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.

<table>
<thead>
<tr>
<th>Authority</th>
<th>Digital World</th>
<th>Sovereignty</th>
<th>Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>(Duarte, 2017; Li &amp; Yang, 2021)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual</td>
<td>(Kelton et al., 2022; Zhuk, 2023)</td>
<td></td>
<td>(Didehvar &amp; Danaeefard, 2010; Taylor, 2023)</td>
</tr>
<tr>
<td>Cyber</td>
<td>(Palaniappan, 2022; Wu, 1996)</td>
<td></td>
<td>(Jayawardane et al., 2015; Mihr, 2014)</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Section</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sovereignty</td>
<td>&quot;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&quot;.</td>
</tr>
</tbody>
</table>
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.
<table>
<thead>
<tr>
<th>Subject</th>
<th>Name</th>
<th>Publisher</th>
<th>Date</th>
<th>&quot;Sovereignty&quot;</th>
<th>&quot;Boundary&quot;</th>
<th>General Reference</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Israel National Cybersecurity Strategy</td>
<td>Prime Minister's Office; National Cyber Directorate</td>
<td>September 2017</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>(Israel National Cyber Security Strategy in Brief, 2017)</td>
<td></td>
</tr>
<tr>
<td>The IDF Strategy</td>
<td>Israel Defense Forces</td>
<td>July 2016</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>&quot;Protection of air space, surrounding sea and cyberspace&quot;</td>
<td>(The IDF Strategy, 2016)</td>
</tr>
<tr>
<td>National Cyber Concept for Crisis Preparedness and Management</td>
<td>Israel National Cyber Directorate</td>
<td>6 November 2018</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>&quot;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)&quot;</td>
<td>(National Cyber Concept for Crisis Preparedness and Management, 2018)</td>
</tr>
<tr>
<td>Focus Questions For Cyber Policy Makers</td>
<td>Israel National Cyber Directorate</td>
<td>17 September 2018</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>(Focus Questions for Cyber Policy-Makers, 2018)</td>
<td></td>
</tr>
<tr>
<td>Best Practice Reducing cyber security risks in video surveillance cameras</td>
<td>Israel National Cyber Directorate</td>
<td>12 April 2018</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>(Best Practice Reducing Cyber Security Risks in Video Surveillance Cameras, 2018)</td>
<td></td>
</tr>
<tr>
<td>Use of Cloud Services - Addendum to the Cyber Defense Methodology for an Organization</td>
<td>Israel National Cyber Directorate</td>
<td>29 October 2017</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>(Addendum to the Organizational Cyber Security Methodology Use of Cloud Services, 2017)</td>
<td></td>
</tr>
<tr>
<td>The Corporate Defense Methodology – V1.0</td>
<td>Israel National Cyber Directorate</td>
<td>18 April 2017</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>(The Corporate Defense Methodology, 2017)</td>
<td></td>
</tr>
<tr>
<td>Year</td>
<td>Issue</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2022</td>
<td>“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”.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>CERT-IL Operating Guidelines</td>
<td>Israeli National Cyber Directorate 4 March 2015, - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1995</td>
<td>Computer Law, 1995</td>
<td>Government of Israel 25 October 1995, - - - “Civilian Space” - cyberspace that includes all the governmental and private bodies in the State of Israel, excluding special bodies”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>Government Resolution No. 3611</td>
<td>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”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>Government Resolution No. 2443</td>
<td>Government of Israel 15 February 2015, - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>Government Resolution No. 2444</td>
<td>Government of Israel February 2015, - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td>Protection of privacy regulations (data security) 5777-2017</td>
<td>Government of Israel 8 May 2017, - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2018</td>
<td>2018 Memorandum of the National Cyber Directorate – Draft Bill in Progress</td>
<td>Government of Israel 2018, - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021</td>
<td>Proposed Law of the National Cyber Directorate</td>
<td>Government of Israel 4 March 2021, - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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" (מונחון סייבר לאנשי מקצוע, 2022). 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 & Caveltiy, 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


