

INACH Global Pulse Brief Series

Introduction

This report provides a brief overview of the Israeli online climate and the presence of cyber hate and disinformation within the context of political instability, the Hamas-led attack on October 7, 2023, and the ongoing Israeli military operations in Gaza and along the northern border. The online world has become a key battleground where narratives are contested, with social media and messaging platforms serving as accelerators for both discourse and coordinated manipulation campaigns. The combination of domestic political fragmentation, global influence operations, and algorithm-driven content dissemination continues to contribute to increased polarization, a rise in hate speech, and a decline in public trust across sectors.

Historical Context

Between 2019 and 2022, Israel held five general elections within a period of 36 months, reflecting a deep crisis of political legitimacy. This prolonged instability weakened government structures and increased reliance on digital campaigning. Political actors on all sides increasingly relied on algorithms, bots, and fake social media profiles to shape voter perceptions. These tools amplified echo chambers and fueled the spread of misinformation, including manipulated videos and slanderous allegations targeting political opponents. The information environment was further degraded by coordinated inauthentic behavior—both domestic and foreign—seeking to deepen existing tensions between secular and religious populations, Jewish and Arab citizens, and left- and right-leaning voters.

A further source of tension was the government's plan to implement a major judicial reform aimed at limiting the role of the Supreme Court and shifting authority in favor of the executive branch. The proposed reforms triggered widespread backlash within the legal and security sectors. Critics warned that the changes could destabilize the system of checks and balances in Israel's democratic framework—especially concerning given the absence of a

formal constitution—and might undermine judicial independence, weakening the country's already fragile democratic order. These developments fueled online discourse, led to large-scale protests, and fostered digital mobilization both in support of and in opposition to the reforms.¹

Post-October 7 Dynamics

The Hamas attack on October 7, 2023—which resulted in the deaths of over 1,200 people and the abduction of civilians—marked a turning point in Israel's security discourse. In the aftermath, digital platforms became arenas for public mourning, outrage, and political debate. Government efforts to manage the fallout through narrative control include public information campaigns and the strategic use of military censorship to limit the spread of sensitive or controversial material. Prime Minister Netanyahu's public accusations of operational failures by military intelligence agencies have drawn sharp criticism across the political spectrum and sparked weekly protests in Tel Aviv, Jerusalem, and Haifa.

These dynamics have fueled an escalation in online hate speech, with targeted harassment campaigns against activists, journalists, and opposition leaders. Telegram channels and anonymous forums serve as hubs for conspiracy theories alleging internal betrayal and foreign interference. Social media campaigns promoting political messages and protest content remain widespread across major platforms. Simultaneously, doxxing campaigns—often driven by anonymous users and automated accounts—target individuals with opposing views, flooding the digital space with polarizing and hostile content. The result is a highly fragmented public discourse, increasingly shaped by emotionally charged and often misleading information.²

Foreign Influence: Disinformation Campaigns

Iran and other regional actors have significantly escalated their disinformation efforts, using a network of state-sponsored media outlets, proxy actors, and cyber units to influence Israeli public opinion. Iran-linked operations produce multilingual content—Hebrew, Arabic, and English—targeting various demographic groups within Israel. Their tactics include the creation of falsified news websites, the dissemination of deepfake political speeches, and the hijacking of trending hashtags to spread misleading narratives. Topics frequently manipulated include civil-military tensions, corruption allegations against Israeli officials, and fabricated reports of IDF misconduct in Gaza³.

One notable trend is the impersonation of trusted sources, such as journalists and military analysts, to gain credibility. Iran's cyber strategy incorporates psychological operations (PSYOP) methodologies designed to demoralize the Israeli public and erode confidence in the state's resilience during wartime. These efforts are supported by sophisticated tactics, including automated amplification through botnets and cross-platform content laundering⁴.

Highlights PSYOP strategies employed by Iranian-affiliated networks, including impersonation of Israeli military commentators and the use of fake Hebrew-language news

¹ https://www.isoc.org.il/sts-data/survey-of-violent-discourse-2024

² https://www.ynet.co.il/digital/technews/article/rktzoxxwa

³ http://bit.ly/3Y8Yv6C

⁴ Institute for National Security Studies (INSS), Israel – "Iranian Influence Operations: Beyond Cyberattacks" (2024).

The Use of Artificial Intelligence

The integration of AI tools into disinformation ecosystems has increased the volume, realism, and speed of false content dissemination⁵. AI-generated images, audio clips, and videos—some mimicking well-known figures or portraying fabricated "eyewitness" footage—circulate widely. These materials exploit audiences' emotional vulnerability in response to trauma, reinforcing bias and fueling retaliatory sentiments.

Fake images and false news items alleging war crimes—designed for maximum virality—affect international perceptions and policy debates. Within Israel, these materials have intensified public anger and calls for retribution. The increasingly blurred line between authentic and synthetic content continues to strain fact-checking mechanisms and challenges traditional media's ability to act as a reliable source of information.⁶

Thoughts

Disinformation and digital hate are growing threats that demand immediate attention. The following are some proposed approaches:

Improve Digital Literacy

Introduce mandatory media literacy programs across educational institutions, emphasizing critical thinking, source evaluation, and digital ethics. Public awareness campaigns should also target adults who are vulnerable to disinformation.

• Increase Platform Accountability

Promote collaboration between Israeli regulators and technology firms to improve the identification and removal of harmful content. Require regular transparency reports detailing moderation actions, algorithmic changes, and enforcement policies relevant to Israeli users.

Support Independent Monitoring

Allocate funding to civil society organizations and academic institutions that monitor disinformation trends, conduct forensic analysis of information operations, and raise public awareness. Establish a centralized repository for known disinformation campaigns to support cross-agency coordination.

• Foster Inclusive Dialogue

Support community-based programs that promote dialogue between different social groups. Encourage cultural and educational institutions to host forums aimed at depolarizing discourse and reducing online radicalization.

• Invest in Technological Solutions

Advance Al-based tools for content verification, deepfake detection, and textual analysis. Encourage public-private partnerships to develop real-time threat identification technologies and integrate them into national law enforcement and emergency response systems.

pages to spread demoralizing content during periods of conflict escalation. Emphasizes cross-platform dissemination and botnet usage to amplify hostile narratives.

⁵ https://www.mako.co.il/nexter-news/Article-9e1831b2c62ce81026.htm

⁶ https://www.ynet.co.il/digital/technews/article/hjsr115uujg