International Journal of Applied Technology & Leadership
ISSN 2720-5215
Volume 3, Issue 1, January 2024
ijatl@org

Defining Digital Boundaries: A Study on Israel's Cyber Sovereignty Policy

Tal Pavel, PhD

The Institute for Cyber Policy Studies (Israel)

Abstract

Objectives – The research aims to shed light on Israel's official policy towards defining its cyber sovereignty and boundaries based on official Israeli documents published by the Government of Israel, the Israel National Cyber Directorate and the Israel Defense Forces.

Prior Work – The terms "Cyber" and "Sovereignty" define two different domains, the artificial and the physical, which may have broad definitions. Therefore, the literature defines "Cyber Sovereignty" differently while reflecting the term's complexity. Over the years, researchers have analysed Israel's cyberspace from broad aspects. However, the literature lacks examination of the Israeli official stand towards cyberspace sovereignty and, therefore, the ability to draw its cyber boundaries based on official Israel publications.

Approach – The study analysed 17 of Israel's official publications, looking for the terms "Sovereignty" and "Boundaries" and general references to cyber sovereignty.

Results – None of the analysed publications referred directly to the terms "Sovereignty" and "Boundaries" relating to cyberspace—four defined Israeli cyberspace concerning civilian space, excluding the defense establishment but including elements outside national borders.

Implications – The research suggests that a lack of clarity and a well-defined term for "cyber sovereignty" as part of Israeli official documents and a lack of dedicated publications drawing cyber boundaries may be due to (1) strategic ambiguity of Israel's government not referring and defining its cyber sovereignty publicly, (2) lack of cyber

policy maturity of Israel's government regarding the definition of cyber-related terms, or a (3) combination of both. Therefore, the study emphasises the need for future research to analyse the definition of other cyber-related terms of Israeli cyberspace and compare with other states in the region and beyond to analyse the extent of the phenomenon and validate the current findings worldwide.

Keywords: Israel, Cyberspace, Policy, Sovereignty, Boundaries

1. Literature Review

Various terms describe the tangent lines between the digital world and the extent of state, organisation and individual authority. Different aspects of the ramifications of the power over its digital sphere, including technology, international relations, law, and ideology, exist (Lewis, 2020).

Therefore, the different terms constitute the combination of those of the digital world (Data, Internet, Network, Digital, Virtual, Cyber) with those of authority (Sovereignty, Governance), intending to define the ownership, control and security measures for internal and external purposes to confront a wide range of malicious physical and cyber actors and threats. Table 1 ("Digital World and Authority") indicates relevant research literature on the different terms.

		Authority	
		Sovereignty	Governance
Digital World	Data	(Hummel et al., 2021; Snipp, 2016)	(*Definition of Data Governance*, n.d.; *What Is Data Governance?*, n.d.)
	Internet	(Budnitsky & Jia, 2018; Sassen, 1998)	(*Internet Governance Glossary*, 2005; Mueller, 1996)
	Network	(Duarte, 2017; Li & Yang, 2021)	(Carlsson & Sandström, 2008; Sørensen, 2002)
	Digital	('Digital Sovereignty for Europe', 2020; *Navigating Digital Sovereignty and Its Impact on the Internet*, 2022)	(Erkut, 2020; Luna-Reyes, 2017)
	Virtual	(Kelton et al., 2022; Zhuk, 2023)	(Didehvar & Danaeefard, 2010; Taylor, 2023)
	Cyber	(Palaniappan, 2022; Wu, 1996)	(Jayawardane et al., 2015; Mihr, 2014)

Table 1 – Digital World and Authority

Out of the different terms, our research focuses on "Cyber Sovereignty" in Israel's cyberspace as reflected in official Israeli strategies, resolutions, and draft bills.

Cyber Sovereignty – is a vague concept combining two terms, each subject to many definitions and interpretations and representing entirely different and contradicting

domains, mainly because the Internet and cyberspace aim to enable the free flow of information in an environment with vague geographical borders. In contrast, sovereignty leads to control, restrictions, interventions and limitations in a specific and defined place, unit and territory. Therefore, defining Cyber sovereignty may be challenging.

Researchers described the problematic nature of Cyber, arguing that (1) humans have created cyberspace, (2) it is not static but instead continues to expand, (3) multiple stakeholders have been constantly involved in cyberspace since its creation, including governments, the private sectors and civil society, that (4) it is the technology that drives policy decisions, (5) the need of virtual borders in cyberspace to exercise states sovereignty due to cyber confrontations, (6) the technological dependencies on foreign countries, (7) the need for political considerations, (8) the cross-border nature of cyberspace challenges state sovereignty and (8) the fact that the foundation of cyberspace is the physical infrastructures which located in different states and subject to their national jurisdictions (Baezner & Robin, 2018; *Cyber Sovereignty*, n.d.; Palaniappan, 2022).

Thus, the vague concept of "Cyber Sovereignty" is reflected in different definitions. Some are crystal clear: "The application of principles of state sovereignty to cyberspace" (Baezner & Robin, 2018). Others reflect the complexity of defining "Cyber Sovereignty" and its ramifications for international relations.

Avner Simchoni defined well the ramifications of cyber on the very fundamental concepts of states, authority and sovereignty, asserting that "Cyber is also changing the balance of power and the sources of authority that we have known until now, including concepts of sovereignty, territory, monopoly over the means of violence, and changing the ability to use force" (Simchoni, 2017).

Muhammed Can argues that "Cyber Sovereignty" is "a phrase commonly used in the field of internet governance to define the will of states to exercise and sustain control over the Internet domain within their own borders, including political, economic, cultural and technological activities. However, it is not clear how to apply this sovereignty concept to current international relations and international laws" (Can, 2020).

Milton Mueller asserted in 1996 that "the state is tempted to reassert its traditional role, especially when cybersecurity intersects with national security and military power, as it increasingly does" (Mueller, 1996).

Israel Cyberspace – Numerous papers and researches analysed broad aspects of Israeli cyberspace and its operations, including structure (Topor, 2021), strategy (Adamsky, 2017; Siboni & Assaf, 2016), law (Ronen et al., 2018; Siboni & Sivan-Sevilla, 2017), military (Eizenkot, 2018), terrorism (Sharma, 2023), warfare (Cristiano, 2020), Artificial Intelligence (Antebi & Baram, 2020), cyber risk management (Siboni & Klein, 2018), industry (Tabansky & Ben Israel, 2015), international cooperation (Biji Ahuja, 2023), and much more cyber-related aspects.

Israel Cyber Sovereignty – Even though an Israeli official cyber perspective is general and, as a rule, unrelated to its cyber sovereignty, one may find several Israeli official

publications relating to the general concept of sovereignty in cyberspace, not necessarily Israeli cyberspace. Dr. Roy Schöndorf, who served as Israel's Deputy Attorney General (International Law), referred to cyber sovereignty in at least two formal publications. His words may shed some light on the Israeli stand towards its cyber sovereignty.

In December 2020, he addressed the problematic nature of applying laws in cyberspace, "it is not always easy to move from the general statement that international law applies to the cyber domain, to concrete legal rules that bind States and non-State actors in their actual behavior". He affirmed openly the ambiguity of Israel's official position in this regard, admitting that "Accordingly, the State of Israel has largely refrained thus far from making specific statements on whether and how particular rules apply. That is not to say that we take no position – indeed, we have consistently affirmed the application of international law to cyberspace in forums like the UN GGE and the Open-Ended Working Group".

He distinguishes between sovereignty that "connotes independence" and “territorial sovereignty”, which is an "international legal rule" and argues that "States undoubtedly have sovereign interests in protecting cyber infrastructure and data located in their territory. However, States may also have legitimate sovereign interests with respect to data outside their territory". Therefore, the direct conclusion is that "States occasionally do conduct cyber activities that transit through, and target, networks and computers located in other States", pointing to the existing international law (Schöndorf, 2020).

In October 2021, Dr Schöndorf presented the "Summary of Israel's Approach" towards the "Application of International Law to Cyberspace" as published by the Israel Ministry of Foreign Affairs (Schöndorf, 2021). Dr Schöndorf's article was cited almost entirely as the last Anex in the Israel National Cyber Directorate policy paper (*Israel International Cyber Strategy International Engagement for Global Resilience*, 2021).

Due to the rarity of such a public address on cyber sovereignty by an Israeli official, we provide the quotation in Table 2 ("Dr Roy Schöndorf's Reference to Israel's Cyber Sovereignty " according to the relevant section.

Section	Content
Sovereignty	"It is Israel’s view that in international law there is a firmly entrenched legal rule with regard to respecting the territorial sovereignty of other States. However, the application of this rule in the cyber domain raises questions and challenges. In practice, cyber activity in the exercise of State functions often implicates infrastructure physically located in other States, without such activity being deemed by any party a violation of territorial sovereignty. In addition, States' legitimate interests in the protection of data and networks of its citizens and companies hosted abroad, e.g. in cloud computing, should also be borne in mind".

Non-intervention	"In the cyber context, manipulation of election results or interfering with a state's ability to hold an election could also likely be considered a violation of this rule".
State responsibility	Attribution – " A State's decision whether to provide details and to whom, remains its exclusive discretion. " Countermeasures – "There is no absolute duty to notify the responsible State in advance of a countermeasure."
Use of force	"An action taken in accordance with a State's inherent right of self-defense, enshrined in Article 51 of the Charter, against an armed attack conducted through cyber means, may be carried out by either cyber or kinetic means."
The law of armed conflict	"Israel views that only an act expected to cause death or injury to persons or physical damage to objects beyond de-minimis, may constitute an "attack" within the meaning of this term under LOAC".
Cybercrime	"Particular attention needs to be afforded to the protection of government data stored by third-party cloud providers. In Israel's view, such data is not – and should not be made – subject to access requests by law enforcement authorities of other States. Furthermore, Israeli law enforcement agencies, aware of the "going dark" phenomenon, are considering different approaches to address it. To that end, Israel views international cooperation in this field as important."
Human rights	"Israel is a party to seven international human rights conventions. States' applicable obligations under these conventions remain relevant also in the cyber domain, in particular in striving to protect key rights such as freedom of speech and privacy."

Table 2 – Dr Roy Schöndorf's Reference to Israel's Cyber Sovereignty

Nevertheless, there is a lack of an analysis of Israel's official stands towards its cyber sovereignty and cyber boundaries. Therefore, the research intends to analyse the existence and the extent of Israel's official cyber sovereignty and boundaries and to minimise the research gap in this domain.

2. Methodology

We performed the following steps:

1. Map all of Israel's official cyber policies and strategies, published in English and Hebrew by the government of Israel or by the relevant official cyber agencies (Housen-Couriel, 2017; Index of Israeli Cyber Laws and Regulations, 2021; Israel - Cyber Policy Portal, 2022).
2. Collect all the publications to Table 3 – "Israel's Cyber Sovereignty and Boundaries in its Official Cyber Policy Publications".
3. Search for the terms "Sovereignty" and "Boundary" in the context of cyberspace in every publication that appears in Table 3 – "Israel's Cyber Sovereignty and Boundaries in its Official Cyber Policy Publications".

4. Perform a broader indication of cyber sovereignty or boundaries definitions if a document does not explicitly include such a term.
5. Collect all the data and analyse it accordingly in Table 3 – "Israel's Cyber Sovereignty and Boundaries in its Official Cyber Policy Publications".

3. Research Questions

The study analyses the following research questions: (RQ1) What is Israel's official definition of its sovereignty in cyberspace? (RQ2) What are the official boundaries of Israel's cyberspace? (RQ3) Do the definitions differ between the different official sources – the Israeli government and official cyber agencies? (RQ4) What may be the reasons for the current state of Israel's official stand toward its cyber sovereignty and boundaries?

4. Findings

The research analysed 17 official Israeli publications and government resolutions defining Israel's cyberspace policy (10), structure (1), and legal framework, published between 1995 and 2021 by the Government of Israel (8), the Israel National Cyber Directorate (8), and the Israel Defense Forces (1).

Table 3, "Israel's Cyber Sovereignty and Boundaries in its Official Cyber Policy Publications", represents the overall findings, which are:

1. Of 17 official Israeli cyber policy publications and regulations, 14 were analysed based on the English version of the documents and four on the Hebrew version.
2. None of the analysed documents include "Sovereignty" or "Boundaries" relating to Israeli cyberspace.
3. Only four describe the Israeli perception of sovereignty in local cyberspace –the Government of Israel (1), the Israel National Cyber Directorate (2), and the Israel Defense Forces (1).
4. The military strategy document (the Israel Defense Forces Strategy) considers Israeli cyberspace as another dimension that needs to be protected, but with no boundary definition. In contrast, the civilian strategy and legal documents (the Government of Israel and the Israel National Cyber Directorate) refer only to civilian cyberspace and exclude "particular entities", meaning the "Defense Establishment"(*National Cyber Concept for Crisis Preparedness and Management*, 2018).
5. The definitions may seem vague whether the "Protection of air space, surrounding sea and cyberspace" (*The IDF Strategy*, 2016) includes "Elements outside national borders" (*מונחון סייבר לאנשי מקצוע*, 2022).
6. No official Israeli policy paper holds an in-depth and broad discussion on the issue of cyber sovereignty.

Subject	Name	Publisher	Date	"Sovereignty"	"Boundary"	General Reference	Source
Cyberspace Policy	Israel National Cybersecurity Strategy	Prime Minister's Office; National Cyber Directorate	September 2017	-	-	-	(*Israel National Cyber Security Strategy in Brief*, 2017)
	The IDF Strategy	Israel Defense Forces	July 2016	-	-	"Protection of air space, surrounding sea and cyberspace".	(*The IDF Strategy*, 2016)
	National Cyber Concept for Crisis Preparedness and Management	Israel National Cyber Directorate	6 November 2018	-	-	"Israel's civil cyberspace: the cyberspace of all governmental and private parties in the State of Israel, excluding particular entities (the Israel Defense Forces, the Israeli Police, Israel Security Agency, the Institute for Intelligence and Special Operations, and the Defense Establishment)".	(*National Cyber Concept for Crisis Preparedness and Management*, 2018)
	Focus Questions For Cyber Policy Makers	Israel National Cyber Directorate	17 September 2018	-	-	-	(*Focus Questions for Cyber Policy-Makers*, 2018)
	Best Practice Reducing cyber security risks in video surveillance cameras	Israel National Cyber Directorate	12 April 2018	-	-	-	(*Best Practice Reducing Cyber Security Risks in Video Surveillance Cameras*, 2018)
	Use of Cloud Services - Addendum to the Cyber Defense Methodology for an Organization	Israel National Cyber Directorate	29 October 2017	-	-	-	(*Addendum to the Organizational Cyber Security Methodology Use of Cloud Services*, 2017)
	The Corporate Defense Methodology – V1.0	Israel National Cyber Directorate	18 April 2017	-	-	-	(*The Corporate Defense Methodology*, 2017)
	Cyber Defense Doctrine Managing the Risk: Full Applied Guide to Organizational Cyber Defense	Israel National Cyber Directorate	June 2021	-	-	-	(*Cyber Defense Doctrine Managing the Risk: Full Applied Guide to Organizational Cyber Defense*, 2021)

	Cyber term for professionals	Israel National Cyber Directorate	24 April 2022	-	-	"Israeli Cyber Space - The totality of the components of the global cyberspace, in which the State of Israel has rights. including elements outside national borders".	*מונחון סייבר לאנשי מקצוע*, (2022)
Structure	CERT-IL Operating Guidelines	Israel National Cyber Directorate	4 March 2015	-	-	-	*עקרונות הפעולה של המרכז הלאומי לסיוע בהתמודדות עם אירועי סייבר*, (2015
Legal Framework	Computer Law, 1995	Government of Israel	25 October 1995	-	-	-	(חוק המחשבים, תשנ"ה-1995, (1995
	Government Resolution No. 3611	Government of Israel	7 August 2011	-	-	"Civilian Space" – cyberspace that includes all the governmental and private bodies in the State of Israel, excluding special bodies"	(Resolution No. 3611 of the Government - Advancing National Cyberspace Capabilities, 2011)
	Government Resolution No. 2443	Government of Israel	15 February 2015	-	-	-	(Government Resolution No. 2443 - Advancing National Regulation and Governmental Leadership in Cyber Security, 2015)
	Government Resolution No. 2444	Government of Israel	February 2015	-	-	-	(Government Resolution No. 2444: Advancing the National Preparedness for Cyber Security, 2015)
	Protection of privacy regulations (data security) 5777-2017	Government of Israel	8 May 2017	-	-	-	(Protection of Privacy Regulations (Data Security) 5777-2017, 2017)
	2018 Memorandum of the National Cyber Directorate – Draft Bill in Progress	Government of Israel	2018	-	-	-	*תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח-(2018,* 2018)
	2021 Proposed Law of the National Cyber Directorate	Government of Israel	4 March 2021	-	-	-	(הצעת חוק סמכויות לשם חיזוק הגנת הסייבר (הוראת שעה), התשפ"א-2021 ,2021)

5. Discussion and Conclusions

The findings point to the fact that only a few of Israel's official national cyber strategy publications and regulations address the issue of cyber sovereignty. There is no specific official policy paper, or even a chapter in a current one, that defines Israeli cyber sovereignty.

Since the research analysed 17 official documents papers issued by different publishers over a long period (1995-2021), both in English and Hebrew, the findings expose a consistent Israeli approach towards defining official cyber sovereignty. The reason for that ongoing approach may be either (1) a deliberate strategy not to formulate or expose already formulated Israel's definition and stand of its cyber sovereignty or (2) a lack of any official Israeli cyber sovereignty strategy.

Based on Dr Schöndorf's detailed analysis (Table 2 – "Dr Roy Schöndorf Reference to Israel's Cyber Sovereignty") of Israeli official policy and previous analysis of the researcher, we believe the explicit findings may blend both reasons.

Strategic Ambiguity

In a paper with the crystal clear title "Israel's Cautious Perspective on International Law in Cyberspace", Prof Michael Schmitt describes two attitudes towards "whether sovereignty is simply a principle of international law from which binding international law rules emerge, or a primary rule of international law, the violation of which by cyber means constitutes an "internationally wrongful act"", mentioning two positions and the fact that the United States and Israel remain on the fence "either by failing to express a view or by discussing the matter without taking a firm position thereon" (Schmitt, 2020). The same as Dr Schöndorf's claim that "the State of Israel has largely refrained thus far from making specific statements on whether and how particular rules apply" (Schöndorf, 2020).

Detailed analysis of Israeli official policy is rare and may reflect Israel's position towards cyber sovereignty, generally speaking, and not necessarily Israeli cyber sovereignty.

An interesting exception to such ambiguity may be in Dr Schöndorf's analysis, which asserts, "Particular attention needs to be afforded to the protection of government data stored by third-party cloud providers. In Israel's view, such data is not – and should not be made – subject to access requests by law enforcement authorities of other States" (Schöndorf, 2020). In addition to the definition of "Israeli Cyber Space" by the Israel National Cyber Directorate, it explicitly mentions "including elements outside national borders" (2022, מונחון סייבר לאנשי מקצוע). Both statements conclude that Israel considers its cyber sovereignty beyond territorial sovereignty to include exterritorial elements.

Support for this hypothesis on strategic cyber sovereignty ambiguity may be found in international strategic ambiguity relating to cyber norms and specifically to cyber sovereignty (Barker, 2020; Brake, 2015; Broeders & Cristiano, 2020; Chapter Author & Cavelty, 2022; Libicki, n.d.; Palladino & Amoretti, n.d.; Ruohonen, 2021).

Lack of Cyber Policy Maturity

Another explanation may be the lack of maturity in Israel's cyber policy. The author analysed Israel's official cyber policy publications to reveal a lack of reference to issues such as digital privacy (Pavel, 2023) and cyber insurance (Pavel, 2020). In 2020, the author analysed Israel's official cyber policy towards cyber insurance. The findings indicated no cyber insurance reference in 29 relevant official publications by the Ministry of Finance and only one reference among 16 publications of the Israel National Cyber Directorate (Pavel, 2020).

Perhaps the most crucial fact on Israel's immaturity of cyber policy is that even though Israel enacted a computer law in 1995, it lacks cyber law. The government of Israel proposed a cyber law in 2018 and amended the draft bill in 2021, but Israel still has no cyber law.

Therefore, the research can address the research questions and argue that (RQ1) Israel's official definition of cyber sovereignty is probably deliberately vague, refers to civilian cyberspace, and includes elements outside its national borders. Therefore, (RQ2) the extent of the Israeli cyberspace boundaries exceeds its physical boundaries. (RQ3) The research indicates no differences between the very few cyber sovereignty definitions formulated by the Government of Israel and the Israel National Cyber Directorate. Israel Defense Forces Strategy does not define cyber sovereignty but considers it another domain to protect. (RQ4) The reasons for such lack of Israeli official stand and policy towards cyber sovereignty may be either (1) motivated by a deliberate strategic ambiguity, to remain on the fence, (2) due to lack of cyber policy maturity, or (3) a combination of both – a planned strategy with an unplanned negligence.

6. Future research

Based on the current one, future studies may analyse the (1) legal aspects of Israel's cyber sovereignty, including the legal cyber boundaries, based on local analyses, reports and legal activities. Others may analyse the (2) differences in the definitions and scope of Israel's cyber sovereignty across the years, (3) whether such lack of official clear definition also applies to other cyber-related terms of Israeli cyberspace. To (4) compare Israel's cyber sovereignty and boundaries with other countries in the region and beyond to understand whether the phenomena observed in this research are unique to Israel or exist in other countries, to (5) understand what is in common with states that lack an official declared cyber sovereignty, and (6) what steps should the international community take to encourage more clear, transparent and well defined cyber policy sovereignty of states worldwide.

References

1. Adamsky, D. (Dima). (2017). The Israeli Odyssey toward its National Cyber Security Strategy. *Washington Quarterly*, *40*(2), 113–127. https://doi.org/10.1080/0163660X.2017.1328928/ASSET//CMS/ASSET/64A161C4-6C3C-4530-A93A-4B0A489A9940/0163660X.2017.1328928.FP.PNG
2. *Addendum to the Organizational Cyber Security Methodology Use of Cloud Services*. (2017).

https://www.gov.il/BlobFolder/policy/cloud_services/en/Use%20of%20Cloud%20Services%20En.pdf

3. Antebi, L., & Baram, G. (2020). *Cyber and Artificial Intelligence-Technological Trends and National Challenges*. *4*(1). https://www.rt.com/news/401731-ai-
4. Baezner, M. ;, & Robin, P. (2018). *ETH Library Cyber Sovereignty and Data Sovereignty*. https://doi.org/10.3929/ethz-b-000314613
5. Barker, T. (2020, January 16). *Europe Can't Win Its War for Technology Sovereignty*. Foreign Policy. https://foreignpolicy.com/2020/01/16/europe-technology-sovereignty-von-der-leyen/
6. *Best Practice Reducing cyber security risks in video surveillance cameras*. (2018). https://www.gov.il/BlobFolder/policy/iotcameras/en/Security%20Cameras_575480_Sharon3_EN_WEB%20-%20%D7%9E%D7%95%D7%A0%D7%92%D7%A9.pdf
7. Biji Ahuja, N. (2023, July 16). *How India, UAE, Israel are trying to build secure cyberspace*. The Week. https://www.theweek.in/theweek/specials/2023/07/08/building-a-secure-cyberspace-through-the-india-uae-israel-cyber-security-partnership.html
8. Brake, B. (2015). Strategic Risks of Ambiguity in Cyberspace. In *Contingency Planning Memorandum* (Issue 24). https://www.cfr.org/report/strategic-risks-ambiguity-cyberspace
9. Broeders, D., & Cristiano, F. (2020, March 18). *Cyber Norms and the United Nations: Between Strategic Ambiguity and Rules of the Road*. Italian Institute for International Political Studies. https://www.ispionline.it/en/publication/cyber-norms-and-united-nations-between-strategic-ambiguity-and-rules-road-25417
10. Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *Https://Doi.Org/10.1177/1367549417751151*, *21*(5), 594–613. https://doi.org/10.1177/1367549417751151
11. Can, M. (2020). Grey Zone Conflicts in Cyber Domain. *Encyclopedia of Criminal Activities and the Deep Web*, 271–286. https://doi.org/10.4018/978-1-5225-9715-5.CH018
12. Carlsson, L., & Sandström, A. (2008). Network governance of the commons. *International Journal of the Commons*, *2*(1), 33–54. https://www.jstor.org/stable/26522989
13. Chapter Author, B., & Cavelty, D. (2022). Conclusion: The Ambiguity of Cyber Security Politics in the Context of Multidimensional Uncertainty. In *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation* (pp. 239–266). Routledge. https://doi.org/10.3929/ethz-b-000534272
14. Cristiano, F. (2020). Israel: Cyber Warfare and Security as National Trademarks of International Legitimacy. In *Routledge Companion to Global Cyber-Security Strategy*, (pp. 1–20). https://deliverypdf.ssrn.com/delivery.php?ID=083008085091003108112008079098005023014014073092023027101000111086026075106094088125028029021119038017111107029120115024002027122075014092018090006114118080074005022040064023095024091122120030089113090118011015115126117022019024007024093120091009114064&EXT=pdf&INDEX=TRUE
15. *Cyber Defense Doctrine Managing the Risk: Full Applied Guide to Organizational Cyber Defense*. (2021). https://www.gov.il/BlobFolder/generalpage/cyber_security_methodology_2/he/ICDM%20V2.pdf

16. *Cyber Sovereignty*. (n.d.). Thales Group. Retrieved 11 November 2023, from https://www.thalesgroup.com/en/markets/defence-and-security/cyberdefence-solutions/cyber-sovereignty
17. *Definition of Data Governance*. (n.d.). Gartner. Retrieved 11 November 2023, from https://www.gartner.com/en/information-technology/glossary/data-governance
18. Didehvar, F., & Danaeefard, H. (2010). Virtual governance networking policies: A comparative analysis. *Public Organization Review*, *10*(1), 1–16. https://doi.org/10.1007/S11115-009-0079-6/METRICS
19. Digital Sovereignty for Europe. (2020). In *European Parliament*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf
20. Duarte, M. E. (2017). *Network Sovereignty: Building the Internet across Indian Country*. University of Washington Press. https://uwapress.uw.edu/book/9780295741826/network-sovereignty/
21. Eizenkot, G. (2018). *Cyberspace and the Israel Defense Forces*. *2*(3).
22. Erkut, B. (2020). From Digital Government to Digital Governance: Are We There Yet? *Sustainability 2020, Vol. 12, Page 860*, *12*(3), 860. https://doi.org/10.3390/SU12030860
23. *Focus Questions for Cyber Policy-Makers*. (2018). https://www.gov.il/BlobFolder/policy/boardquestions/en/FOCUS%20QUESTIONS%20FOR%20CYBER%20POLICY-MAKERS%20english%20final.pdf
24. Government Resolution No. 2443 - Advancing National Regulation and Governmental Leadership in Cyber Security, 1 (2015). https://ccdcoe.org/uploads/2019/06/Government-Resolution-No-2443-Advancing-National-Regulation-and-Governmental-Leadership-in-Cyber-Security.pdf
25. Housen-Couriel, D. (2017). *National Cyber Security Organisation: ISRAEL*. www.ccdcoe.orgpublications@ccdcoe.org
26. Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data and Society*, *8*(1). https://doi.org/10.1177/2053951720982012/ASSET/IMAGES/10.1177_2053951720982012-IMG2.PNG
27. *Index of Israeli Cyber Laws and Regulations*. (2021). https://csrcl.huji.ac.il/sites/default/files/csrcl/files/state_of_israel_cyber_laws_regulations_and_policies_for_federmann_cyber_center.pdf
28. *Internet Governance Glossary*. (2005). UNESCO. https://en.unesco.org/glossaries/igg?name=1.5%20Internet%20governance
29. *Israel - Cyber Policy Portal*. (2022, November). United Nations Institute for Disarmament Research. https://cyberpolicyportal.org/states/israel
30. *Israel International Cyber Strategy International Engagement for Global Resilience*. (2021). https://www.gov.il/BlobFolder/news/international_strategy/en/Israel%20International%20Cyber%20Strategy.pdf
31. *Israel National Cyber Security Strategy in Brief*. (2017).

32. Jayawardane, S., Larik, J. E., & Jackson, E. (2015). *Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance*. The Hague Institute for Global Justice. https://hdl.handle.net/1887/48177
33. Kelton, M., Sullivan, M., Rogers, Z., Bienvenue, E., & Troath, S. (2022). Virtual sovereignty? Private internet capital, digital platforms and infrastructural power in the United States. *International Affairs*, *98*(6), 1977–1999. https://doi.org/10.1093/IA/IIAC226
34. Lewis, J. A. (2020). *Sovereignty and the Evolution of Internet Ideology*.
35. Li, H., & Yang, X. (2021). Interpretation of Network Sovereignty. *Co-Governed Sovereignty Network*, 29–60. https://doi.org/10.1007/978-981-16-2670-8_2
36. Libicki, M. C. (n.d.). *Military and Strategic Affairs The Strategic Uses of Ambiguity in Cyberspace Examples of Strategic Ambiguity in Physical Space*.
37. Luna-Reyes, L. F. (2017). Opportunities and challenges for digital governance in a world of digital participation. *Information Polity*, *22*(2–3), 197–205. https://doi.org/10.3233/IP-170408
38. Mihr, A. (2014). Good Cyber Governance: The Human Rights and Multi-Stakeholder Approach. *Georgetown Journal of International Affairs*, 24–34. https://www.jstor.org/stable/43773646
39. Mueller, M. (1996). *Sovereignty and Cyberspace: Institutions and Internet governance*.
40. *National Cyber Concept for Crisis Preparedness and Management*. (2018).
41. *Navigating Digital Sovereignty and its Impact on the Internet*. (2022). https://www.internetsociety.org/wp-content/uploads/2022/11/Digital-Sovereignty.pdf
42. Obar, J. A., & Clement, A. (2013). Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.2311792
43. Palaniappan, M. (2022). *Cyber Sovereignty: In Search of Definitions, Exploring Implications*. https://www.orfonline.org/wp-content/uploads/2022/12/ORF_IssueBrief_602_CyberSovereignty.pdf
44. Palladino, N., & Amoretti, F. (n.d.). The Ambiguity of Digital Sovereignty between Cybersecurity and Digital Rights. *International Political Science Association*. Retrieved 16 November 2023, from https://www.ipsa.org/wc/paper/ambiguity-digital-sovereignty-between-cybersecurity-and-digital-rights
45. Pavel, T. (2020). Cyber Insurance Market in Israel - What is the Official Policy? *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020*. https://doi.org/10.1109/CYBERSA49311.2020.9139722
46. Protection of privacy regulations (data security) 5777-2017, 1 (2017). https://www.gov.il/BlobFolder/legalinfo/data_security_regulation/en/PROTECTION%20OF%20PRIVACY%20REGULATIONS.pdf
47. Resolution No. 3611 of the Government - Advancing National Cyberspace Capabilities , 1 (2011). https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Israel_2011_Advancing%20National%20Cyberspace%20Capabilities.pdf
48. Ronen, Y., Siboni, G., & Sivan-Sevilla, I. (2018). *Operations in Cyberspace from the Perspective of International Law*. *2*(3).

49. Ruohonen, J. (2021). The Treachery of Images in the Digital Sovereignty Debate. *Minds and Machines*, *31*(3), 439–456. https://doi.org/10.1007/S11023-021-09566-7/METRICS
50. Sassen, S. (1998). On the Internet and Sovereignty on JSTOR. *Indiana Journal of Global Legal Studies*, *5*(2), 545–559. https://www.jstor.org/stable/25691119
51. Schmitt, M. (2020, December 17). *Israel's Cautious Perspective on International Law in Cyberspace: Part I (Methodology and General International Law)*. EJIL: Talk! https://www.ejiltalk.org/israels-cautious-perspective-on-international-law-in-cyberspace-part-i-methodology-and-general-international-law/
52. Schöndorf, R. (2020, December 9). *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*. EJIL: Talk! https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/
53. Schöndorf, R. (2021, October 25). *Israel's approach on the Application of International Law to Cyberspace*. Mission of Israel to the UN in Geneva. https://embassies.gov.il/UnGeneva/priorities-statements/ScienceTechnologyDevelopment/Pages/Israel-approach-on-the-Application-of-International-Law-to-Cyberspace.aspx
54. Sharma, S. (2023, October 11). *Israel-Hamas conflict extends to cyberspace*. CSO Online. https://www.csoonline.com/article/655223/israel-palestine-conflict-extends-to-cyberspace.html
55. Siboni, G., & Assaf, O. (2016). *Guidelines for a National Cyber Strategy*. https://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/SystemFiles/INSS%20Memorandum%20153%20-%20Guidelines%20for%20a%20National%20Cyber%20Strategy.pdf
56. Siboni, G., & Klein, H. (2018). *Guidelines for the Management of Cyber Risks*. *2*(2), 23. https://krebsonsecurity.com/2017/05/credit-card-breach-at-kmart-stores-again.
57. Siboni, G., & Sivan-Sevilla, I. (2017). *Israeli Cyberspace Regulation: A Conceptual Framework, Inherent Challenges, and Normative Recommendations*. *1*(1).
58. Simchoni, A. (2017). *Campaign in Cyber or Cyber in the Campaign*. *1*(3). http://e.vnexpress.net/news/news/cyber-
59. Snipp, C. M. (2016). What does data sovereignty imply: what does it look like? In *Indigenous Data Sovereignty: Toward an Adena* (pp. 39–55). https://library.oapen.org/bitstream/handle/20.500.12657/31875/624262.pdf?sequence#page=63
60. Sørensen, E. (2002). Democratic Theory and Network Governance. *Administrative Theory & Praxis*, *24*(4), 693–720. https://doi.org/10.1080/10841806.2002.11029383
61. Tabansky, L., & Ben Israel, I. (2015). *The National Innovation Ecosystem of Israel*. 15–30. https://doi.org/10.1007/978-3-319-18986-4_3
62. Taylor, J. F. (2023). The role of relational and transactional factors in the adoption of virtual governance strategies. *Journal of Business and Industrial Marketing*, *38*(4), 788–801. https://doi.org/10.1108/JBIM-08-2021-0393/FULL/XML
63. *The Corporate Defense Methodology*. (2017). https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/en/Cyber%20Defense%20Methodology%20for%20an%20Oragnization.pdf

64. Government Resolution No. 2444: Advancing the National Preparedness for Cyber Security, 1 (2015). https://ccdcoe.org/uploads/2019/06/Government-Resolution-No-2444-Advancing-the-National-Preparedness-for-Cyber-Security.pdf
65. *The IDF Strategy*. (2016).
66. Topor, L. (2021, October). *Israel—a Cyber Nation? A Critical Review of Israeli Cyberspace*. The Jerusalem Strategic Tribune. https://jstribune.com/topor-israel-cyber-defense/
67. *What is data governance?* (n.d.). IBM. Retrieved 11 November 2023, from https://www.ibm.com/topics/data-governance
68. Wu, T. S. (1996). Cyberspace Sovereignty--The Internet and the International System. *Harvard Journal of Law & Technology*, *10*. https://heinonline.org/HOL/Page?handle=hein.journals/hjlt10&id=657&div=&collection=
69. Zhuk, A. (2023). Virtual Sovereignty: Examining the Legal Status of Micronations in Cyberspace Through the Case of the Republic of Errant Menda Lerenda. *Digital Society 2023 2:3*, *2*(3), 1–13. https://doi.org/10.1007/S44206-023-00067-X
70. הצעת חוק סמכויות לשם חיזוק הגנת הסייבר (הוראת שעה), התשפ"א-2021, 1 (2021). https://www.law.co.il/media/computer-law/cyber_defense_bill_draft_version2_2021.pdf
71. חוק המחשבים, תשנ"ה-1995, 1 (1995). https://www.nevo.co.il/law_html/law00/72393.htm
72. *מונחון סייבר לאנשי מקצוע*. (2022). https://www.gov.il/he/Departments/General/terms
73. *עקרונות הפעולה של המרכז הלאומי לסיוע בהתמודדות עם איומי סייבר*. (2015). https://www.gov.il/BlobFolder/news/certpri/he/principles.pdf
74. *תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח-2018*. (2018). https://www.gov.il/BlobFolder/news/cyberlawpublic/he/%D7%AA%D7%96%D7%9B%D7%99%D7%A8%20%D7%97%D7%95%D7%A7%20%D7%94%D7%92%D7%A0%D7%AA%20%D7%94%D7%A1%D7%99%D7%99%D7%91%D7%A8%20%D7%95%D7%9E%D7%A2%D7%A8%D7%9A%20%D7%94%D7%A1%D7%99%D7%99%D7%91%D7%A8%20%D7%94%D7%9C%D7%90%D7%95%D7%9E%D7%99%20%D7%94%D7%AA%D7%A9%D7%A2%D7%97-2018%20%D7%9C%D7%94%D7%A4%D7%A6%D7%94.pdf