

Unveiling Israel's Cyber Legal Landscape: A Comprehensive Analysis of Cybersecurity Regulations and Policies

Lecturer **Adriana-Iuliana STANCU**¹

Dr. **Tal PAVEL**²

Abstract

The world's countries formulate laws, regulations and legal frameworks to define broad aspects of cyberspace within their domain, including institutions responsible for the local cyberspace, their areas of activity and responsibility, administrative subordination and even those who stand at their heads—including the definition of criminal activities in cyberspace, crime and terrorism, and topics such as the state's cyber borders and sovereignty, the citizens' online information security as well as their right to online privacy and the ways to ensure it. The research examines Israel's governmental activity to regulate cyberspace, the scope of the existing regulations and laws, their development over the years, and an attempt to fill in the gaps in the current regulation activities of cyberspace in Israel. The findings reveal that despite Israel being a cyber power based on various international indicators and media references over the years, and despite the activity of the Israel government starting in 1997 to regulate the issue of cyberspace, Israel currently lacks a governmentally approved cyber law defining Israeli cyberspace, institutions, activities and responsibilities. Further research may compare Israel's cyber regulations with other similar cyber nations and portray differences and lessons to be learned by Israel to regulate its cyberspace, in addition to Israel's involvement in international cyber conventions and regulations.

Keywords: cyber; law; policy; Israel; cybersecurity.

JEL Classification: K23, K24

1. Introduction

Israel has been considered a cyber power³ and even a top or a leading cyber power⁴. On the contrary, reports and indexes do not consider Israel among the top global cyber power: (1) International Institute for Strategic Studies (IISS) rank Israel in tier two of global cyber powers with Australia, Canada, China, France, Russia and the UK⁵; (2) the ITU Global Cybersecurity Index Israel at the rank 36 out of 194 countries, and rank 23 out of Europe countries⁶; (3) the National Cyber Security Index (NCSI) on December 2021 ranked Israel 37 out of 175 countries, with a constant decline from rank 24 in 2019⁷; (4) the National Cyber Power Index 2022 ranked Israel 19 out of 30 countries⁸ and (5) the Cyber Defense Index that does not include Israel among the "world's major economies according to their collective cybersecurity assets, organisational capabilities, and policy stances"⁹.

Since some of those indexes include the cyber legal framework and measures as indicators for national cyber capabilities, it is necessary to analyse the legislation adopted by Israel to regulate

¹ Adriana-Iuliana Stancu - „Dunărea de Jos” University of Galati, Romania, Director of the Legal Science Department, Faculty of Law, and Administrative Sciences, adriana.tudorache@ugal.ro.

² Tal Pavel - Founder & Director, The Institute for Cyber Policy Studies, Israel, taloo88@gmail.com.

³ Amsellem, D. (2020). Israel cyber power. *Herodote*, 177178(2), 281–296. <https://doi.org/10.3917/HER.177.0281>; Coillet-Matillon, P. (2022, November 15). *Behind the scenes of Israel's cyber power*. InCyber. <https://incyber.org/en/behind-scenes-israel-cyber-power/>; Matania, E., Cilluffo, F. J., & Cardash, S. L. (2017). *Israel: The Making of a Cyber Power (Case Study)*. <https://www.jstor.org/stable/resrep21011.9>.

⁴ Freilich, C. D. (Charles D., Cohen, M. S., & Siboni, G. (n.d.). *Israel and the cyber threat: how the startup nation became a global cyber power*; 26. Patra, A. (2022, April 19). The Journey of Israel to become a top Cyber Power. Technotification. <https://www.technotification.com/2022/04/journey-of-israel-to-become-top-cyber-power.html>; Tabansky, L. (2022, March 21). *How Israel Became a Top Cyber Power*. The National Interest. <https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/how-israel-became-top-cyber-power>; *Threat profile - Israel*. (n.d.). Hunt & Hackett. Retrieved 15 June 2023, from <https://www.huntandhackett.com/threats/israel>.

⁵ *Cyber Power – Tier Two*. (2021, 28 June). International Institute for Strategic Studies (IISS). <https://www.iiss.org/research-paper/2021/06/cyber-power---tier-two/>.

⁶ Global Cybersecurity Index 2020. (2021). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf. 1.

⁷ *NCSI: Israel*. (2021, 22 December). National Cyber Security Index (NCSI). <https://ncsi.ega.ee/country/il/>.

⁸ Voo, J., Hemani, I., & Cassidy, D. (2022). *National Cyber Power Index 2022*. www.belfercenter.org/project/cyber-project.

⁹ The Cyber Defense Index 2022/23. (2023). In MIT Technology Review. <https://mittrinsights.s3.amazonaws.com/CDIreport.pdf>.

cyberspace. Based on Israel's official cyber legal regulations, the research questions are: (RQ1) What topics and domains are covered and discussed in the Israeli cyber regulations? (RQ2) What are the changes and developments in Israeli Cyber regulations? (RQ3) What is the maturity of Israel's official cyber regulations?

2. Government resolutions

The regulation of the defence of Israel's cyberspace began two and a half decades ago with different regulations that most of the private sector in Israel is not subject to any binding regulation. At the same time, the state "relies on market forces and collaboration in order to find the correct balance between suitable protection and the cost of achieving it" while imposing regulations on private companies in sectors considered critical infrastructure¹⁰.

The following part will detail the significant milestones in the regulations of cyberspace and cybersecurity in Israel:

- **1997 - TEHILA.** The researchers agree that 1997 was the major milestone in Israel's Cyberspace with the establishment of TEHILA (a Hebrew acronym for the Government Infrastructure for the Internet Era) in the office of the Accountant General in the Ministry of Finance as the e-government platform and "one of the first governmental cybersecurity agencies in the world" to provide government offices and authorities with a secure and protected platform for connection to the Internet, secured infrastructure for the provision of services to the public and to meet the cyber threat¹¹. The Center for Israel Government Information Security was established at TEHILA to confront cyber threats. Among its functions were "following up on information security events around the world with particular attention to network attacks of concern to Israel, coordinating among governmental bodies in order to solve security problems, connecting government bodies with external bodies, and conducting research in the field", with a CERT team (Computer Emergency Response Team) operated as part of TEHILA aimed to "provide immediate response to information security events in government organizations or bodies of international size"¹².

- **2002 - National Information Security Authority (NISA).** Decision B/84 of the Ministerial Committee on National Security regarding "Responsibility for the Protection of Computerized Systems in the State of Israel, 2002", established the National Information Security Authority (NISA), operating within the General Security Service (GSS), to instruct and protect vital computerized systems of selected public and private civil organizations, mainly its critical national infrastructure¹³.

- **2011 - Israel National Cyber Bureau (INCB).** Government Resolution 3611, from 27 August 2011, established the Israel National Cyber Bureau (INCB) under the Prime Minister's office as the first national advisory and consolidating body for cyber security. The resolution defines "cyberspace", "cyber security", and "civilian space", among others¹⁴.

- **2014 - ICT Authority.** Government Resolution 2099, from 10 October 2014, established Israel's ICT Authority "to serve as a center of knowledge and professional advice for IT services, make information system more efficient, promote technological innovation among ministries and units, put at their disposal advanced technologies to improve services to the public and minimize bureaucracy, and promote an open government policy". One of the several core objectives of the ICT

¹⁰ Siboni, G., & Sivan-Sevilla, I. (2019). *Regulation in Cyberspace*. https://www.inss.org.il/wp-content/uploads/2019/04/Memo190new_e.pdf.

¹¹ Cohen, M. S., Freilich, C. D., & Siboni, G. (2015). Israel and Cyberspace: Unique Threat and Response. *International Studies Perspectives*, 1–15. <https://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/Israel%20and%20cyberspace.pdf>; Deputy FM Elkin: *Israel's Cyber Security 16 October 2013*. (2013, 16 October). Israel Ministry of Foreign Affairs. <https://embassies.gov.il/MFA/PressRoom/2013/Pages/Deputy-FM-Elkin-Israel's-Cyber-Security-16-Oct-2013.aspx>; Even, S., & Siman-Tov, D. (2012). *Cyber Warfare: Concepts and Strategic Trends*. [https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/\(FILE\)1337837176.pdf](https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/(FILE)1337837176.pdf); Housen-Couriel, D. (2017). *National Cyber Security Organisation: ISRAEL*. https://ccdcoe.org/uploads/2018/10/IL_NCSO_final.pdf.

¹² Even, S., & Siman-Tov, D., *op. cit.*, 2012.

¹³ Cohen, M. S., Freilich, C. D., & Siboni, G. (2015). Israel and Cyberspace: Unique Threat and Response. *International Studies Perspectives*, 1–15. <https://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/Israel%20and%20cyberspace.pdf>; *Israel National Cyber Security Strategy in Brief*. (2017).

¹⁴ Advancing National Cyberspace Capabilities, Prime Minister Office (2011).

Authority is the Cyber Defense, defined as "the authority will work through the units towards cyber defense, promoting information security and cyber defense through guidelines, controls and enforcement. The authority will also establish a national Security Operations Center (SOC) to manage cyber threats"¹⁵.

• **2015 - Israel National Cyber Security Authority (INCSA).** Government Resolution 2444, from 15 February 2015, formed the Israel National Cyber Security Authority (INCSA) under the Prime minister's office and established the national CERT¹⁶.

• **2016 - The IDF Strategy.** Israel Defense Forces strategy from July 2016 asserting the need for "force buildup in Cyberspace" to be based on:

a) "Establishing a Cyber Arm, which will serve as a Principal Command, subordinate to the Chief of the General Staff, for operations and force buildup of the IDF's cyberspace capabilities. It will be in charge for planning and implementing the cyber domain campaign.

b) Development of technological capabilities for cyber defense for the operational capabilities and for supporting capabilities (personnel, logistical systems)"¹⁷.

• **2017 - Israel National Cyber Directorate (INCD).** Government Resolution 3270, dated 17 December 2017, merged the Israel National Cyber Bureau (INCB) and Israel National Cyber Security Authority (INCSA) into one centre, the Israel National Cyber Directorate (INCD)¹⁸.

• **2018 – Israel Cyber Security Draft Bill.** On June 2018, the Israel National Cyber Directorate (INCD) published the Cyber Security Draft Bill for the public's comments to regulate the INCD activity while implementing the government's decisions. The draft bill is the latest stage of creating a national cyber security authority as part of the national cyber security authority. It contains three chapters: (1) the organizational chapter - which defines the organizational aspects of the INCD, (2) the operative chapter – which defines the powers required to detect cyber attacks and deal with them, (3) The regulatory chapter – which defines the with national and sectoral regulation to raise the level of resilience of the sectors and determines the role of the INCD as the national regulation in the field of cyber security. During 2019-2020, the INCD performed more than 30 meetings with relevant individuals, institutions and government ministries to discuss the comments on the draft bill¹⁹.

On March 2021 published, the draft bill of cyber defence and the National cyber directorate based on the 2018 draft bill²⁰. The draft bill gained widespread criticism regarding the power granted to the INCD and the citizen's privacy²¹.

The following table present Israel's cyber policy papers, regulations and draft bills between 1995 and 2021²².

¹⁵ *Strategic Plan 2016-2018*. (2016). https://www.gov.il/blobFolder/generalpage/stratigy_eng/he/STRATIGY-%20ICT%20ATHORITY%20-%20ENGLISH.pdf.

¹⁶ Advancing National Regulation and Governmental Leadership in Cyber Security, 2015; Advancing the National Preparedness for Cybersecurity, 2015

¹⁷ *The IDF Strategy*, 2016.

¹⁸ Government Resolution 3270, Prime Minister Office (2017). https://www.gov.il/he/Departments/policies/dec_3270_2017.

¹⁹ Cahane, A. (n.d.). *The New Israeli Cyber Draft Bill – A Preliminary Overview*. The Federmann Cyber Security Center – Cyber Law Program. Retrieved 16 June 2023, from <https://csrcl.huji.ac.il/news/new-israeli-cyber-law-draft-bill>; Cyber Security Draft Bill, Israel National Cyber Directorate (2018). <https://www.gov.il/he/departments/news/cyberlawpublic>; Levush, R. (2019). Israel: Knesset Passes Amendment Law Recognizing Role of National Cyber Directorate in Protecting Cyberspace. *Library of Congress, Washington, D.C. 20540 USA*. <https://www.loc.gov/item/global-legal-monitor/2019-07-22/israel-knesset-passes-amendment-law-recognizing-role-of-national-cyber-directorate-in-protecting-cyberspace/>.

²⁰ *Powers for Strengthening Cyber Defense (Provisional Measure) Bill*, 1 (2021). <https://www.gov.il/he/Departments/Policies/principles>.

²¹ Housen-Couriel, D., Mimran, T., & Shany, Y. (2021, 7 May). *Israel's Version of Moving Fast and Breaking Things: The New Cybersecurity Bill*. Lawfare. <https://www.lawfareblog.com/israels-version-moving-fast-and-breaking-things-new-cybersecurity-bill>; Ravia, H., Hammer, D., & Amir, A. (2021). *Cybersecurity*; Schwartz-Altshuler, T. (2023, 5 January). *Israel's cybersecurity is a ticking time bomb*. The Jerusalem Post. <https://www.jpost.com/opinion/article-726659>.

²² *Index of Israeli Cyber Laws and Regulations*. (2021). <https://ccdcoe.org/uploads/20/Israel-Cyber-Policy-Portal>. (2022, November). United Nations Institute for Disarmament Research. <https://cyberpolicyportal.org/states/israel>.

Table 1

Subject	Topic	Name	Resolution	Publisher	Date
Cybersecurity Policy	Strategy Documents	Israel National Cybersecurity Strategy	"Israel's national cyber security strategy is, first and foremost, a means of realizing the Israeli cyber vision by keeping cyberspace safe and by confronting the various cyber threats, in accordance with the country's national interests"	Prime Minister's Office; National Cyber Directorate	September 2017
		The IDF Strategy	Force Buildup in Cyberspace, Defense and Offense in Cyberspace	Israel Defense Forces	July 2016
	Implementation Frameworks	Government Plans, 2017-2018	• Outlines implementation tasks for 2017-2018 for the National Cyber Bureau and National Cyber Security Authority (NCSA); • Resolves that the NSCA will continue to push forward innovative cybersecurity projects; • Resolves that technical systems built by the NSCA will be implemented; Outlines plan to transfer responsibilities for critical infrastructure protection from the security service to the NCSA	Government of Israel	5 March 2017
Structure	National Center or Responsible Agency	Israel National Cyber Bureau (INCB)	Mandated to formulate and promote the implementation of a comprehensive and formal cyber strategy, to articulate and lead national cyber policy	Prime Minister's Office	7 August 2011
		Israel National Cyber Security Authority (INCSA)	Had overall national responsibility for cyber defense: oversees cyber defense actions so as to provide a comprehensive response against cyber-attacks including dealing with threats and events in real time	Prime Minister's Office	September 2016
		Israel National Cyber Directorate (INCD)	Responsible for protecting the civilian cyber space	Prime Minister's Office	
	Key Positions	Head		Israel National Cyber Bureau (INCB)	December 2017
		Head		Israel National Cyber Security Authority (INCSA)	
	Dedicated Agencies and Departments	Knesset Subcommittee for Cyber Defense	Subcommittee of the Foreign Affairs and Defense Committee of the Knesset	The Knesset	
		Department of Emergency, Information Security and Cyber, State Attorney's Office	Responsible for the indictment and prosecution of criminals that have committed cybercrimes	Ministry of Justice	
	National CERT or CSIRT	Israel National Cyber Event Readiness Team (CERT-IL)	Encompasses all of Israel other than the military and Israeli critical infrastructure	Israel National Cyber Directorate (National Cyber Security Authority)	1 July 2014
Legal	Legislation	Computer Law, 1995	Specifies penalties for computer	Government of	25 October

Framework			offenses, including disrupting or interfering with a computer or computer material, false information or false output, unlawful penetration into computer material, and penetration into computer material in order to commit another offence	Israel	1995
		Government Resolution No. 3611	Advancing National Cyberspace Capabilities	Government of Israel	7 August 2011
		Government Resolution No. 2443	Advancing National Regulation and Governmental Leadership in Cyber Security	Government of Israel	15 February 2015
		Government Resolution No. 2444	Advancing the National Preparedness for Cybersecurity	Government of Israel	February 2015
		Government Resolution No. 3270	Merges National Cyber Bureau and National Cyber Security Authority into one center, the National Cyber Directorate	Government of Israel	17 December 2017
		2018 Memorandum of the National Cyber Directorate – Draft Bill in Progress		Government of Israel	2018
		2021 Proposed Law of the National Cyber Directorate		Government of Israel	2021
Cooperation	Multilateral Agreements	Convention on Cybercrime (Budapest Convention)	"a framework that permits hundreds of practitioners from Parties to share experience and create relationships that facilitate cooperation."	Council of Europe	1 September 2016
	UN Processes	Represented at the Group of Governmental Experts - Developments in the field of information and telecommunications in the context of international security		United Nations	2009
	Bilateral and Multilateral Cooperation	Australia-Israel Leaders' Roundtable in Cybersecurity and Memorandum of Understanding in Cybersecurity Cooperation	Exchange of views on challenges and best practice responses in the field of cyber security in the government and commercial context	Israel National Cyber Directorate	30 October 2017
		Discussions, Armenia-Israel	Discussions on several issues, including cybersecurity	Ministry of Regional Cooperation	26 July 2017
		Joint Statement, Visegrad (V4)-Israel	Agreed, inter alia, to explore the possibility of further strengthening joint cooperation in the areas of defense and defense industry, cyber security, hybrid threats, non-proliferation and information and know-how sharing	Prime Minister	19 July 2017
		Agreement of cooperation in the field of cyber-security, Japan-Israel	Increased investments and joint activity in this field, establishes joint training programs and joint work seminars	Ministry of Economy and Industry	11 May 2017
		Agreement, Honduras-Israel	Framework agreement between Honduras and the Israeli Ministry of Defense on a number of issues, including the establishment of a national CERT in Honduras	Ministry of Defense	23 March 2017

		Joint Statement, Australia-Israel	Agreed, inter alia, to explore opportunities for bilateral cooperation in the field of cyber as well as promote global cybersecurity efforts that enhance an open, free and secure internet	Prime Minister	22 February 2017
		Cooperation, Israel-Zambia, Ethiopia, Uganda, South Sudan, Rwanda, Kenya, Tanzania	Cooperation between Israel and 7 African countries on security and economic matters, including cyber security	Prime Minister	5 July 2016
		Global Forum on Cyber Expertise, Member	A global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building		2015
		Joint Cooperation in the Field of Cyber Security, Czech Republic-Israel	Agreement to share information, best practices and lessons learned regarding cyber security threats and events as well as other relevant issues related to their national cyber security frameworks	National Cyber Bureau	25 November 2014
	Membership	International Telecommunications Union (ITU)			

3. Multilateral treaty commitments

International Telecommunications Union Constitution Convention and Regulations – from its establishment in 1865, the International Telegraph (later Telecommunication) Conventions established the basic principles for international telegraphy, radiotelegraph, telecommunication and International Telecommunication²³. Israel signed 35 ITU agreements²⁴.

Budapest Convention (23 November 2001) – the Convention on Cybercrime²⁵ "is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception"²⁶. On 9 May 2016, Israel deposited accession to the Budapest Convention on Cybercrime and joined the 68 parties of the convention²⁷.

4. Conclusions

(RQ1) The cyber regulations of Israel reveal an ongoing activity to regulate the cyberspace of Israel, especially concerning cyber security and the ability of different sectors to protect themselves from cyber threats and attacks that prevent loss and damage, especially damaging the states and its components. Therefore, such regulations established the relevant governmental institutions, defining their authority, power and heads.

(RQ2) The development of cyber regulation in Israel consisted of two main phases but without a national strategic concept. (1) Cybersecurity regulations of the private sector are defined as critical

²³ *Constitution and Convention Collection*. (n.d.). International Telecommunication Union. Retrieved 16 June 2023, from <https://www.itu.int/en/history/Pages/ConstitutionAndConvention.aspx>.

²⁴ *List of Agreements for Israel*. (n.d.). International Telecommunication Union. Retrieved 16 June 2023, from <https://www.itu.int/online/mm/scripts/gensel26?ctryid=1000100566>.

²⁵ *The Budapest Convention (ETS No. 185) and its Protocols*. (n.d.). Council of Europe. Retrieved 16 June 2023, from <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.

²⁶ *Details of Treaty No.185*. (n.d.). Council of Europe. Retrieved 16 June 2023, from <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatyid=185>.

²⁷ *Israel joins Budapest Convention*. (2016, 9 May). Council of Europe. <https://www.coe.int/en/web/cybercrime/-/israel-joins-budapest-convention>.

to national security and consist of critical infrastructure. (2) the regulation covers the civilian sectors and transfers the state cyberspace's power from the intelligence agencies to a dedicated cyber²⁸.

(RQ3) Alongside with consistent and widespread cyber regulations across two and a half decades, the establishment of relevant government institutions and involvement in the international cyber process, multilateral agreements, and bilateral and multilateral cyber cooperation, Israel lacks a coherent and comprehensive cyber law, despite several attempts, and was not able to approve the cyber law draft bill since first publish to public comments on June 2018.

Future research may compare Israel's cyber regulations with other tier 1/tier 2 cyber power states, EU members and its neighbours.

Bibliography

1. Advancing National Regulation and Governmental Leadership in Cyber Security, Prime Minister Office (2015). https://www.gov.il/he/departments/policies/2015_des2443.
2. Advancing the National Preparedness for Cybersecurity, Prime Minister Office (2015). https://www.gov.il/he/departments/policies/2015_des2444.
3. Amsellem, D. (2020). Israel cyber power. *Herodote*, 177178(2), 281–296. <https://doi.org/10.3917/HER.177.0281>.
4. Cohen, M. S., Freilich, C. D., & Siboni, G. (2015). Israel and Cyberspace: Unique Threat and Response. *International Studies Perspectives*, 1–15. <https://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/Israel%20and%20cyberspace.pdf>.
5. Coillet-Matillon, P. (2022, November 15). *Behind the scenes of Israel's cyber power*. InCyber. <https://incyber.org/en/behind-scenes-israel-cyber-power/>.
6. *Constitution and Convention Collection*. (n.d.). International Telecommunication Union. Retrieved 16 June 2023, from <https://www.itu.int/en/history/Pages/ConstitutionAndConvention.aspx>.
7. *Cyber Power – Tier Two*. (2021, 28 June). International Institute for Strategic Studies (IISS). <https://www.iiss.org/research-paper/2021/06/cyber-power---tier-two/>.
8. Cyber Security Draft Bill, Israel National Cyber Directorate (2018). <https://www.gov.il/he/departments/news/cyberlawpublic>.
9. *Deputy FM Elkin: Israel's Cyber Security 16 October 2013*. (2013, 16 October). Israel Ministry of Foreign Affairs. <https://embassies.gov.il/MFA/PressRoom/2013/Pages/Deputy-FM-Elkin-Israel's-Cyber-Security-16-Oct-2013.aspx>.
10. *Details of Treaty No.185*. (n.d.). Council of Europe. Retrieved 16 June 2023, from <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185>.
11. Even, S., & Siman-Tov, D. (2012). *Cyber Warfare: Concepts and Strategic Trends*. [https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/\(FILE\)1337837176.pdf](https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/(FILE)1337837176.pdf).
12. Freilich, C. D. (Charles D., Cohen, M. S., & Siboni, G. (n.d.). *Israel and the cyber threat: how the startup nation became a global cyber power*.
13. *Global Cybersecurity Index 2020*. (2021). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.
14. Advancing National Cyberspace Capabilities, Prime Minister Office (2011). https://www.gov.il/he/departments/policies/2011_des3611.
15. Government Resolution 3270, Prime Minister Office (2017). https://www.gov.il/he/Departments/policies/dec_3270_2017.
16. Housen-Couriel, D. (2017). *National Cyber Security Organisation: ISRAEL*. https://ccdcoe.org/uploads/2018/10/IL_NCSO_final.pdf.
17. Housen-Couriel, D., Mimran, T., & Shany, Y. (2021, 7 May). *Israel's Version of Moving Fast and Breaking Things: The New Cybersecurity Bill*. Lawfare. <https://www.lawfareblog.com/israels-version-moving-fast-and-breaking-things-new-cybersecurity-bill>.
18. *Index of Israeli Cyber Laws and Regulations*. (2021). <https://ccdcoe.org/uploads/20>.
19. *Israel - Cyber Policy Portal*. (2022, November). United Nations Institute for Disarmament Research. <https://cyberpolicyportal.org/states/israel>.
20. *Israel joins Budapest Convention*. (2016, 9 May). Council of Europe. <https://www.coe.int/en/web/cybercrime/-/israel-joins-budapest-convention>.
21. Levush, R. (2019). Israel: Knesset Passes Amendment Law Recognizing Role of National Cyber Directorate in Protecting Cyberspace. *Library of Congress, Washington, D.C. 20540 USA*. <https://www.loc.gov/item/global-legal-monitor/2019-07-22/israel-knesset-passes-amendment-law-recognizing-role-of-national-cyber-directorate-in-protecting-cyberspace/>.

²⁸ Siboni, G., & Sivan-Sevilla, I. *op. cit.*, 2019.

22. *Israel National Cyber Security Strategy in Brief*. (2017).
23. *List of Agreements for Israel*. (n.d.). International Telecommunication Union. Retrieved 16 June 2023, from <https://www.itu.int/online/mm/scripts/gensel26?ctryid=1000100566>.
24. Matania, E., Cilluffo, F. J., & Cardash, S. L. (2017). *Israel: The Making of a Cyber Power (Case Study)*. <https://www.jstor.org/stable/resrep21011.9>.
25. *NCSI: Israel*. (2021, 22 December). National Cyber Security Index (NCSI). <https://ncsi.ega.ee/country/il/>.
26. Patra, A. (2022, April 19). *The Journey of Israel to become a top Cyber Power*. Technotification. <https://www.technotification.com/2022/04/journey-of-israel-to-become-top-cyber-power.html>.
27. *Powers for Strengthening Cyber Defense (Provisional Measure) Bill, 1* (2021). <https://www.gov.il/he/Departments/Policies/principles>.
28. Ravia, H., Hammer, D., & Amir, A. (2021). *Cybersecurity*.
29. Shwartz-Altshuler, T. (2023, 5 January). *Israel's cybersecurity is a ticking time bomb*. The Jerusalem Post. <https://www.jpost.com/opinion/article-726659>.
30. Siboni, G., & Sivan-Sevilla, I. (2019). *Regulation in Cyberspace*. https://www.inss.org.il/wp-content/uploads/2019/04/Memo190new_e.pdf.
31. *Strategic Plan 2016-2018*. (2016). https://www.gov.il/blobFolder/generalpage/stratigy_eng/he/STRATIGY-%20ICT%20ATHORITY%20-%20ENGLISH.pdf.
32. Tabansky, L. (2022, March 21). *How Israel Became a Top Cyber Power*. The National Interest. <https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/how-israel-became-top-cyber-power>.
33. *The Budapest Convention (ETS No. 185) and its Protocols*. (n.d.). Council of Europe. Retrieved 16 June 2023, from <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.
34. *The Cyber Defense Index 2022/23*. (2023). In *MIT Technology Review*. <https://mittrinsights.s3.amazonaws.com/CDIreport.pdf>.
35. *The IDF Strategy*. (2016).
36. Cahane, A. (n.d.). *The New Israeli Cyber Draft Bill – A Preliminary Overview*. The Federmann Cyber Security Center – Cyber Law Program. Retrieved 16 June 2023, from <https://csrcl.huji.ac.il/news/new-israeli-cyber-law-draft-bill>.
37. *Threat profile - Israel*. (n.d.). Hunt & Hackett. Retrieved 15 June 2023, from <https://www.huntandhackett.com/threats/israel>.
38. Voo, J., Hemani, I., & Cassidy, D. (2022). *National Cyber Power Index 2022*. www.belfercenter.org/project/cyber-project.