'the defense of national infrastructures which are essential for maintaining a stable and productive life in the State of Israel'; (3) advancing the country's status as a global centre for the development of information technologies; and (4) encouraging interdisciplinary cooperation among academia, industry, the private sector, and government ministries.[34] Additional government Resolutions, in particular Resolutions 2443[35] and 2444[36] discussed below, elaborate upon these national priorities and expand the institutional capacity for cybersecurity by establishing a National Cyber Defence Directorate[37] that includes both the INCB and a National Cyber Security Authority.[38]

[29] The Kaspersky 2015 Report also gives Israel a high-risk rating of 47.3%' ('high risk') for local cyber threats, <https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_EN.pdf>.

[30] For previous government initiatives regarding information security, see State Controller and Ombudsman, 'Critique and Oversight in Information Systems', 4th ed., February 2005, (Hebrew), <http://www.pmo.gov.il/BikoretHamedina/files/bakarot%20ve%20bikoret%202005.doc>.

[31] National Cyber Initiative, 'Special Report for the Prime Minister', National Council on Research and Development, Ministry of Science, 2011 (Hebrew). The Initiative was headed by Professor Isaac Ben Israel, who headed Mafat and currently chairs the National Council on Research and Development.

[32] Ibid.

[33] Government Resolution 3611, 7 August 2011, <http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf>.

[34] Ibid. See also Tabansky, Lior and Ben Israel, Isaac, 'Cybersecurity in Israel', Springer, 2015, pp. 49-54; Lewis, James 'Advanced Experiences in Cybersecurity Policies and Practices', Inter-American Development Bank, Discussion Paper IDB-DP-457, 2016, pp. 24-25.

[35] Government Resolution 2443, 15 February 2015 (Hebrew), http://www.pmo.gov.il/Secretary/GovDecisions/2015/Pages/des2443.aspx; (English) < https://ccdcoe.org/sites/default/files/documents/Government%20Resolution%20No%202443%20-%20Advancing%20National%20Regulation%20and%20Governmental%20Leadership%20in%20Cyber%20Security.pdf>

[36] Government Resolution 2444, 15 February 2015 (Hebrew), < http://www.pmo.gov.il/Secretary/GovDecisions/2015/Pages/des2444.aspx>; (English) < https://ccdcoe.org/sites/default/files/documents/Government%20Resolution%20No%202444%20-%20Advancing%20the%20National%20Preparedness%20for%20Cyber%20Security.pdf>.

[37] INCB, 'Background for the Government Resolutions Regarding Advancing the National Preparedness for Cyber Security and Advancing National Regulation and Governmental Leadership in Cyber Security', 2015.

[38] Some of these developments were the subject of an enquiry by the State Comptroller's Office in its 2016 Annual Report (State Controller's Report 67A, 1 November 2016, Chapter 2 (Hebrew)). <http://www.mevaker.gov.il/he/Reports/Report_552/b9842c3e-e157-4f16-9529-df1aca2002cb/101-cyber.docx>.

The **Israeli Defense Forces** (IDF) have been concerned with cyber security issues and cyber threats for decades;[39] however, consistent with their approach in other areas of defence policy, few details regarding national cyber security considerations and policy in the military sphere are shared with the public. A departure from this pattern took place in August 2015, with the publication by Chief of Staff Gadi Eisenkot of the *IDF Strategy*, an unclassified summary of the IDF's overall military approach.[40] This document includes several references to the IDF's position on cyber security, including the understanding that cyberspace is a military realm; the prioritisation of continued building of cyber defence and offence capacity at the strategic, operative and tactical levels; threat awareness in cyberspace; and, at the organisational level, the initiation of a process to establish the cyber command structure within the IDF. The *IDF Strategy* document notes that cyber defense in war and emergency situations is essential to ensuring the continued operation of national institutions in times of tension, as well as the effective performance of the IDF.[41]

In general, Israel's national cyber security objectives and priorities may be characterised at present by the implementation of a process of greater public transparency, institutional innovation, and governmental investment in both short-term objectives (i.e., subsidies for cyber security-related companies) and long-term ones (i.e., the Ministry of Education's *Magshimim* programme and matriculation exam in cyber security studies available as an option for high-schoolers). Since 2011, the Prime Minister's Office has taken the lead in promoting Israeli cyber security objectives both domestically and internationally. Chapter 3 herein elaborates upon some of these initiatives.

2.2. National laws and directives

Several Israeli laws deal specifically with issues related to information security, among them the Computers Law of 1995;[42] the Protection of Privacy Law of 1981 and associated regulations, including the Protection of Privacy Regulations (Data Security) 5777-2017;[43] the Encouragement for Industrial Research and Development Law of 1984;[44] the Defense Exports Control Law of 2007;[45] the Communications (Telecommunications and Broadcasting) Law of 1982;[46] the Law for Regulating Security in Public Bodies of 1998;[47] the Electronic Signature Law of 2001;[48]

---

[39] Raska, Michael, 'Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy', RSIS Policy Report, 8 January 2015, <https://www.rsis.edu.sg/rsis-publication/gpo/confronting-cybersecurity-challenges-israels-evolving-cyber-defence-strategy/#.WGOXhfl97SE>.

[40] Israel Defense Forces Strategy, 2015, <https://www.idf.il/media/5679/%D7%90%D7%A1%D7%98%D7%A8%D7%98%D7%92%D7%99%D7%99%D7%AA-%D7%A6%D7%94%D7%9C.pdf >; See also Herzog, Mike, 'New IDF Strategy Goes Public', 28 August 2015, <http://www.washingtoninstitute.org/policy-analysis/view/new-idf-strategy-goes-public>.

[41] Ibid, p. 18 . See also Hathaway, Melissa, 'Cyber Readiness Index 2.0', Potomac Institute, 2015, p. 30; and Baram, Gil, 'Israeli Defense in the Age of Cyber War', Middle East Quarterly, Winter 2017, <http://www.meforum.org/6399/israeli-defense-in-the-age-of-cyber-war>.

[42] Computers Law of 1995 (Hebrew), <http://law.co.il/media/computer-law/computers_law_nevo.pdf>.

[43] Protection of Privacy Law of 1981, <http://www.justice.gov.il/En/Units/ILITA/Documents/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf>; Protection of Privacy Regulations (Data Security) 5777-2017 (Hebrew), draft bill available at < http://fs.knesset.gov.il//20/Committees/20_cs_bg_381332.pdf>. Additional regulations flowing from the Protection of Privacy Law are available at: <http://www.justice.gov.il/En/Units/ILITA/Pages/Legislation-and-other-documents.aspx>.

[44] Encouragement for Industrial Research and Development Law of 1984 (Hebrew), <https://www.nevo.co.il/law_html/law01/p181m2_001.htm#_ftn1 >.

[45] Defense Export Control Law of 2007, < http://www.exportctrl.mod.gov.il/NR/rdonlyres/7B53DDE6-AEE8-47BC-AEFA-1AF325FB96D0/0/Defense_Export_Contro_Law.pdf >.

[46] Communications (Telecommunications and Broadcasting) Law of 1982 (Hebrew), <http://www.nevo.co.il/law_html/Law01/032_002.htm>.

[47] Law for Regulating Security in Public Bodies of 1998 (Hebrew), <http://www.nevo.co.il/law_html/Law01/111M1_001.htm>

[48] Electronic Signature Law of 2001, <http://www.financeisrael.mof.gov.il/FinanceIsrael/Docs/En/legislation/Others/5761-2001_Electronic_Signature_Law.pdf>.

and the Biometric Database Law of 2009.[49] In addition, key definitions relevant to Israel's cyberspace activity have been provided by government resolutions 3611, 2443 and 2444, respectively, of the terms 'cyberspace'[50] and 'civilian space';[51] 'cyber security';[52] and 'cyber security services market'[53] and 'sector'[54].

In August 2016, the Knesset passed a new counter-terrorism law, which broadened the definition of 'terrorist act' to include damage to infrastructure, systems and essential services, which may in the future be interpreted to include such terrorist activity utilising cyberspace.55 That same month, the Israeli State Attorney published guidelines outlining prosecutorial policy regarding offenses related to the possession, use and distribution of pedophilic content on the internet.[56]

At the sectoral level, the Bank of Israel has issued a directive on cyber security measures ('Directive 361') and a Letter on Risk Management in a Cloud Computing Environment in 2015, requiring Israeli banks, *inter alia*, to have a cybersecurity strategy in place and to designate a senior official responsible for cyber security.[57] In August 2016, the Supervisor of Capital Markets issued a directive on Cyber Risk Management.[58] The Director-General of the Ministry of Health issued a directive to health service providers on the protection of digital health data in February 2015.[59] A draft document on cybersecurity information sharing guidelines was circulated by the Antitrust Authority in February 2017.[60]

[49] Law on Inclusion of Biometric Means of Identification in Identity Documents and in an Information Database Law of 2009 (Hebrew), <https://www.nevo.co.il/Law_word/law14/law-2217.pdf>; amended in early 2017, < https://www.nevo.co.il/law_word/law14/law-2607.pdf>.

[50] 'Cyberspace' is defined in Resolution 3611 as '…[T]he physical and non-physical domain that is created or composed of part or all of the following components: mechanised and computerised systems, computer and communications networks, programs, computerised information, content conveyed by computer, traffic and supervisory data and those who use such data.' ('Definitions'), (n 33).

[51] Ibid.

[52] 'Cyber Security' is defined in Resolution 3611 as '..[P]olicies, security arrangements, actions, guidelines, risk management protocols and technological tools designated to protect cyberspace and allow action to be taken therein.' (ibid). The later Resolution 2444 defines it as 'The range of actions for the prevention, mitigation, investigation and handling of cyber threats and incidents, and for the reduction of their effects and of the damage caused by them prior, during and after their occurrence',(n 36).

[53] Resolution 2443,(n 35).

[54] Ibid.

[55] Ministry of Justice, The Legal Counseling and Legislation Department (International Law), 'Background Description of the The Counter-Terrorism Law, 5775-2015', 2016, <http://www.justice.gov.il/Units/InternationalAgreements/HumanRightsAndForeignRelations/Faq/CounterTerrorismLaw5775-2015_BackgroundDescriptionJune2016.pdf>.

[56] 'Guidelines of the State Prosecutor regarding the possession, use and distribution of pedophilic content on the internet' (Hebrew), No. 2.22, 31 August 2016, < http://www.justice.gov.il/Units/StateAttorney/Guidelines/02.22.pdf>.

[57] Bank of Israel, Supervisor of Banks, Proper Conduct of Banking Business Directive 361, 'Cyber Defense Management', 15 March 2015, <http://www.boi.org.il/en/BankingSupervision/SupervisorsDirectives/ProperConductOfBankingBusinessRegulations/361_et.pdf> and Letter on Risk Management in a Cloud Computing Environment, 29 June 2015, <http://www.boi.org.il/en/BankingSupervision/LettersAndCircularsSupervisorOfBanks/LettersOfTheBankingSupervisionDepartment/201514en.pdf>.

[58] Supervisor of Capital Markets, 'Management of Cyber Risks in Institutional Bodies', 31 August 2016 (Hebrew), <www.mof.gov.il/hon/documents/הסדרה-וחקיקה/.../th_2014-117.pdf>.

[59] Director-General of the Ministry of Health, 'Data Protection in Computerized Systems in the Health Sector', Directive 3/15, 15 February 2015 (Hebrew), <http://www.health.gov.il/hozer/mk03_2015.pdf>.

[60] See Antitrust Authority,'Draft Hearing on Information Sharing Guidance for Dealing with Cyber Threats'" (Hebrew), <http://www.antitrust.gov.il/files/34485/%D7%98%D7%99%D7%95%D7%98%D7%AA-%D7%92%D7%99%D7%9C%D7%95%D7%99_%D7%93%D7%A2%D7%AA_%D7%A1%D7%99%D7%99%D7%91%D7%A8-_012017.pdf >.

2.3. Other national cyber security initiatives

2.3.1. Regulation of cyber security professions

In December 2015, the INCB published a policy paper on the regulation of the cyber security professions in Israel.[61] The basis for the policy, in line with government Resolutions 2443 and 2444, is the need to ensure that Israeli companies, government bodies and other organisations will be able to ensure a high level of cyber security by utilising professionals accredited with a specified level of professionalism, reliability and ethics. In formulating the need for national regulation and the role of the government in advancing it, the INCB incorporated the work of a public commission convened in 2014 ('the Shafran Commission') to explore both the need for regulation of this sector and its possible structuring.[62] The new policy, to be fully implemented by 2021, identifies five cyber professions that will be regulated; the knowledge base and training required for each of them; and the means for their regulation.[63] Qualified professionals will undergo periodic re-testing and a national listing of those who qualify will be made available. The leading regulatory body for the gradual implementation of this policy will be a unit within the NCSA.[64]

2.3.2. International engagement

At the international level, Israel participated as a member of the United Nations' Group of Government Experts (GGE) which issued a report on developments in the field of information and telecommunications in the context of international security in 2015.[65]

The country formally acceded to the Council of Europe's 2001 Convention on Cybercrime on 1 September 2016,[66] and has forged bilateral cooperative relationships to promote cybersecurity with a number of countries and international organisations, including through bilateral treaties.

Together with the work undertaken by the INCB, Israel's Ministry for Foreign Affairs has designated a Cybersecurity Coordinator, responsible for developing contacts and cooperation at the bilateral and multilateral levels.

3. National organisational structure for cyber security and cyber defence in Israel

3.1. Political and strategic management and national cyber security coordination

As noted in Section 2.1 above, the **Israeli National Cyber Bureau** (INCB) was established in 2011 by government resolution 3611 in order to consolidate civilian cyber security at the national level. Its purview within the Prime Minister's Office is to serve as an advisory body to the Prime Minister, governmental ministries, and other governmental authorities. The INCB recommends national cyber security policy and promotes its implementation throughout the government.

---

[61] INCB, 'Policy on Regulation of Cybersecurity Professions', (Hebrew), 31 December 2015, <http://www.pmo.gov.il/SiteCollectionDocuments/cyber/hagana.pdf>.
[62] Report of the Public Committee for the Defining Cyber Defense Professions ('Shafran Committee'), 2014.
[63] INCB, (n 61), p. 2. The five cybersecurity professions are: cyber defense practitioner with 'hands-on' capability, penetrating testing specialist, forensics specialist, cybersecurity methodology specialist, and technology specialist. Each profession has two levels of qualification, and overall requirements include Israeli citizenship, no criminal record, and age of majority.
[64] Ibid, p. 5.
[65] 'Report', Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015, <http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174>.
[66] Chart of signatures and ratifications, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=ATj3pi6h>.

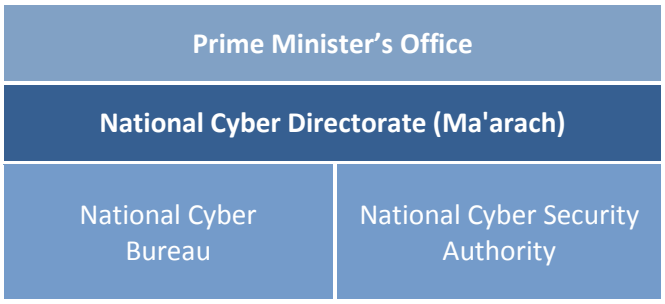
In February 2015, the INCB moved ahead with formulating two operative government resolutions on cyber security, setting the stage for the implementation of important elements of the national cyber security strategy and establishing a second national cybersecurity organ, the **National Cyber Security Authority** (NCSA), discussed below. The INCB and the NCSA together constitute the **National Cyber Directorate** (*Ma'arach*).

The first of these documents is Resolution 2443, entitled *Advancing National Regulation and Governmental Leadership in Cyber Security*.[67] This document sets out the approach of integrating new cyber security regulations within the already-established purview of existing government ministries and other regulators,[68] each one of which will assume additional regulatory capacities in its own sector of responsibility (e.g., the Ministry of Transportation will be charged with regulating cyber security for the transportation sector). Additionally, Resolution 2443 sets out the authority and capacity for the INCB's regulation of the market for cyber security professionals, services and products; elements of which are elaborated in the December 2015 policy paper discussed above in Section 2.3.1.[69]

The second is Resolution 2444, entitled *Advancing the National Preparedness for Cyber Defense*.[70] This resolution establishes a new body – the **NCSA**.

The NCSA is charged with the mission of defending cyberspace by conducting, operating and implementing 'all the operational defensive efforts in cyberspace at the national level, from a holistic perspective, for the purpose of providing a complete and continuous defensive response to cyber attacks, including handling cyber threats and incidents in real time, formulating an ongoing situational awareness, consolidating and analyzing intelligence, and working with the defense community.'[71] Among other tasks, it is charged with maintaining Israel's CERT, increasing the country's preparedness and resilience, developing a national cyber doctrine, and promulgating a cyber security law that will amend existing legislation and add new regulation, as needed.

The eventual governmental structure envisaged in Resolutions 2443 and 2444 will thus encompass by the end of 2017 a National Cyber Directorate (*Ma'arach*) consisting of two institutional pillars: the existing INCB and the new NCSA (see Figure 1).[72] Additionally, the establishment in each government ministry of intra-government and sectoral points of reference for cyber security policy implementation is likely to provide a broad framework for future national implementation of joint objectives and priorities.



[67] Resolution 2443, (n 35). See also INCB, 'Background for the Government Resolutions Regarding Advancing the National Preparedness for Cyber Security and Advancing National Regulation and Governmental Leadership in Cyber Security', 15 February 2015, <https://ccdcoe.org/sites/default/files/documents/Background_for_the_Government_Resolutions_Regarding_Cyber_Security-February_2015.pdf>.
[68] In addition to existing ministerial regulatory authorities, examples of relevant regulators include the Antitrust Authority and the Securities Authority.
[69] The INCB had convened a statutory public committee on this issue in 2014; see 2.3.1 above.
[70] Resolution 2444, (n 36) and INCB, (n 67).
[71] Resolution 2444, ibid, art 2 (a).
[72] Resolution 2444, ibid, art 3.

3.2. Cyber incident management and coordination

3.2.1. CERT-IL

The Israeli Cyber Event Readiness Team (CERT-IL) is a department of the NCSA, on the basis of Government Resolution 2444.[73] It has responsibility for national cyber security incident management, intelligence sharing with trusted partners in Israel and abroad, developing cyber security best practices, promoting cyber security awareness, and 'providing a single point of contact in Israel regarding cyber security threats and incidents for international corporations, cyber security companies and other CERTs'.[74]

3.2.2. Police

The Israel Police established a cyber division in 2012 in order to deal with cybercrime and to serve as a central focal point for the development of expertise in digital forensics and evidence .[75] It is located within elite national police division, *Lahav* 433.[76]

3.3. Critical infrastructure protection

With respect to cyber security objectives regarding the protection of critical infrastructure, Israel began to set out and implement a national policy in 2002 with Resolution No. B/84 of the National Security Ministerial Committee. This Resolution added a level of protection and supervision to certain computerised systems deemed "essential" (although there was no initial reference specifically to these systems as 'critical infrastructure')[77] and its provisions were eventually incorporated into the abovementioned Law for Regulating Security in Public Bodies.[78] The Resolution also established a new agency, the **National Information Security Agency** (NISA) operating within the General Security Service (GSS), to determine the criteria for regulation of specified governmental and private-sector bodies. NISA's task is to prepare cyber security objectives, develop a plan for their implementation, and oversee their implementation together with the appropriate government ministry. Resolution B/84 stipulated the establishment of a Steering Committee to provide guidance and oversight to the NISA in this respect. The regulated bodies include government ministries; the court and prison systems; the Bank of Israel and other banks; selected defence industries; gas, energy and water companies; hospitals; communications suppliers, including ISPs; the El Al national airline; Israel Railways; ports; the stock exchange; and *Bituach Leumi* (the social security authority).

---

[73] Israel National Cyber Event Readiness Team, <https://cert.gov.il/CERT-IL/Pages/CERT-IL.aspx> ; CERT-IL RFC 2350, <https://cert.gov.il/CERT-IL/SiteAssets/RFC2350.pdf>.

[74] Ibid.

[75] Israel Police, <http://www.police.gov.il/contentPage.aspx?pid=308&mid=9>.

[76] Ministry of Public Security, Information Center, ´New National Crime Unit Inaugurated`, <http://mops.gov.il/Documents/Publications/InformationCenter/Innovation%20Exchange/Innovation%20Exchange%2014/LAHAV433.pdf>.

[77] Ministerial Committee on National Security Affairs, Decision B/84 of December 11, 2002, 'Responsibility for the Protection of Computerised Networks in the State of Israel' (Hebrew). The wording "critical infrastructures was not used, rather, 'supervised' and 'protected' entities.

[78] Law for Regulating Security in Public Bodies, <http://www.nevo.co.il/law_html/Law01/111M1_001.htm>. See also Goldschmidt, Roi, 'Cyberspace and the Protection of Critical Infrastructure', (Hebrew), Knesset Center for Research and Information, 12 May 2013, <http://www.knesset.gov.il/committees/heb/material/data/mada2013-05-13.doc>; Haber, Eldar and Zarsky, Tal, 'Means of Protection of Essential Infrastructure in Israel's Cyberspace' (Hebrew), *Mishpat UMimshal*, Vol. 18 (forthcoming) < http://weblaw.haifa.ac.il/he/Journals/lawGov/17/cyberspaceProtec.pdf>; and 'Cybersecurity for Infrastructure: A Critical Analysis', 43 Florida State Law Review (forthcoming).

The authorities of NISA in this respect are currently transitioning to the NCSA.[79] Currently, the INCB chairs the committee that vets and approves the regulation of critical infrastructure.[80] It should be noted that specific entities are regulated , in contrast to a sectoral approach.[81]

3.3.1. Emergency preparedness and crisis management

Israel's emergency preparedness and civilian crisis management, including online aspects of preparedness, is under the responsibility of the Ministry of Public Security, the Ministry of Defense and the Home Front Command.[82] NISA and NCSA also hold responsibility, respectively within their areas of authority, for emergency preparedness and functioning of certain entities.

The **National Emergency Management Authority**[83] has carried out exercises, in conjunction with the IDF Home Front Command, that include elements dealing with cyber attacks that target critical infrastructure, such as the national electricity grid.

3.4. Military cyber defence and cyber intelligence

As mentioned above, the **IDF** is engaged with cyber security as an integral part of its military strategy and is in the process of establishing the structure and authority of its cyber command. [84] In addition, the IDF Cyber Defender training course was instituted in 2012, in addition to several other military training programmes for military cyber security.[85]

Cyber intelligence in Israel is within the purview of the military and defence sectors.[86] The collection and processing of cyber intelligence, which is classified by nature, is conducted in accordance with the relevant legal obligations, including, as applicable, the Surveillance Law of 1979[87] and the Protection of Privacy Law of 1981.[88]

3.5. Private sector involvement and cooperation between academia and the business sector

Israel has been among the pioneers of multi-stakeholder cyber security cooperation among government, academia, and private sector entities. Cooperation in the cyber security field is a natural extension of the already-existing paradigm of such national cooperation in other areas.

One of Israel's flagship initiatives in this respect is the CyberSpark Innovation Initiative project in Beersheba.[89] It was established in 2014 as a joint venture of the INCB, the Municipality of Beersheba, Ben Gurion University, and industrial partners such as EMC (RSA), Lockheed Martin, IBM, Deutsche Telekom, JVP Cyber Labs and Elbit. The IDF and CERT-IL are also involved with CyberSpark initiatives, which also include outreach to the diplomatic community

[79] Resolution 2444, (n 36), art 9.
[80] See Goldschmidt, (n 77).
[81] The changing role of NISA in this respect, following the establishment of the NCSA, was addressed in legislation passed by the Knesset in August 2016, see Resolution 2444, (n 36), art 9; Security Regulation Act for Public Bodies (Order), 2016, <http://www.justice.gov.il/SitePages/OpenFile.aspx?d=4A49CqZQMS1fP4a9tebtos0BjvZ2KvXSHziexf6Zm0Y%3D> (Hebrew).
[82] Ministry of Public Security, Public Information in Emergency Crisis Situations, <http://mops.gov.il/English/HomelandSecurityENG/Pages/IE_17_PublicInfoEmegency.aspx>.
[83] The functions of this now-defunct Authority have been transferred several times between ministries, and are currently within the Ministry of Defense.
[84] Elran, Meir and Siboni, Gabi, 'Establishing an IDF Cyber Command', INSS Insight No. 719, 8 July 2015.
[85] IDF Spokesman, 'IDF's Cyber Defenders Complete Training Course', 25 January 2013, <http://www.idf.il/1283-18154-en/Dover.aspx>.
[86] Elran and Siboni, (n 84).
[87] Surveillance Law of 1979, <http://www.nevo.co.il/law_html/Law01/077_001.htm>.
[88] Protection of Privacy Law,(n 43).
[89] CyberSpark Innovation Initiative project, <http://www.cyberspark.org.il/#!about-cyberspark/c1a40>.

and the hosting of executive seminars for cyber security personnel from around the globe. Since its launch, CyberSpark has created a multi-stakeholder 'eco-system' for government, academia, industry, local government and civil society.[90]

Government support for Israel's cybersecurity industry and business sector comes from several sources. The Office of the Chief Scientist in the Ministry of the Economy (now the **National Authority for Technological Innovation**) has provided a variety of R&D and investment instruments through its R&D fund, the *Kidma* and *Magnet* programmes, and incubator support; and the *Meimad* programme supports dual-use cyber R&D.[91] Some of these initiatives are also supported in cooperation with the INCB.

3.5.1. Private sector

There are approximately 360 cyber security companies in Israel, and measurement of the sector in 2016 estimated Israeli exports of cyber-related products and market financing, respectively, at approximately USD 6 billion.[92] This performance relies on business relationships with both academia and the government, as well as more mature companies 'mentoring' start-ups. One example is the Israel Electric Company's entering into a joint venture in 2013 with young entrepreneurs to open CyberGym, a successful cyber defence training and consulting firm. Several government initiatives for international outreach and cooperation are also ongoing.[93]

In addition to the CyberSpark initiative discussed above, some 20 cybersecurity R&D centres have been established in Israel by multinational corporations in order to develop security solutions for the global market. These include PayPal, IBM, VMWare, General Electric, Cisco, CA Technologies, McAfee, and Ciscom. A number of other global corporations are also establishing cyber centres in Israel at present.

Israel Aerospace Industries (IAI) leads the Israeli Cyber Companies Consortium (IC3) – a group of Israel's leading cyber companies with complementary realms of expertise. IC3 was launched in January 2016 as part of the Israeli Ministry of Economy's Consortium programme. IC3 members cooperate with leading government cyber defence organisations, cutting-edge technology companies, start-ups and international cyber and intelligence companies.[94]

3.5.2. Academia

Israel has nine research universities, two of which were ranked among the top 100 academic institutions worldwide in 2016 and include computer science departments (Hebrew University and the Technion).[95] In keeping with the national prioritisation and funding of academic cyber security studies by the Ministry of Science, Technology and Space in 2012, the INCB has reached agreements to establish dedicated cyber centres of excellence at several universities, beginning with the establishment of an interdisciplinary cyber research centre at the University of Tel Aviv in 2014.[96] The technology transfer companies associated with all Israeli universities provide a ready-made

[90] CyberSpark Innovation Initiative project, <http://www.cyberspark.org.il/#!new-page/cwzu>.
[91] Office of the Chief Scientist, 'R&D Incentive Programs', pp. 9-10, <http://www.economy.gov.il/Publications/Publications/DocLib/RnD_IncentivePrograms_English.pdf>.
[92] Start-Up Nation Central, (n 5), pp. 3-4; CSIS and Intel Security, 'Report: Hacking the Skills Shortage', 2016, p. 10, <http://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf>; The Economist, 'Israel's Computer Security Firms', 1 August 2015, <http://www.economist.com/news/business/21660112-internet-security-has-become-bigger-export-earner-arms-cyber-boom-or-cyber-bubble >.
[93] Several industry and civil society organisations provide support for the cyber security industry and businesses, including the Israel Export Institute, the Association of Electronics and Software Industries and the Herzliya Accelerator Center.
[94] Israeli Cyber Companies Consortium (IC3), <http://www.iai.co.il/Sip_Storage//FILES/4/42124.pdf>.
[95] Shanghai Ranking, World University Rankings, <http://www.shanghairanking.com/World-University-Rankings-2016/Israel.html>.
[96] Blavatnik Interdisciplinary Cyber Research Center, <https://icrc.tau.ac.il/>.

mechanism for cooperation with the business sector, while protecting academics' research and intellectual property.[97]

At the secondary school level, Israel provides a number of national-level cyber security study and training programmes. The *Magshimim* and *Nitzanei Magshimim* programmes operate as after-school enrichment modules for students on the country's geographical and social periphery.[98] The *Gvahim* programme prepares pupils for a high school matriculation exam in cyber security, maths and computer science. All of these programmes receive support from the Ministry of Education, the IDF and the INCB.

Israel's prioritisation of academic inquiry and scientific research places the country 7th among OECD countries for ICT-related patents.[99] Additionally, the World Economic Forum's Global Competitiveness report for 2015-2016 rates Israel 3rd globally for innovation and 15th for technological readiness out of 144 global economies.[100] The country is connected with several global research and development networks, including Next Generation Internet, the US's Internet 2 Network, the EU's GEANT data network for the research and education community, and Seventh Framework Programme (FP7), the London-based Point of Presence, the Global Forum for Cyber Expertise, and the Mediterranean Consortium Quantum extension, Q-Med. Ongoing ICT and cyber security research cooperation between the industrial and academic sectors in Israel is supported and facilitated, in particular, by the Prime Minister's Office, the Ministry of Science, and the Chief Scientist of the Ministry of the Econom National Authority for Technological Innovation .[101] Within the Ministry of Defense and in cooperation with the Israeli Defence Forces (IDF), the Directorate of Defence R&D (*Mafat*) heads similar initiatives[102] and has a dedicated cyber research unit.[103] It also cooperates with the INCB, as with the *Masad* programme promoting dual-use cyber technology development.

[97] The national umbrella organisation is the Israel Tech Transfer Organisation, <http://www.ittn.org.il/about.php?cat=18&incat=0>.
[98] The *Magshimim* program webpage, <http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Magshimim%20Leumit%20program.pdf>.
[99] OECD, 'Digital Economy Outlook 2015', Table 1.8, <http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/oecd-digital-economy-outlook-2015_9789264232440-en#page43>.
[100] World Economic Forum, 'Global Competitiveness Report 2015-2016', <http://reports.weforum.org/global-competitiveness-report-2014-2015/economies/#economy=ISR>.
[101] This governmental unit was formerly the Chief Scientist of the Ministry of the Economy, and was given an autonomous statutory status as the National Authority for Technological Innovation in October 2015 by Amendment No. 7 to the Promotion of Industrial Research and Development Law, 5775-2015. The amendment came into effect on 1 January 2016.
[102] See Tabansky and Israel, (n 34).
[103] Israel Defense, 'New Cyber Directorate in Mafat', 12 March 2013, <http://www.israeldefense.co.il/en/content/new-cyber-directorate-mafat>.

Abbreviations

CERT	Computer Emergency Response Team
CERT-IL	Israel National Cyber Event Readiness Team
GDP	Gross Domestic Product
GSS	General Security Service
ICT	Information and Communications Technology
IDF	Israel Defense Forces
IIX	Israel Internet eXchange
INCB	Israeli National Cyber Bureau
ISP	Internet Service Provider
ITU	International Telecommunication Union
NCSA	National Cyber Security Authority
NIS	Israeli New Sheqel
NISA	National Information Security Agency
OECD	Organisation for Economic Co-operation and Development
R&D	Research and Development
UK	United Kingdom (of Great Britain and Northern Ireland)
UN	United Nations
US	United States (of America)
USD	US Dollar

References

Policy

Bank of Israel, Supervisor of Banks, 'Letter on Risk Management in a Cloud Computing Environment', 29 June 2015, <http://www.boi.org.il/en/BankingSupervision/LettersAndCircularsSupervisorOfBanks/LettersOfTheBankingSupervisionDepartment/201514en.pdf>

Bank of Israel, Supervisor of Banks, 'Proper Conduct of Banking Business Directive 361 on Cyber Defense Management', 16 March 2015, <http://www.boi.org.il/en/BankingSupervision/SupervisorsDirectives/ProperConductOfBankingBusinessRegulations/361_et.pdf>

Bank of Israel, Supervisor of Banks, Proper Conduct of Banking Business Directive 418, 'Opening of Accounts via the Internet', 15 July 2014, <http://www.boi.org.il/he/BankingSupervision/LettersAndCircularsSupervisorOfBanks/HozSup/2427.pdf>

Director-General of the Ministry of Health, 'Data Protection in Computerized Systems in the Health Sector', Directive 3/15, 15 February 2015, (Hebrew), <http://www.health.gov.il/hozer/mk03_2015.pdf>

INCB, 'Background for the Government Resolutions Regarding Advancing the National Preparedness for Cyber Security and Advancing National Regulation and Governmental Leadership in Cyber Security', < http://www.pmo.gov.il/Secretary/GovDecisions/2015/Pages/des2443.aspx>

INCB, 'Policy on Regulation of Cybersecurity Professions' 2015, (Hebrew), <http://www.pmo.gov.il/SiteCollectionDocuments/cyber/hagana.pdf>

Israel Defence Forces, 'IDF Strategy', 2015 (Hebrew), <http://www.idf.il/SIP_STORAGE/FILES/9/16919.pdf>

Ministerial Committee on National Security Affairs, Decision B/84 of December 11, 2002, 'Responsibility for the Protection of Computerized Networks in the State of Israel' (Hebrew)

Report of the Public Committee for the Defining Cyber Defense Professions ('Shafran Committee Report') August 2014, (Hebrew)

State Controller and Ombudsman, 'Critique and Oversight in Information Systems', 4th ed., 2005 (Hebrew), <http://www.pmo.gov.il/BikoretHamedina/files/bakarot%20ve%20bikoret%202005.doc>

Supervisor of Capital Markets, 'Management of Cyber Risks in Institutional Bodies' (Hebrew), 31 August 2016, <www.mof.gov.il/hon/documents/וחקיקה-הסדרה/.../th_2014-117.pdf>

Law

Communications (Telecommunications and Broadcasting) Law of 1982 <http://www.nevo.co.il/law_html/Law01/032_002.htm>

Computers Law of 1995, <http://law.co.il/media/computer-law/computers_law_nevo.pdf>

Electronic Signature Law of 2001
<http://www.financeisrael.mof.gov.il/FinanceIsrael/Docs/En/legislation/Others/5761-2001_Electronic_Signature_Law.pdf>

Encouragement for Industrial Research and Development Law of 1984,
<http://www.tamas.gov.il/NR/exeres/DEAF9131-D2B3-4BA4-A804-B10C6BC7E2F7.htm>

Inclusion of Biometric Means of Identification in Identity Documents and in an Information Database Law of-2009, <http://smartid.gov.il/SiteCollectionDocuments/bio_law.pdf>

Law for Regulating Security in Public Bodies of 1998
<http://www.nevo.co.il/law_html/Law01/111M1_001.htm>

Protection of Privacy Law of 1981,
<http://www.justice.gov.il/En/Units/ILITA/Documents/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf>

Regulation No. 5761-2001 on Privacy Protection (Transfer of Data to Databases Abroad),
<http://www.justice.gov.il/En/Units/ILITA/Documents/PrivacyProtectionTransferofDataabroadRegulationsun.pdf>

Supervision of Security Exports Law of 2007
<http://www.moital.gov.il/NR/exeres/D7EEC291-DF6C-4AE9-856F-1D45624DB4B0.htm>

Israel Government, Government Resolution 3058 27 March 2011
<http://www.pmo.gov.il/Secretary/GovDecisions/2011/Pages/des3058.aspx>

Israel Government, Government Resolution 2097, 10 October 2014
<http://www.pmo.gov.il/Secretary/GovDecisions/2014/Pages/dec2097.aspx>

Israel Government, Government Resolution No. 2444, 15 February 2015, Advancing the National Preparedness for Cyber Security, (Hebrew), < http://www.pmo.gov.il/Secretary/GovDecisions/2015/Pages/des2444.aspx>; (English)
<https://ccdcoe.org/sites/default/files/documents/Government%20Resolution%20No%202444%20-%20Advancing%20the%20National%20Preparedness%20for%20Cyber%20Security.pdf>.

Israel Government, Government Resolution No. 1046, 15 December 2013, The National Inititative 'Digital Israel' (Hebrew)

Israel Government, Government Resolution No. 3611, 7 August 2011, Advancing the National Capacity in Cyberspace
<http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf>

Other

Bezeq, 'Life in the Digital Age' (Hebrew), 2017, <http://www.bezeq.co.il/media/PDF/internetreport_2016.pdf>

CBS, 'Statistical Abstract of Israel 2015',
<http://www.cbs.gov.il/reader/shnaton/templ_shnaton_e.html?num_tab=st09_07&CYear=2015>

Council of Europe, Convention on Cybercrime, Chart of signatures and ratifications,
<https://www.coe.int/en/web/conventions/full-list/conventions/treaty/185/signatures?p_auth=ATj3pi6h>

CSIS and Intel Security, 'Report: Hacking the Skills Shortage', 2016,
<http://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf>

CyberSpark Innovation Initiative project, <http://www.cyberspark.org.il/#!about-cyberspark/c1a40>

The Economist, 'Israel's Computer Security Firms', 1 August 2015,
http://www.economist.com/news/business/21660112-internet-security-has-become-bigger-export-earner-arms-cyber-boom-or-cyber-bubble.

Goldschmidt, R., 'Cyberspace and Protection of Critical Infrastructures', Knesset Center for Research and Information, 2013 (Hebrew)

Hathaway, Melissa, Cyber Readiness Index 2.0, Potomac Institute, 2015.

Herzog, Mike, 'New IDF Strategy Goes Public', 28 August 2015 , <http://www.washingtoninstitute.org/policy-analysis/view/new-idf-strategy-goes-public>

IDF Spokesman, 'IDF's Cyber Defenders Complete Training Course', 25 January 2013, <http://www.idf.il/1283-18154-en/Dover.aspx>

Israel Defense, 'New Cyber Directorate in Mafat', Israel Defense, 12 March 2013,
<http://www.israeldefense.co.il/en/content/new-cyber-directorate-mafat>

Israeli Internet Association, Statistics Database (Hebrew), <http://en.isoc.org.il/tech_eng/sts_eng.html>

Israel National Cyber Event Readiness Team CRT-IL, <https://cert.gov.il/CERT-IL/Pages/CERT-IL.aspx>

ITU and UNESCO, 'The State of Broadband 2016',
<http://www.broadbandcommission.org/Documents/reports/bb-annualreport2016.pdf>

Elran, Meir and Siboni, Gabi, 'Establishing an IDF Cyber Command', INSS Insight No. 719, 8 July 2015.

Lewis, James, 'Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States,' Inter-American Development Bank, 2016,
<https://publications.iadb.org/bitstream/handle/11319/7759/ Advanced-Experiences-in-Cybersecurity-Policies-and-Practices-An-Overview-of-Estonia-Israel-South-Korea-and-the-United%20States.pdf?sequence=2>.

Ministry of Communications, 'Telecommunications in Israel 2013',
<http://www.moc.gov.il/sip_storage/FILES/5/605.pdf>.

National Cyber Initiative, 'Special Report for the Prime Minister', National Council on Research and Development, Ministry of Science, May 2011 (Hebrew)

OECD, 'Digital Economy Outlook 2015', < http://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm>

Office of the Chief Scientist, 'R&D Incentive Programs', <http://www.economy.gov.il/Publications/Publications/DocLib/RnD_IncentivePrograms_English.pdf>

UNGA, 'Report of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', 22 July 2015, <http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174>

Raska, Michael, 'Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy', RSIS Policy Report, 8 January 2015, <https://www.rsis.edu.sg/rsis-publication/gpo/confronting-cybersecurity-challenges-israels-evolving-cyber-defence-strategy/#.WGOXhfl97SE>

Start-Up Nation Central, 'Israel's Cybersecurity Industry In 2016', 2017

Tabansky, Lior and Ben Israel, Isaac, 'Cybersecurity in Israel', Springer, 2015

Tsipori, Tali,'Israeli cybersecurity grabs 8% global market share', Globes, 4 April 2016, <http://www.globes.co.il/en/article-israeli-cyber-industry-hits-the-big-time-1001114669>

World Economic Forum, 'Global Competitiveness Report 2014-2015', <http://reports.weforum.org/global-competitiveness-report-2014-2015/economies/#economy=ISR>