

## Roundtable 3: Public Policy and Civil Society in Addressing Disinformation in Israel

**Date:** 29 May 2025 | Location: INSS, Tel Aviv

**Session Moderator:** Adv. Amit Ashkenazi, former Legal Advisor to Israel's National Cyber Directorate.

**Focus:** Interface between policy, regulation, and civil society roles in countering disinformation

**Rapporteur:** Yarden Amir (ISOC-IL)

### **Participants and Discussion Contributors:**

**Dr. Asaf Wiener** - VP Research & Public Policy, ISOC-IL. **Guy Barhan** - Strategic Consultant. **Ofir Dayan** - Research Associate in the Israel-China Policy Center, INSS. **Ofir Barel** - Yuval Ne'eman Workshop – Tel Aviv University. **Yulia Lishchka** - Delegation of the European Union to Israel. **Dr. Nir Greenberg** - Department of Software and Information Systems Engineering, Faculty of Engineering Sciences, Ben Gurion University. **Dr. Ido Baum** - Director, Brandeis Institute. **Mr. Yosi Aviram** - Strategy Division, Israel National Cyber Directorate.

---

### **Key Challenges and Issues**

- Significant **gaps in current regulatory frameworks** highlight the complex interplay between freedom of expression, responsibilities of global digital platforms, civil accountability, and the increasing use of social media for information warfare and foreign interference.
- Ongoing **tensions between freedom of expression and public (Israeli) Interests of online safety and national security**. Emphasis was placed on the unique regulatory void that characterizes global digital platforms, posing substantial challenges in managing content dissemination and accountability mechanisms.
- Participants shared a consensus that **Israel, like many democracies, faces a systemic threat from disinformation**, amplified by unregulated digital platforms operating outside national jurisdiction.
- Questions were raised on how **Israel can regulate, or otherwise affect global platforms' practices** within its legal and democratic framework.

- Concerns were raised about the ability to build upon the concept of “classic” public interest-focused public agencies that are independent and professional, in times of rising populist emotions and increasing political influence.

## Messages from the Roundtable:

- **Need of a multi-layer, multi-stakeholder response** due to the hybrid nature of disinformation, intersecting online speech, national security and public safety, media policy, and democratic governance, and the challenges it poses to more traditional forms of government activity, as well as the risks from such government activity. Any solution needs to be mindful of the current challenges to **democratic governance** and the potential risks for misuse of government powers
  - On the **conceptual level**, the global reach of technology companies and the need for cross-border cooperation can serve as a mitigating factor to a single jurisdiction’s potential misuse of powers.
  - This leads to a **policy design** requirement: that any intervention include checks and balances that take into account existing tensions and utilize the unique features to promote a safer online environment.
  - Israel requires sustained, multi-sector collaboration among government bodies, academic institutions, and civil society organizations to develop innovative and context-sensitive solutions for countering disinformation.
  - Civil society organizations are essential stakeholders in the fight against disinformation. The state should actively facilitate the work of civil society groups by reducing bureaucratic barriers and strengthening their operational capacities.
- Call for **cross-sectoral policy planning**, aligning security, regulation, and civic empowerment under one framework.
- **Suggested a 3-layer framework for filling the legislative-regulatory void in Israel:**
  - **Security and Law Enforcement Layer:** focused on removing illegal content and deterring malicious actors.

- **Liability and Regulatory Layer:** promotes behavior-based governance tools (rather than content-based censorship) for platform accountability.
  - **Civic-Ethical Layer:** emphasizes digital literacy, civic resilience, and democratic norms.
- The need to tackle FIMI as well as DIMI within the information ecosystem, while general agreement in the roundtable that some of the measures against FIMI will also reduce DIMI.
- Israel needs to develop a uniform approach for engagement with the international platforms, perhaps based on the idea of a digital ambassador.
- While the FIMI and DIMI challenges warrant a coordinated approach based on a national policy (such as Israel's national cybersecurity policy, for instance), there are risks associated with more active government involvement in this area. In this sense, a soft coordination mechanism in which civil society takes a leading role may be better.
- The government can invest in addressing some obstacles to improve reliability. One is through financing basic research and the universities' activity in this space. In addition, it can promote a university-based "National Internet Observatory", which can collect information based on citizen membership, thus overcoming some of the platform transparency issues.
- The state can also provide an innovation-friendly legal environment, such as safe harbors for web scraping to enable FIMI research, and "regulatory sandboxes" to promote technology development and reduce legal risk. This was raised as a challenge to some of the technologies in this area, seen as "dual use", thus drawing attention from the Defense establishment and making investments more risky.
- One participant (RemedyColab) described a project developed with academia to map technological offerings to deal with FIMI, cataloging such technologies according to their potential role in mitigating attacks based on the DISARM framework.
- Participants stressed the need for national situational awareness, including public-private information sharing, and having a central resource collecting and disseminating information about FIMI operations.

- In the same vein, participants discussed the importance of sharing technical indicators to mitigate attacks and ensure cross-platform safety.
- One participant highlighted the different types of disinformation harms, which begin with potential individual harms, move to collective harms such as targeting minorities, and can reach the national level.
- One participant suggested a more comprehensive engagement with platforms to promote shared responsibility for the safety of the online arena.
- In the area of AI, participants shared concerns about attacks that contaminate the information arena by publishing fake information on multiple websites in order to affect LLM training and outputs.
- Similar to the way search engine optimization promotes content on the internet, it was suggested that similar techniques, for legitimate and illegitimate reasons, are being developed today.
- Current standardization efforts relating to AI-generated content, including the platforms' obligation to display such markings, were also mentioned.

## Resources for research and policy development for Disinformation Resilience in Israel

- The EU's [FIMI toolbox](#) and the [Disinformation Kill Chain](#) as comparative models to structure potential Israeli interventions.
- The World Economic Forum, [Global Risks Report 2025](#).

- [היערכות לאומית מול השפעה והתערבות זרה באמצעות רשתות חברתיות: ממצאים גלובליים ותמונת מצב ישראלית \(2024\)](#)  
אסף וינר
- [מתווה לאסדרת רשתות חברתיות בישראל \(2023\)](#)  
תהילה שוורץ אלטשולר, אסף וינר, אייל זילברמן
- [קווים מנחים להתמודדות ישראל עם השפעה זרה במרחב הסייבר והרשתות החברתיות \(2024\)](#)  
עמית אשכנזי