Insight

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

A Conceptual Failure: Following the State Comptroller's Report on Countering Foreign Interference in Elections

David Siman-Tov and Ofer Fridman[1] | No. 2167 | July 13, 2026

The State Comptroller's report highlights significant deficiencies in Israel's preparedness to counter foreign interference in the digital sphere. These include the lack of a comprehensive national policy, coordination gaps, and only partial preparedness ahead of the elections. This article argues that these findings reflect a broader problem: the absence of an agreed-upon national concept regarding both the threat itself and the methods to address it. Accordingly, it proposes developing an integrated strategic approach that encompasses intelligence, regulation, strategic communications, civil society, digital literacy, and resilience against new challenges posed by artificial intelligence systems.

The State Comptroller's report on Israel's response to foreign influence in the digital sphere, published on July 7, 2026, prompts a broad discussion on one of the emerging threats to national security. It is certainly possible to read it as another audit report detailing failures in coordination among government ministries, the absence of policy, and deficiencies in preparedness. Yet, such a reading would miss its primary significance: **for the first time, a state institution has systematically reviewed the characteristics of the foreign digital interference problem, as well as how it is perceived (or not) by the entities responsible for national security.** The Comptroller's report points to an urgent need to formulate a national conceptual framework for countering Foreign Information Manipulation and Interference (FIMI), even though the threat has been recognized for approximately a decade by security agencies, the political stakeholders, and academia.

This conceptual gap is evident in the report's very title, which defines the threat as "foreign influence in the digital sphere," despite the fact that foreign influence is a central and often legitimate component of international relations. International actors always strive to influence the agenda and decision-making processes of other actors to achieve their own goals and strategic objectives. As such, foreign influence does not inherently constitute a threat. For example, grants provided by international organizations to support disadvantaged populations in Israel within the digital sphere represent a form of foreign influence, but this is not what the State Comptroller has in mind. Rather, the report points to a very specific type of foreign influence called "interference," occurring when the influence exerted by a

---

[1] Dr. Ofer Fridman is a Senior Lecturer at King's College London.

specific international actor (e.g., Iran) is perceived by the targeted actor (Israel) as contrary to its values, norms, or laws. In other words, although the report speaks broadly of foreign influence, it actually refers to a specific type of influence that interferes with organic and legitimate public discourse in Israel and poses a threat to its national security. Consequently, **this article uses the term "foreign interference" rather than "influence,"** in accordance **with the terminology and conceptual frameworks commonly used in the field.**

The report does not reveal a new threat, nor does it point to an isolated failure. Rather, **it documents an ongoing, systemic gap between the evolving nature of the threats facing liberal democracies and the slow, inconsistent manner in which Israel has organized its response to them.** In recent years, foreign interference has become one of the primary strategic tools employed by rival states. It is becoming increasingly clear that the challenges Israel faces do not stem from a lack of professional expertise or technological capabilities, but rather from the absence of an agreed-upon conceptual framing of the threat and how to address it, and from the lack of resolve on the part of all stakeholders to mount an effective response.

The challenge of countering foreign interference is not merely institutional or structural, nor is it simply a question of the division of responsibility. The fundamental complexity of tackling foreign interference in the digital sphere challenges the Israeli establishment because it is, by definition, a multi-dimensional problem—one that demands being broken down into several content areas under a single, overarching conceptual framework.

Foreign interference in the digital sphere differs from traditional security threats. It does not take place in a military theater but rather within the civil domain; it is not aimed at directly damaging infrastructure or military forces, but at influencing public perceptions, attitudes, and behavior; and it relies on a combination of foreign actors, global platforms, and at times, domestic actors as well. For this reason, it is difficult to assign this responsibility to a single professional agency. Instead, it requires integrating intelligence, regulation, strategic communications, education, technology, and civil society within a single, unified conceptual framework.

In the Israeli context, FIMI threats originating from foreign states (Iran), major powers (Russia), and even ostensibly civil organizations (the Muslim Brotherhood, the "ISNAD" network) have been identified in recent years. These cases are clearly only the tip of the iceberg, and it is reasonable to assume that additional threats originate from other countries and operate in other languages. Notably, most of the threats identified so far have been in Hebrew, likely due to the extensive activities of civil society organizations and heightened media awareness.

The core challenge stems from the division of responsibility for addressing the strategic problem of foreign interference across multiple agencies, each of which defines the problem and develops a response to it from its own institutional perspective, without comprehensive coordination. Intelligence agencies—led by the Israeli Security Agency (Shin Bet)—view the phenomenon of foreign interference as an intelligence collection and analysis problem: identifying hostile activities, attributing them to foreign actors (state or non-state), providing assessments to decision-makers regarding the adversary's intentions and capabilities and disrupting them. While this holds an immense value, the classified nature of intelligence modus operandi prevents high-profile operations in the digital sphere and exposure of interference attempts at the speed and scale required to boost public awareness and

national resilience. **Another challenge for intelligence agencies is that foreign interference frequently intertwines with domestic political campaigns. This creates a conceptual and operational barrier for these organizations, which are naturally reluctant to monitor domestic political system.**

Government ministries responsible for strategic communications (such as the Prime Minister's Office, the National Public Diplomacy Directorate, and the Ministry of Foreign Affairs) tend to view foreign interference as a messaging problem, namely the need to construct and disseminate accurate narratives to compete with the adversary's disinformation. This approach also has value, particularly in a field that chronically suffers from a lack of resources relative to the scale of the challenge. However, **strategic communications, even when executed exceptionally well, address the symptom rather than the root cause**. It assumes that a better message can compete within a hostile information environment—an assumption that holds true under conditions of good-faith competition, but fails under conditions of deliberate epistemic information pollution.

The justice system, public policy, and civil society view foreign interference as a content management and transparency problem—identifying false content, labeling it, removing it, and requiring platforms to be more transparent about how their algorithms amplify it. While these are necessary measures, they are insufficient on their own. This is particularly true given that Israeli law and public policy have yet to systematically address how information is disseminated in the digital sphere, especially regarding mechanisms related to inauthentic information dissemination and content-promoting algorithms. Content labeling assumes that users can act based on labels, and it fails to address the underlying strategies of foreign interference. More often than not, the objective of a foreign interference campaign (such as widening political polarization in Israeli society) is achieved only after the operation itself (such as masquerading as activists within a specific political camp) is exposed and labeled.

Consequently, **each one of the government bodies mentioned in the report deals, or has dealt, with only part of the problem**. Security agencies focus on foreign actors from their own perspective; the Ministry of Justice handles legislation; the National Cyber Directorate addresses technological aspects; the Ministry of Education offers curricula on digital literacy and critical thinking; and civil society voluntarily develops independent research and monitoring capabilities, raises awareness of the phenomenon, and promotes local educational initiatives. Yet no one sees the full picture.

Furthermore, the discussion should not focus solely on which government body will be responsible for this domain. The State Comptroller's recommendation—that the National Security Council formulate a framework to serve as the basis for a government decision to establish a dedicated coordinating body under the Prime Minister's Office, with its own budget and authority—is a correct and necessary step. However, **an organizational structure is no substitute for a conceptual framework**: a new body will succeed only if it operates based on an agreed-upon definition of the threat, the objectives of the response, the division of responsibility among agencies, and the relationship between the state and civil society. Without this, even a newly established mechanism is likely to replicate the very same failures. Israel must recognize that foreign interference in the digital sphere is a major strategic challenge that demands a comprehensive and systemic approach.

Over several decades, Israel has developed effective mechanisms for addressing well-defined, emerging threats: terrorism, high-trajectory weapons (rockets and missiles), cyberattacks, and tunnels. For each of these, there has been a clear institutional division of responsibility, established patterns of operation, and agreed-upon metrics for success. Foreign interference is fundamentally different. It takes place within the civil domain, does not generally violate the law, operates through private global platforms, and at times even leverages local actors to deepen existing societal rifts. It does not naturally fall under the purview of a single body—be it intelligence, cyber, law, or communications. **Rather, it is a threat that lies at the intersection of national security, technology, democracy, and societal resilience, making it inherently difficult to address effectively.**

The required first step, therefore, is the **formulation of a national conceptual framework for countering foreign interference. Such a framework must recognize FIMI as a permanent feature of Israel's threat landscape**, rather than an isolated occurrence that arises only on the eve of elections or during a security crisis. It must integrate intelligence activities, regulation, cooperation with digital platforms, and a tangible reinforcement of civil society through resources, technology, and formal recognition, alongside developing research capabilities, investing in digital literacy, and building social resilience. It must also ensure that efforts to counter foreign interference are conducted in a manner that safeguards the core principles of democratic governance, foremost among them freedom of expression, transparency, and public oversight.

The gap highlighted by the State Comptroller takes on a particular urgency ahead of the Knesset elections in October 2026. An election period is exceptionally fertile ground for foreign interference, raising genuine concerns regarding the potential manipulation of electoral outcomes and the undermining of public trust in them. The report indicates that preparedness began far too late. While recent adjustments can be observed in the preparations of the Central Elections Committee, these efforts have been deferred until the last moment and continue to address symptoms rather than build enduring resilience.

In recent years, a new technological dimension has been added to the threat. When public engagement with this issue first began in Israel, the main focus of attention was on social media networks. Now, a new intermediary layer has emerged: artificial intelligence systems and Large Language Models (LLMs) that respond to user queries, fundamentally reshaping the nature of the threat—shifting it **from a threat characterized by disinformation campaigns to one defined by the pollution of the information sources themselves and data poisoning**. This does not mean that social networks have ceased to be a primary arena for interference; rather, the challenge has become more complex and diversified. Alongside the struggle over public discourse on social networks, a new battle is unfolding over the data from which AI systems learn and the manner in which they present it to users. The gaps pointed out by the report are unlikely to narrow anytime soon, and may even widen if the counter-interference framework is not updated.

Conclusion and Recommendations

Ultimately, the primary contribution of the State Comptroller's report lies not merely in identifying deficiencies or recommending the establishment of a new body. Its significance rests in the fact that it exposes a deeper problem—a conceptual failure. As long as Israel fails to recognize the cognitive domain as a strategic arena of conflict and integrate it into its national security doctrine, organizational reforms

and improved inter-agency coordination will not suffice to address the threat. **It is therefore vital not only to point out the threat itself, but also to get to the root of the failure and the reasons behind Israel's unsubstantial response.**

We wish to add three points of emphasis to the Comptroller's recommendations:

1. Protecting the digital information environment from manipulation and inauthentic information dissemination must be made a permanent pillar of Israel's national security strategy. This should include developing metrics to assess the threat and measure resilience, investing in long-term societal resilience—including the early "inoculation" of the public against manipulation—and strengthening international cooperation.
2. Effective governance of the digital information environment cannot be achieved without civil society. Civil society organizations and academia should be institutionalized as formal partners—not merely sources of reporting—through sustained funding, access to technology, and official recognition, as they currently shoulder much of the burden of monitoring and research.
3. Israel's strategic framework for countering foreign interference must remain sufficiently flexible to identify and adapt to emerging threats in the rapidly evolving digital information environment.

Editors of the series: Anat Kurz, Rinat Harash, Eldad Shavit and Keri Rosenbluh