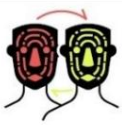
The national struggle with foreign influence in the digital space

Table of Contents

מילון מונחים | השפעה זרה

 דיסאינפורמציה (Disinformation)	מידע כוזב המופץ במכוון כדי להטעות, לפגוע או להשפיע על דעת הקהל והמדיניות הציבורית.
 מידע מטעה / מפוברק (Misinformation)	מידע שגוי או שאינו מבוסס על עובדות, המופץ לציבור ללא כוונת זדון.
 מאל-אינפורמציה (Mal-information / Mis-cntext)	מידע עובדתי ואמיתי שהוצא מהקשרו במטרה לעשות מניפולציה, להטעות ולייצר מצג שווא.
 חדשות כזב (Fake News)	הפצת מידע שקרי או מסולף המוצג בצורה מכוונת כדיווח חדשותי אמיתי. חדשות כזב משמש לעיתים קרובות להפצת דיסאינפורמציה, להשפעה על דעת הקהל או ליצירת פרובוקציות פוליטיות וחברתיות.
 דיפ פייק (DeepFake)	טכנולוגיה מבוססת בינה מלאכותית המאפשרת לשנות או לעבד את התוכן של תמונות או סרטונים מבלי שניתן יהיה להבחין שהתכנים זויפו.
 התנהגות לא אותנטית מתואמת (Coordinated inauthentic behavior - CIB)	רשת של חשבונות מזויפים הפועלים במתואם להטיית דעת הקהל, תוך הסתרת זהותם האמיתית של העומדים מאחוריהם.
 בוטים	חשבונות ברשתות החברתיות המופעלים באופן אוטומטי באמצעות תוכנה על ידי גורמים עוינים, מתחזים למשתמשים אמיתיים ומשמשים לצרכים שונים כגון הפצת דיסאינפורמציה ותעמולה.
 טרולים	משתמשים שמפרסמים בכוונה תכנים פוגעניים או מעוררי מחלוקת במרחב הדיגיטלי כדי למשוך תשומת לב, להכעיס, לעורר פרובוקציה או להפריע לשיח במרחב זה.
 אווטאר	זהות ויזואלית המייצגת משתמש במרחב הדיגיטלי. ניתן להשתמש באווטאר להתחזות ברמת אמינות גבוהה.
 FIMI (Foreign Information Manipulation and Interference)	דפוס התנהגות שאינו חוקי ברובו, המאיים או בעל פוטנציאל להשפיע לרעה על ערכים, נהלים ותהליכים פוליטיים. פעילות זו נושאת אופי מניפולטיבי, ומבוצעת על ידי שחקנים מדינתיים או לא מדינתיים.
 תיבת תהודה (Echo Chamber)	מצב שבו מידע, רעיונות או אמונות מתחזקים ונשמעים שוב ושוב בתוך קהילה מוגדרת, ללא חשיפה לדעות שונות. הדהוד ברשת נגרם כאשר אלגוריתם מזהה את ההעדפות של משתמשים ו"דוחף" להם תוכן דומה, במקום תוכן מגוון.

introduction

Foreign influence - general

Foreign influence operations, which aim to influence the feelings, opinions, or behavior of the target country's public in order to achieve a strategic goal, are not new practices. Foreign influence refers to the set of operations through which an international actor can influence a specific target audience and decision-makers in order to advance its interests. Influence operations can be perceived differently depending on the interests, values, and norms of each country. In the broad sense [1]

At one end of the spectrum are legitimate influence efforts that are not perceived as jeopardizing the national interests and values of the affected country. For example, traditional diplomatic activities, lobbying activities carried out in accordance with the provisions of the country's law, cultural collaborations, and the use of communication channels. These activities are often carried out with academic transparency, investments in companies, and in accordance with the relevant provisions of the law. [2]

At the other end of the spectrum are efforts at influence, sometimes called "foreign interference" or "hostile foreign influence," which refer to illegitimate actions by a foreign entity that aim to harm the interests or values of the affected state and, in some cases, go so far as to fundamentally undermine the state's sovereignty. These actions are generally carried out covertly or subversively. These actions can be expressed, for example, in attempts to influence public opinion and decision-makers through manipulation of the media; in influence operations on social networks; in leveraging investments in strategic infrastructure to exert political pressure; in leveraging investments in technology companies and academic collaborations to obtain sensitive technologies; and in attempts to influence legislation and regulation.
[3]

This report focuses on efforts to protect the Israeli public from foreign influence in the digital space, which is carried out in a disguised manner with the aim of harming Israel's national interests (hereinafter referred to in this report as foreign influence).

Foreign influence in the digital space

In recent years, the importance of the influence dimension in the field of information has become more acute, including, among other things, the exploitation of the digital space for influence purposes, the spread of false news, the misuse of data and its manipulation. One of the main arenas in which attempts at foreign influence are made is social networks, for example through campaigns that include misleading information and disinformation, combined with various methods to increase

---

1 The term "foreign influence" has various definitions and interpretations. According to some, there is a distinction between "foreign influence" and "foreign interference," but there is no consistent distinction between the ways in which these concepts are used. Some limit foreign influence to the information domain, while others refer to influence as activity in various fields such as trade and investment; some emphasize the purpose of influence as a central part of the definition; some refer to the aspect of transparency versus covert influence; and some distinguish between legitimate or legal activity and activity that is not. See Dr. Ofer Friedman, "The Conceptualization of the Terms Foreign Influence and Foreign Intervention," **Modi'in - Halacha and Acts :** 10 **Foreign Influence and Intervention as a Strategic and Intelligence Challenge** (2024) (hereinafter - **Intelligence - Law and Practice** 10), Institute for National Security Studies, Ministry of Intelligence (Ministry of Innovation, Science and Technology) and the Institute for Research on Intelligence Methodology (IIM), 2024, pp. 8 - 15.

2 Economic activity and investments by foreign entities in specific areas of the local economy allow for the development of a "cluster of influence" resulting from multiple holdings by a foreign entity. In this context, see: Advisory Committee for Examining National Security Aspects of Foreign Investments, **Methodology for Examining National Security Aspects of Foreign Investments** (2024). https://www.gov.il/BlobFolder/policy/foreign-investment-board-methodology/he/Procedures_foreign-investment-board-methodology.pdf.

3 The Institute for Security Studies in collaboration with the FakeReporter Association, commissioned by the Ministry of Intelligence, **Foreign Intervention and Influence on Social Media in Israel, Policy Research** (2023). On this subject, see also : https://www.fbi.gov/news/testimony/worldwide-threats-110519.

4. These are carried out by states and organizations while impersonating a local entity (or distributing those messages to a non-hostile foreign entity), in such a way that the target audience is unaware that they are being exposed to content distributed by a hostile foreign entity, the purpose of which is to harm the interests of the target audience.

Foreign influence reflects a threat to the proper functioning of the democratic regime: its purpose is to influence public opinion and the way people act and vote in elections, to create political or public instability, to incite panic and undermine public confidence in government, to derive advantages in the context of a military conflict, and to influence the activities of politicians, organizations, and individuals.[5]

Figure 1: **Consequences of foreign influence**

Disinformation is a key tool in the hands of geopolitical actors interested in spreading extremist beliefs and influencing electoral systems.[6] According to the World Economic Forum, the massive spread of disinformation in the digital space has been identified as a key global risk that could serve as a potential catalyst for the erosion of social cohesion and undermine trust in information and political processes.

Similarly, according to the OECD , the spread of false information (Fake News) is misleading, polarizing, and damaging to public debate and the social fabric. Disinformation and false information campaigns, strategically organized by[7] domestic or foreign actors, can have far-reaching effects in a variety of policy areas, including public health and national security. These phenomena undermine trust in facts,

---

4 https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702575/EXPO_IDA(2023)702575_EN.pdf

5 Amit Ashkenazi, "A Proposal for Guidelines for Israel's Dealing with Foreign Influence in Cyberspace and Social Networks," **Intelligence – Law and Practice ,** 10 Institute for National Security Studies, Ministry of Intelligence (Ministry of Innovation, Science and Technology) and the Institute for Research on Intelligence Methodology (MIMT) (2024). (2023), p. 24.

6 Shoa, C., also see, this is about the World Economic Forum, Ciampaglia, GL, Varol, O. et al. The global risks report (2018) The spread of low-credibility by social bots content

7 https://www.oecd.org/en/publications/facts-not-fakes-tackling-disinformation-strengthening-information-integrity_d909ff7a-en.html

Exacerbating existing tensions and making it difficult to create the social agreements needed to cope
With complex challenges.

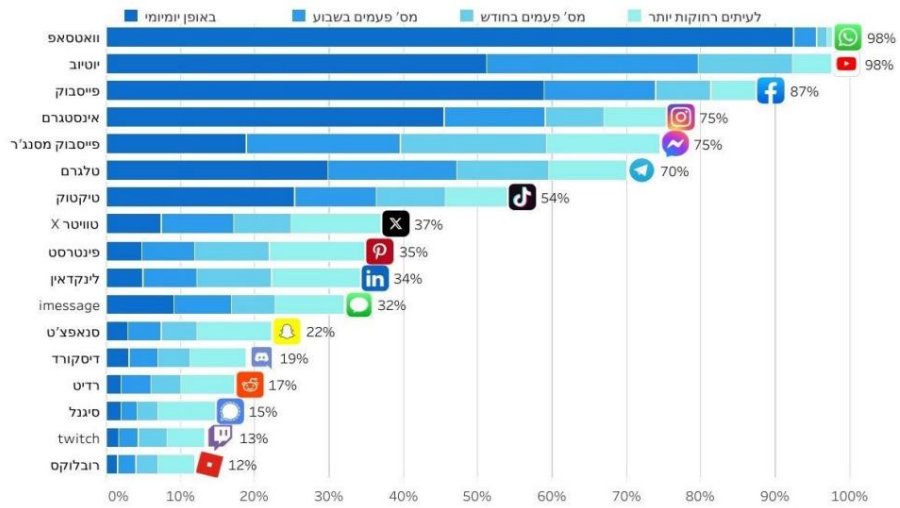
The scope of the company's activities

Social networks hold significant benefits for the individual and for democratic society. They allow everyone to voice their opinion, reach broad audiences without cost or territorial limitations, be exposed to a variety of opinions and ideas, and be updated almost instantly on what is happening around the world. In recent years, the use of social networks has increased worldwide, and in Israel in particular.
Below is data on the use of social networks worldwide and in Israel.

Figure 2: **The number of social media users worldwide, February 2025**

8, processed by the State Comptroller's Office.Source: Digital 2025: Global Overview Report

Figure 3: **The extent of use of social networks and online services in Israel (among those aged 18 and over) - 2024 data**



.[9]Source: Israeli Internet Association

For many, social media has replaced traditional media channels. A growing audience now consumes news from social media, sometimes exclusively.

[8] https://datareportal.com/reports/digital-2025-global-overview-report

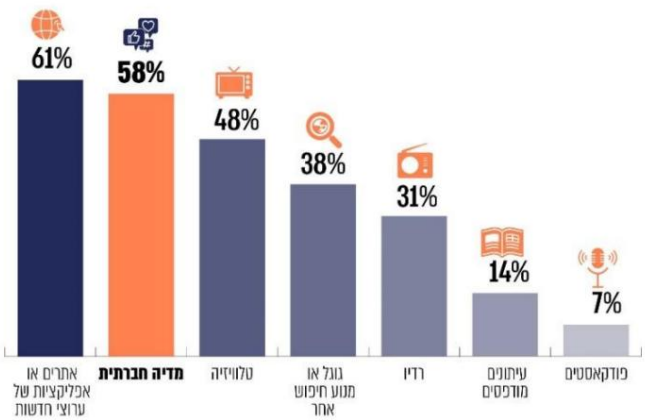
[9] Israeli Internet Association, Use of Social Networks and Online Services in Israel: 2024 Data with Demographic Segmentations (2024), https://www.isoc.org.il/sts-data/online_services_index

Figure 4: **Proportion of users of social media as a source of news consumption in selected countries around the world, February 10, 2024**
18 years old and older,

According to 2025 Statista data, processed by the State Comptroller's Office.

Similarly, in Israel, the use of social networks as a source of news consumption is relatively widespread.

Figure 5: **How the Israeli public frequently consumes news, according to different information technologies, 11,2024, ages 18 and over**



According to a survey by the Israeli Internet Association and the Technion, processed by the State Comptroller's Office.

Data from a survey by the Israeli Internet Association and the Technion indicate that approximately 58% of Israelis frequently update their news via social media. The survey also revealed that 78% of secular young people (Arabs and Jews) up to the age of 39 prefer to update their news via social media. As age increases, the rate of use of social media decreases and news consumption is mainly via television (71% among those aged 50 and over) and via websites or apps for news consumption (65%).

10 https://www.statista.com/statistics/718019/social-media-news-source
11 https://www.isoc.org.il/sts-data/media-and-disinformation-survey-il

From the above, it appears that a significant proportion of the population around the world and in Israel uses social networks, and they serve as a central channel for consuming news. The establishment of social networks as a central channel for public discourse, information consumption, and news illustrates the possibility of maintaining direct, continuous communication with the majority of the population through social networks, without the need for an intermediary, and for this reason they serve as a channel for attempts at foreign influence. [12]

We use digital maps and the company's network to provide information about the region.

Z R H

The characteristics of the digital space, and in particular social networks, are exploited by those who attempt to exert foreign influence to achieve their goal: social networks allow users to maintain anonymity; to disguise the user's true identity and deceive other users about his identity and goals; to overcome territorial restrictions for the purpose of distributing messages, along with low costs for their creation and distribution, and the ability to target audiences. The economic model and algorithmic structure of social networks, rapid distribution and targeting [13] And the use of "bots" and "avatars" - make it possible to create the impression that public opinion is leaning in a certain [14] direction and influence the exposure of certain content, thereby distorting the authentic discourse.

Social networks create “echo chambers” of like-minded users, who primarily disseminate and receive information that aligns with their worldview, thereby reducing their exposure to alternative viewpoints. This dynamic strengthens ties between previously isolated groups, while at the same time leading to the radicalization of opinions and deepening polarization regarding policies, public institutions, events, moral issues, and social trends. Deepening polarization may reduce the ability to reach compromises and undermine social cohesion. [15]

The use of artificial intelligence tools holds almost unlimited possibilities when it comes to foreign influence. A hostile entity can use them to create credible content tailored to the target audience - text, images, video, in large [16] In the digital space volumes and with low investment in a short time; overcome cultural and language barriers, easily create many fictitious identities that will spread and resonate messages in a systematic and continuous manner, while strengthening the authenticity of those identities and making their exposure complex.

US Department of Homeland Security (DHS)

The 2025 Homeland Security Threat Assessment found that Iran, China, and Russia are expanding their use of generative artificial intelligence to create more persuasive text, audio, and synthetic fake videos, potentially improving their ability to reach U.S. audiences while obscuring their true origins. [17]

Various publications indicate that various countries have used artificial intelligence in an attempt to exert foreign influence.

---

12 Assaf Wiener, "National Preparedness Against Foreign Influence and Intervention Through Social Networks: Global Findings and an Israeli Situational Picture," **Intelligence - Law and Practice** 10 Institute for National Security Studies, Ministry of Intelligence (Ministry of Innovation, Science and Technology) and the Institute for Research on Intelligence Methodology (2024) Directing tailored messages to specific groups or individuals, while analyzing information collected about them while surfing the web.

13 Dganit Peikovsky and Eviatar Matanya, **"Cyber Influence Operations - Characteristics and Insights",** The Campaign for Consciousness - Strategic and Intelligence Aspects, Intelligence Halacha and Practice (2019) .

14 https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf, p. 74.

15 For more information, see Lt. Col. T.Z., serving in the Intelligence Directorate, “The War of Influence in the Network: Artificial Intelligence as a Disengaging Weapon,” **Intelligence - Law and Practice ,** 10, Institute for National Security Studies, Ministry of Intelligence (Ministry of Innovation, Science and Technology) and the Institute for Research on Intelligence Methodology (IMM), (2024), pp. 172-179.

16 Homeland Threat Assessment, 2025. https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf

17

Image 1: **Different countries' use of artificial intelligence for influence18**

Source: Microsoft Digital Defense Report, 2024.

The above indicates that the characteristics of the digital space, and in particular social networks, are being exploited for attempts at foreign influence. The use of artificial intelligence tools and technological advances are expected to increase the motivation of those with vested interests to intervene and influence target audiences in a way that could undermine the perception of reality and cause social and political damage, including improper interference in elections, widening rifts in society, directing public discourse in accordance with foreign interests, and undermining public trust in the country's ins

D u g m a n a t l i s y o n a t l i s h e p e h z r h in the digital world

USA: The issue of foreign influence in the digital space and the risks inherent in it rose to the public agenda during the 2016 US presidential election. In 2017, the US intelligence community published an assessment stating that Russia attempted to influence the US election through an influence campaign, in order to undermine public confidence in the American democratic process and promote the chances of one candidate being elected over another.[20] The assessment noted that the influence campaign included overt and covert actions, including on social media, and also that the scope of Russia's activities had increased considerably compared to previous influence operations.[21]
A study published in 2023 estimated that at least 32 million US Twitter users were exposed to content from a Russian influence operation during the 2016 presidential election. It should be clarified that the study did not find any

18 https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft- brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf

19 It should be noted that in 2025, changes occurred in the United States' dealing with threats of foreign influence and interference in the digital space. On this matter, see David Siman Tov, "The Trump Administration's Withdrawal from the Fight Against Foreign Interference - Strategic Implications," Institute for National Security Studies (2025).

20 Office of the Director of National Intelligence, Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytical and Process Cyber Incident Attribution, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf

21 Evaluation of the US Department of Justice's Efforts to Coordinate Information Sharing About Foreign Malign Influence Threats to US Elections, 2024
Office of the Attorney General's Office also reported this; https://oig.justice.gov/sites/default/files/reports/24-080.pdf
GAO, US Government Accountability Office, - American State Comptroller FOREIGN DISINFORMATION: Defining and Detecting Threats (September 26, 2024 (

Evidence of a significant relationship between exposure to foreign influence campaigns and changes in attitudes, polarization, or voting patterns.[22]

It has been noted that Britain is a target of Russian disinformation campaigns and political influence operations, and concerns have been raised that Russia attempted to influence the 2016 referendum on Britain's membership of the EU.[23] **BRITAIN: In** a 2020 report by the British Parliament's Intelligence and Security Committee

The European.

TAIWAN: Taiwan's National Security Council (NSB) published a report in 2024 on China's patterns of disinformation against Taiwan on social media, including the use of artificial intelligence tools, fake accounts, and impersonation of local officials, to undermine public trust in the government and create social tensions. 24

EUROPEAN UNION: The European Union addresses manipulation and foreign interference in information (hereinafter - FIMI25). A report published by the Union in 2025 details how, alongside official and identified channels, Russia and China[26] are using the digital space extensively and covertly for FIMI activity. In this, FIMI events were identified that were directed against 90 different countries, especially Ukraine, as well as against France, Germany, Moldova. It was noted that social media platforms served as an arena for FIMI activity, through tactics such as botnets, coordinated and inauthentic behavior, impersonation[27] and countries in Africa and the creation of fake news sites, and the use of artificial intelligence tools.

GERMANY: In June 2024, the German Federal Foreign Office published a report analyzing the activities of a campaign. It was identified that this campaign is working to undermine public support for Ukraine[28] Pro-Russian in Germany (Doppelganger) and increase political polarization in Europe. The report noted that over a six-week period (December 2023 to January 2024), over 50,000 fake accounts were identified that published over 1.8 million posts in the German language. It was also noted that the network demonstrated a high level of automation, and on certain days managed to publish more than one tweet per second in a coordinated manner. In addition, it emerged that the campaign was based, among other things, on a network of over 60 websites that impersonated legitimate news organizations, and that at least 16 artificial news portals were identified that published over 12,900 articles over a 14-month period. The report clarified that the campaign's posts were regularly viewed ·millions of times per month. 29

---

22 Nature, Exposure to the Russian Internet Research Agency foreign influence campaigns on Twitter in the 2016 US election and its relationship to attitudes and voting, 2023.

23 Intelligence and Security Committee of Parliament, "Russia'" HC 632 (21 July 2020)

24 https://www.nsb.gov.tw/en/assets/documents/%E6%96%B0%E8%81%9E%E7%A8%BF/1eeba30c-ebf8-459a-8fe3-ed2a54cb4ca0.pdf?utm_source=chatgpt.com

25 FIMI - Interference and Manipulation of Foreign Information, defined by the European Union as "pattern "Behavior that is largely illegal, that threatens or has the potential to negatively affect political values, procedures, and processes. This activity is manipulative in nature, carried out in a deliberate and coordinated manner, by state or non-state actors, including proxies and elements operating from within or outside their territory."

26 https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en

27 European External Action Service (EEAS) (March 2025) 3rd EEAS Report on Foreign Information Manipulation and Interference Threats https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

28 Federal Foreign Office, Germany Targeted by the Pro-Russian Disinformation Campaign "Doppelganger", 2024

29 However, the viewing data includes not only real users, but also "self-generated" views generated by the campaign's bot accounts, so it is difficult to accurately assess the reliability of the data and the extent of exposure.

ROMANIA: In December 2024, the Romanian court annulled the first round of the presidential election. The decision stated that voters had been misinformed by an election campaign in which one of the country's 30 of the candidates was promoted aggressively, circumventing the provisions of the law and exploiting the algorithms of social media platforms. Following this and in light of the existence of indications that external actors interfered in the presidential elections in Romania through the use of social networks, the European Union opened an investigation against one of the social networks. In this regard, the President of the European Commission stated: "We must protect our democracies from any kind of foreign interference. When we suspect this, especially during elections, we must act quickly and decisively." [31]

D o g m a n a t I n i s y o n a t l o f t h e s h e r e b e r t h e d i g i t l i s h e r e n t i o n in Israel

As for Israel, in recent years, including since the outbreak of the "Iron Swords" War (hereinafter - the Iron Swords War), attempts at foreign influence on the Israeli public have been identified by various countries, including Iran, who identified the polarization in Israeli society as an opportunity to advance their goals. Examples of this will be presented below.

1. A November 2022 Cyber Command document noted that over the years, foreign influence campaigns have been identified that aim to promote agendas and narratives that benefit the governments in whose name those behind them operate, through activity on social networks. For example, in 2019-2020, a platform of fictitious accounts operating on social networks was identified that impersonated American politicians and American and Israeli media outlets in order to promote Iranian interests in the region; and in 2022, Iran invested efforts in conducting the awareness campaign against Israel, for example around the elections, Iranian Jerusalem Day, and the start of the school year. The aim of these moves was to create unrest and division in the Israeli public by echoing messages in text messages (SMS) and on social networks.

2. Various documents from one of the security agencies from 2023 noted that in recent years, increasing activity of foreign influence on Israeli society has been identified, which accompanied social protests and even the recent Knesset elections, and that the activity is carried out mainly on social networks, which serve as a comfortable platform for anonymous activity to spread ideas and stir up discourse.

The documents also show that the Iranian security and intelligence agencies identified the protests in Israel in 2023 as a significant opportunity to initiate influence activities aimed at undermining internal stability in Israel, deepening divisions, and inflaming events on the ground into violence. Another motif identified in the influence activities surrounding the protests is a desire to encourage people to move from online activity to the field - creating contact with people in Israel in an attempt to motivate them to take action, to the point of violent activity and activity that serves a variety of Iranian needs. It also appears that at the same time, attempts were identified to conduct influence activities against Israeli Arabs.

3. In addition, attempts at foreign influence activity were identified online around the election campaign sequence. These attempts were made while impersonating elements from all sides of the internal disputes in Israel, and on a variety of networks - Facebook, Instagram, Telegram, Twitter, and WhatsApp. In addition, in June 2023, a number of foreign online campaigns were identified, and it was assessed that these campaigns constitute platforms through which covert foreign intervention will be carried out during the elections.

4. Another campaign that was identified was called “The Traitors’ Trial.” In the framework of which photos and details of police officers were published alongside the caption “Traitors.” It was assessed that this was an Iranian action, as part of its effort to exploit the

30 RULING No. 32 of 6 December 2024 on the annulment of the electoral process for the election of the President of Romania in 2024
https://www.ccr.ro/wp-content/uploads/2025/02/RULING-No-32-2024.pdf

31 European Commission - Press release (17.12.24

The protest against the reform is intended to deepen social polarization in Israel, encourage violence between groups in the population, and destabilize the country. The Israel Police issued a statement to the public, stating that, according to security officials, there is a high probability that this is a campaign by a foreign country aimed at causing friction in the public.[32]

Image 2: **Israel Police announcement about a foreign country's campaign from June 2023**

Source: Israel Police, Twitter.

On January 5, 2024, the Shin Bet released information to the public about several online platforms that are suspected of being operated by the Israeli government. In particular, it was revealed that as part of the protests for the return of the abductees, Iranian security officials are promoting, through various online platforms, active actions of hanging signs they have drafted, photographing protesters, and filling out surveys in order to obtain personal information. It was noted that campaigns suspected of being operated by Iranian security officials were identified, including the "Tears of War" campaign, which promoted inflammatory and radicalizing content and worked to recruit Israelis using fictitious profiles to carry out missions regarding the abductees; the "Second Israel" and "Avengers" campaigns - which operated undercover on various platforms to inflame political discourse and deepen divisions in Israel.[33] by Iranian security officials

6. A study conducted in 2025 for the Ministry of Diaspora 34 identified, among other things, bot networks that operate in a coordinated manner, and with a high probability under the direction of Iran, designed to intimidate the public in Israel through publications with threatening messages and intensifying vulnerabilities in the army and the home front.

32 Israel Police, message from 11.6.23 - Twitter.

33 Shin Bet website ,Shin Bet reveals several online platforms suspected of being operated by Iranian security officials (15.1.24)

34 Ministry of Diaspora and the Fight against Anti-Semitism, **organized activity of Iranian support on social media through fake accounts as part of the war "with the people of Kalavi" (after the first days of fighting)** (June 2025).

Image 3: **Examples of social media posts intended to scare the Israeli public**

Source: Ministry of Diaspora Affairs and the Fight against Anti-Semitism.

,On February 7, 2025, the National Cyber Directorate published a National Cyber Defense Strategy document. [35]
In its statement, the organization stated that efforts to influence the mind of foreigners have increased to an unprecedented extent and have become a significant threat to national security and social resilience. It was noted that the purpose of these attacks is to undermine trust in government institutions, erode the sense of personal security while engaging in cyber-terrorism, deepen social divisions and damage the community fabric, harm public morale and influence public opinion in Israel and around the world.

Technology companies also occasionally address foreign influence operations they have detected. One report noted that Iran had carried out influence operations against Israel, including by using the companies' names from February 36, 2024. Destabilization, intimidation, and undermining international support for Israel. This includes the identification of activities by Iranian groups that used impersonation techniques to spread false messages about the hostages and send threatening messages to Israelis; and cases were even identified in which Israelis were encouraged to hang political posters on by Iranian impersonators. [37]

35 https://www.gov.il/BlobFolder/news/cyber_strategy_2025/he/Israel%20National%20Cyber%20Security%20Strategy%202025.pdf Command, National Cyber Defense Strategy, 2025. Microsoft,

36 Iran surges cyber-enabled influence operations in support of Hamas, 2024

37 Microsoft periodically publishes an analysis of risks and trends in the digital space based on its own analyses. In particular, the company addresses attempts at foreign influence in its publications.

Image 4: **Hanging political posters at the instigation of Iranian elements**

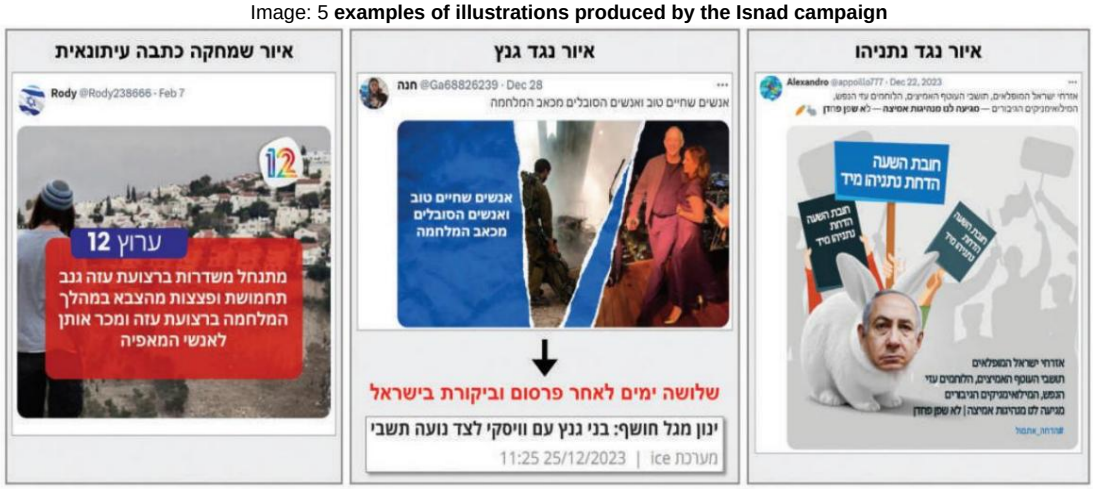
Source: Microsoft Threat Intelligence, 2024.

In 2023-2024, another company reported on foreign influence networks operating in a coordinated and inauthentic manner originating, among others, in Russia, Iran, and China. Some of the influence operations were directed against Israel 38

Alongside technology companies, civil society and research groups are also conducting in-depth research and attempting to describe 40 39 . In a 2024 article

To detect foreign influence on social networks using various tools A foreign influence network called "Isnad", which aims to bring about an end to the Iron Sword War on terms favorable to Hamas, by influencing Israeli public opinion. The data analysis carried out revealed that between December 2023 and August 2024, thousands of messages were written as part of the campaign, and the number of fake profiles operating as part of the campaign on the social network X (formerly Twitter) alone was between 300 and 1,000.

Image: 5 **examples of illustrations produced by the Isnad campaign**



Source: "'Isnad' a Civil-Islamist Foreign Influence Campaign" 41

38 /https://transparency.meta.com/en-gb/metasecurity/

39 Among these factors are the Fake Reporter Association, INSS, the Institute for the Study of Intelligence Methodology, and the Center for the Study of Intelligence

40 Heritage. See Michal Farah and Inbar Yasur, "'Isnad': A Civil-Islamist Foreign Influence Campaign," **Intelligence – Law and Practice** 10, Institute for National Security Studies, Ministry of Intelligence (Ministry of Innovation, Science, and Technology), and the Institute for the Study of Intelligence Methodology (2024), pp. 81-113. Ibid.

41

Image 6: **An example of a tweet produced by the Isnad campaign, which infiltrated the internal discourse in Israel**

Source: "'Isnad' a Civil-Islamist Foreign Influence Campaign."

As can be seen in the example above, foreign influence may penetrate domestic discourse and even discussion among decision-makers at the national level.

Foreign influence in the digital space may have different patterns of operation. For example, in September 2024, approximately 5 million SMS messages were sent to citizens of the country, including some that were supposedly sent on behalf of the Home Front Command and included an emergency alert for immediate entry into a protected area, in order to cause panic among the public. A statement issued by the Cyber Directorate stated that after investigating the incident, it emerged that Iran and Hezbollah were behind the sending of the messages. The text messages 42

Image 7: **Example of a text message sent to millions of citizens by Iran and Hezbollah**

D u g m a u t l n i s y u n u t l h s p e h z r h b z i r h h b i n - l a u m i t s h n u e d u l p g u e b a i n t r s i m y israel i m y s

Alongside attempts at foreign influence on the Israeli target audience, actions have also been identified that aim to influence the international audience's position regarding Israel and its actions and may affect its freedom of decision and action in a variety of areas. For example, reports from the Ministry of Strategic Affairs from 2019-2021 revealed that hostile foreign elements operated through influence campaigns on social media to create the false impression that there was widespread anti-Israeli discourse in various contexts, for example:

2019: The report revealed that various organizations around the world were involved in improper public opinion influence activities to present the appearance of a large-scale popular campaign against Eurovision, public broadcasters and artists , thereby exerting pressure on them to join the demand not to hold Eurovision in Israel.

42 Announcement from the National Cyber Directorate on the subject of "Iran and Hezbollah behind the distribution of alarming text messages" (19.9.24).

DERODENUSHATIONALEGITIMCIONSONGONS ,

After the outbreak of the Iron Sword War, the Ministry of Diaspora revealed in several studies that there was extensive, inauthentic, coordinated activity on social media, the purpose of which was to spread false messages in Arabic and English against Israel among international target audiences. A study that analyzed the discourse on the social network X in the first three weeks of the war indicated the presence of fake profiles[43] who dealt with inciting content during the war. In a study from 2025 Among other things, bot networks were identified that operated in a coordinated manner, and with a high probability directed at Iran, to undermine relations between the United States and Israel, especially around the possibility of an attack on Iran, as well as bots that were seen to incite hostility toward Israel and Jews in the United States and to present it to the world as a terrorist state.

Image: 8 **Examples of social media posts that encourage hostility towards Israel and Jews around the world**

Source: Research by the Ministry of Diaspora and the Fight against Anti-Semitism, 2025.

The US Directorate of National Intelligence also identified attempts at foreign influence activities regarding Israel and published a statement on 9.7.24, according to which Iranian government officials tried to exploit the wave of demonstrations surrounding the war in Gaza to advance their interests and posed as activists on social media to encourage the demonstrations and even provide financial support to the protesters. [45]

One example of the dissemination of campaigns that encourage hostility and delegitimization towards Israel and its actions is an Iranian influence campaign that was identified by an Israeli company.[46] The campaign was conducted in the early days of the Iron Swords War (starting on 11.10.23) with the aim of creating and establishing the narrative of genocide in Gaza as early as possible, through widespread distribution on social media. The first image reflects the campaign's activity in the first 48 hours after its inception, when the discourse on the subject was mainly carried out by the campaign's operators, while the second image reflects the successful launch.

---

43 A fake profile was defined in the study as a profile that does not belong to the private use of a known person or organization, and is intended to impersonate a person in order to manipulate the discourse.

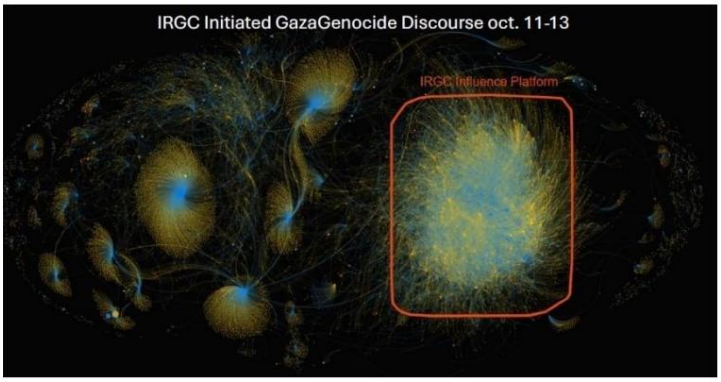
44 Ministry of Diaspora and Combating Anti-Semitism, organized **activity of Iranian support on social media through fake accounts as part of the "Kalavi" war (after the first days of fighting)** (June 2025).

45 Statement from the Director of National Intelligence, ODNI News Release No. 17-24, 9.7.24

46 Next Dim Company.

of the operation, when the discourse that the campaigners initiated under the Gazagenocide label became marginal in relation to the anti-Israeli discourse on this issue.

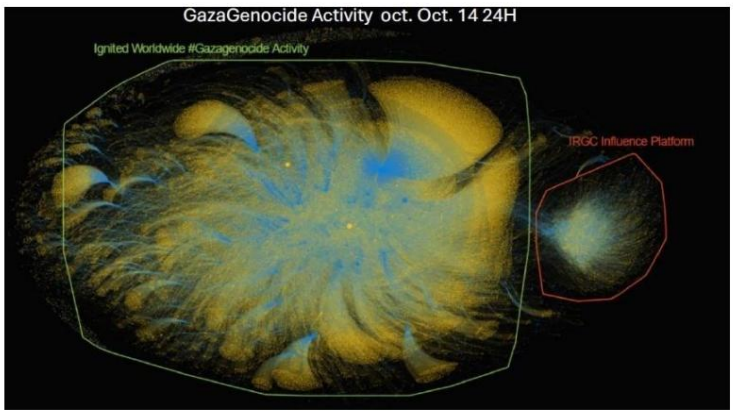
Image 9: **Activity on the Gaza genocide** issue **in the first 48 hours after the start of the impact activity (starting on 11.10.23)**



Source: Dim Next Company. *****

The section marked in red reflects the activities of a specific Iranian entity carrying out the foreign influence.

Image 10: **The assimilation of the Gaza genocide narrative and the expansion of anti-Israeli discourse**



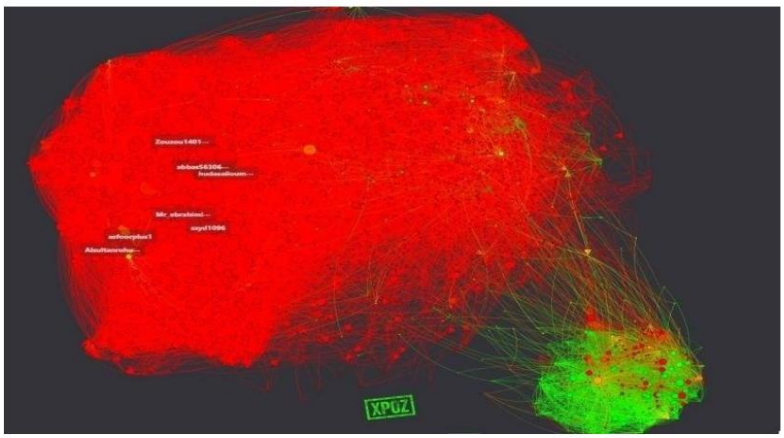
Source: Dim Next Company. *****

The section marked in red reflects the activities of a specific Iranian entity carrying out the foreign influence; the section marked in green reflects the anti-Israeli discourse that took place around the Gaza genocide issue.

Regarding the discourse that took place on social media,[47] another example can be seen in the analysis carried out by a certain social media company surrounding an event that occurred at Al-Ahli Hospital in Gaza in October 2023. Israel was accused of causing an explosion at the hospital, even though in reality the explosion was caused by a failed rocket launch by one of the terrorist organizations in Gaza.

47 XPOZ company.

Image 11: **Promoting a false narrative through coordinated inauthentic activity on social media**



Source: XPOZ Company.

*** Red markings represent inauthentic users (bots and identities with abnormal behavior, according to XPOZ Company classification algorithms ;) Green markings represent authentic users.**

The discourse analysis illustrates an attempt to influence public opinion through the coordinated echoing of a false narrative by a large number of inauthentic users, apparently dictated and led by elements hostile to Israel, who accused Israel of bombing the hospital.

Dealing with foreign influence in the digital space includes several main complementary pillars: identifying and assessing the threat; monitoring attempts at influence; action against online platforms, for example to remove content and close websites; and actions to raise awareness of the existence of attempts at foreign influence online and for the wise consumption of information (digital literacy). Alongside these actions, there may be additional actions, such as on the diplomatic level, against those behind the distribution of the content.

Figure 6: **Components of dealing with foreign influence in the digital space**

The issue insists that dealing with foreign influence in the digital space involves significant [48] Professional literature challenges, one of the main of which is the fear of harming freedom of expression. This is especially true given both the difficulty of tracing the identity of the publisher or distributor of the content, and the difficulty of knowing whether it is a hostile foreign entity, or part of the local discourse. This is because attempts at foreign influence are often carried out in the open civil space of social networks, which allows for the mixing of factors.

48 The campaign for consciousness - strategic and intelligence aspects, **Intelligence, Halacha and Practice,** (2019); "Intelligence - Halacha and Practice - Foreign Influence and Intervention as a Strategic and Intelligence Challenge", Institute for National Security Studies, Ministry of Intelligence (Ministry of Innovation, Science and Technology) and the Institute for Research on Intelligence Methodology (2024).

Israelis and foreigners. Another challenge concerns the difficulty of legal systems in dealing with misleading, harmful, or manipulative content - as long as it is not illegal.

Taking into account the risks identified by international organizations and various countries, stemming from attempts at foreign influence in the digital space, particularly during election periods, and the existence of such attempts regarding Israel, the State Comptroller decided to examine whether Israel has examined the risk and its implications and how it is dealing with it.

Audit operations

Between July 2024 and January 2026, the State Comptroller's Office conducted an audit of the government's dealing with foreign influence in the digital space. The audit dealt with identifying and assessing the threat and dealing with foreign influence, including during election periods. The audit was carried out at the National Security Headquarters (hereinafter - NSH), the Prime Minister's Office (hereinafter - PM's Office), the General Security Service (hereinafter - Shin Bet), the National Cyber Directorate (hereinafter - Cyber Directorate), the Central Elections Committee, the Ministry of Justice - the Cyber Department of the State Attorney's Office (hereinafter - Cyber Department), the Ministry of Defense - the Administration for Research and Development of Weapons and Technological Infrastructure (hereinafter - MAFAT), the Ministry of Education and the Ministry of Communications. Completion checks were held at the National Emergency Authority (hereinafter - RAHL) at the Ministry of Defense, the Ministry of Diaspora and the Fight against Anti-Semitism (hereinafter - Diaspora Ministry), the Ministry of Intelligence (which closed in March 2024) and the Ministry of Innovation, Science and Technology (hereinafter - Ministry of Innovation). In addition, meetings were held with civil society organizations, research and academic entities, and companies. Technologies dealing with the subject.

As stated, this report focuses on protecting the country's citizens from foreign influence efforts in the digital space. However, the threat posed by foreign influence at all levels is broader and includes many aspects such as: foreign investments, ties to academia and research institutes, investment in essential infrastructure, and the acquisition of technologies. This requires preparation and in-depth examination, including learning from the findings of this report.

The Subcommittee of the Knesset's State Audit Committee decided not to place this report in its entirety on the Knesset table, but to publish only parts of it, in order to preserve state security, in accordance with Section 17 of the State Comptroller Law, 5718-1958 [consolidated version].

Identifying the threat of foreign influence in the digital space

Identifying the threat in the world

The development of the digital arena, alongside the rise in awareness of the existence of foreign influence in this space and its characteristics, has led countries and international organizations to include the issue of foreign influence in the digital space as part of the definition of their threat environment.

EUROPEAN UNION: The European Union considers foreign information manipulation and interference (FIMI), including disinformation, to be one of the fastest-growing security and political challenges for the European Union, its immediate neighbours The European Union [49] and for global security and stability.
also sees FIMI as a tool that could undermine public trust in the legitimacy and effectiveness of democratic institutions; contribute to increasing polarization and division within the European Union; affect its ability to implement its policies within and outside the EU; escalate political violence in conflict zones and undermine its efforts to maintain peace around the world. The EU reports noted that hostile actors

[49] European Parliament, Foreign interference in EU democratic processes: Second report, 2023

FIMI is also used against countries seeking to join the Union, to divert them from the path of accession, sometimes while harming the policies and values of the European Union itself.[50]

The European Parliament has established two special committees to examine foreign interference in the EU's democratic processes - the first in 2020 and the second in 2022. Based on their findings, MEPs formulated recommendations to improve the EU's resilience to disinformation and foreign interference and to maintain the integrity of the work to expose information manipulation and disinformation.[51] The elections. In addition, a special task force was established. The task force's periodic reports deal with defining the methodology for examining hostile activity and include recommendations for state decision-makers and civil society to understand the threat and its implications, as well as tools for dealing with it .[52] At the same time, awareness-raising activities are taking place among EU citizens and a toolkit has been developed. In November 2025, the European Commission announced the launch of the " European Democracy Shield, " a package of measures designed to strengthen European democracy.[53] Educational tools on the topic of elections[54] Democratic states in the EU countries. Within this framework, a European Center for Democratic Resilience is being established that is intended to pool knowledge and resources from the EU institutions and its member states in order to help them identify and deal with threats to democracy, including dealing with manipulation and foreign interference in information and disinformation, while improving identification and response capabilities in this regard.

The OECD **DCE O:55** considers FIMI to be one of the aspects that threatens the integrity of information, which is essential for the exercise of the right to freedom of opinion and expression. In December 2024, recommendations were adopted on strengthening societal resilience to false information, misleading information and other forms of information manipulation. The recommendations point to the need to address the risks inherent in FIMI as well as efforts by foreign actors to weaken democracies using these practices.[56]

The World Economic Forum : 57th Annual Report of the World Economic Forum, which reviews global risks for the years 2024-2025, The risk of disinformation and false information was ranked at the top of the short-term risk list, due to its ability to undermine social stability and trust in government, and it is also included in the long-term risk list. The 2025 report noted that it is a key tool that foreign actors use to influence voter intentions; to sow doubt among the general public around the world about what is happening in conflict zones; or to serve as a mechanism to damage the image of products or services from another country.

50 https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

51 The task force was established as part of the European External Action Service (EEAS)

52 European External Action Service (EEAS) (February 2023) 1st EEAS Report on Foreign Information Manipulation and Interference Threats - Towards a framework for networked defence, https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information- 2nd Report (February 2024) manipulationand-interference-threats_en https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulationand-interference-threats_en ; 3rd Report (March 2025) https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport- March-2025-05-Digital-HD.pdf

53 https://www.europarl.europa.eu/topics/en/article/20240404STO20215/foreign-interference-how-parliament-is-fighting-the-threat-to-eu-democracy

54 European Commission, "European Democracy Shield: Empowering Strong and Resilient Democracies", Brussels, 2025

55 https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0505#backgroundInformation

56 https://www.oecd.org/en/publications/facts-not-fakes-tackling-disinformation- strengthening-information-integrity_d909ff7a-en.html

57 The World Economic Forum https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf ;

58 https:// weforum.org/publications/global-risks-report-2024

Figure 7: **World Economic Forum: Global risks in the short and long term ranked by severity**

Source: WEF - Global Risks Report, 2025.

UN: In the UN Global Risks Report 2024, which examined 28 risks, the risk arising from misinformation and false information topped the vulnerability index - an index that weighs the level of importance of the risk and the level of preparedness to deal with it. The risk was ranked third in importance and 25th in terms of government preparedness to deal with it. The report noted that this risk has the potential to exacerbate geopolitical tensions, create social divisions, and make it difficult to respond to crises. It was further noted that distrust and skepticism create an environment in which misinformation can be strategically deployed in order to manipulate public opinion and public policy. The report notes that in the coming decades, the risk of disinformation is expected to continue to intensify.

US :60 The issue of foreign influence in the digital space was included in the definition of the United States' threat environment. As part of the presentation of the global threat map to the Senate National Security Committee, the FBI addressed foreign influence operations in 2019. It was noted that the purpose of foreign influence operations is to: The aim against the United States is to spread disinformation, advance the political agenda of foreign countries, and undermine trust in democratic values and institutions; that this is a threat that has changed significantly due to globalization and the anonymity enabled by the Internet, and that the most common form of influence is attempts by adversaries outside the United States to covertly spread fake and false messages among large numbers of Americans on social media platforms. The FBI 's 2023 threat map also noted

59 The report is based on a survey conducted among stakeholders from government, the private sector, civil society and academia in 136 countries. https://unglobalriskreport.org

60 For more information on the United States' dealing with foreign influence operations, see Lt. Col. (res.) Yonatan Kedar and A., "The United States' Dealing with the Threat of Foreign Influence and Intervention," **Intelligence - Law and Practice** 10, Institute for National Security Studies, Ministry of Intelligence (Ministry of Innovation, Science and Technology) and the Institute for Research on Intelligence Methodology (MIMT) (2024), pp. 231-242. As stated, in 2025, changes occurred in the United States' dealing with threats of foreign influence and intervention in the digital space. On this subject, see David Siman Tov, **The Trump Administration's Withdrawal from the Fight Against Foreign Intervention - Strategic Implications,** Institute for National Security Studies (2025).

61 https://www.fbi.gov/news/testimony/worldwide-threats-110519

That the digital space has changed the nature of the threat of foreign influence, and that various countries are trying to increase division in the United States and undermine citizens' trust in democratic institutions and processes.[62]

The United States Department of Homeland Security noted in its 2025 Homeland Security Threat Assessment that state actors will continue to pose a threat to homeland and public security, including continuing to 63 by 2025. Use traditional media, inauthentic websites, social media, online bots, trolls, and individuals to amplify narratives that support their interests and conduct information operations targeting the United States to inflame divisions within the country. The Intelligence Community's 2025 Intelligence Assessment Report noted that China will continue its hostile influence efforts to weaken the United States, and that elements in China will increase their capabilities to spread disinformation.[64]

CAIRO: In the run-up to the 2017 French elections, a cyberattack and fake news campaign was identified with the aim of influencing a candidate's chances of being elected president. As a result, France began to examine the issue and revealed that a significant portion of the messages disseminated against France and the democratic regime on social media were the result of inauthentic behavior and manipulation of information by the monitoring and protection[65] Foreign actors. The growing understanding of the threat led in 2021 to the establishment of a dedicated body against foreign interference (VIGINUM). The organization's activities are limited to core issues concerning France's national sovereignty, and are carried out in cooperation with domestic and international government bodies dealing with the subject. The organization periodically publishes reports dealing with campaigns that have been detected. For example, in 2025, the organization published a report dealing with Russian influence operations on public opinion in France and Europe, including regarding the war in Ukraine.[66]

Countries and international organizations around the world, including the European Union, the OECD , and the World Economic Forum, have identified the threat of foreign influence in the digital space, including the use of disinformation as a strategic risk.

Countries differ in how they deal with this threat, and it is influenced, for example, by the assessment of the risk, its geopolitical environment and the internal values of each country. Dealing with the issue includes aspects that, by their nature, are not made public. However, some countries and organizations are publicly addressing some of the actions they are taking, such as promoting legislative measures to deal with this risk, as well as establishing dedicated task forces to deal with this risk, alongside[67]; establishing a disinformation challenge Harnessing existing agencies to address the issue; and formulating action plans to deal with it.[68]

62 FBI, (2023) Worldwide Threats to the Homeland

63 Homeland Threat Assessment, 2025. https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf

64 https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf

65 https://www.sgdsn.gouv.fr/files/files/Publications/RA-Viginum-Annee1-32p-V20_EN_LQP-1.pdf

66 https://www.sgdsn.gouv.fr/files/files/Publications/RA-Viginum-Annee1-32p-V20_EN_LQP-1.pdf

67 See more: Inter-organizational think tank (led by David Siman-Tov), "Disinformation Systems and the Influence of Foreign Factors on Consciousness", The Campaign on Consciousness - Strategic and Intelligence Aspects, **Intelligence, Law and Practice,** (2019); Dudi Siman Tov and Liav Sela, **The Role of Intelligence in the Face of Foreign Influence on Democratic Processes - In-depth** Research (2020).

68 Tools of disinformation, from the Cybersecurity and Infrastructure Security Agency For example see https://www.eeas.europa.eu/eeas/inside-infrastructure-foreign-information-manipulation-and-interference-fimi-operations_en Disinformation.ch, (CISA)

Identifying the threat in Israel, gaps and deficiencies in providing an inter-organizational government response to deal with it

In parallel with the identification of the threat in various countries around the world, starting in 2017, various government agencies in Israel also identified the threat of foreign influence in the digital space, and in particular on social networks, and the need to formulate a national inter-organizational response to deal with it. It should be noted that alongside the government agencies that identified the threat, research institutes, academia, and civil society agencies also published various publications on the threat inherent in foreign influence in general and foreign influence in the digital space in particular.[69] Various publications raised, among other things , the need to recognize the threat as a potential strategic threat, which requires systemic organization. Since 2020, the Shin Bet has been carrying out certain operations to detect and monitor attempts at foreign influence online (see below in the chapter relating to monitoring operations).[70] Organizations to deal holistically with the issue. Below is a breakdown of the government actions taken in these years:

2017 - 8:201 November **1.1 DISCUSSIONS IN THE NSC AND THE WORK OF THE CYBER ACTION** 2017 A discussion was held in the NSC with the aim of reviewing the threat of espionage and foreign influence on the State of Israel, the responses from the security community bodies and the gaps in the issue at the national level. In concluding the discussion, the Head of the NSC stated, among other things, that the State of Israel is a target for espionage and foreign influence from superpowers and other adversaries, and that thwarting espionage and monitoring foreign influence touch on many dilemmas and tensions, including the tension between democracy and civil rights and security constraints. He further noted that the discussion on the subject is required "in order to ensure that the system does not fall asleep in the absence of a clear signature of enemy/ adversary activity." The Head of the NSC instructed to examine gaps in the field, including in the law.

In 2017, the National Cyber Directorate conducted a staff study on the subject of dealing with cyber influence operations. The staff study noted that foreign influence or information warfare are familiar practices, to which new tools have recently been added in cyberspace that increase the threat, and that the realization of the threat of foreign influence through these tools "can amount to a tangible harm to the independence of a state and the proper conduct of society, including basic democratic procedures, as has been demonstrated, among other things, in recent elections and referendums in the US, the UK (Brexit), France, Italy, and more."

The work of the headquarters noted that the national response is lacking and that there is no entity or entities that consider themselves responsible for dealing with the problem; and that since the threat of foreign influence is not confined to the cyber field but is part of a broader discipline, it is necessary to formulate an interdisciplinary response that involves various bodies. As part of the response, efforts should be made to harness civil society organizations and research institutes, as well as to initiate critical outreach and education activities among the general public.

The headquarters' work detailed difficulties in dealing with the threat, including tension between freedom of expression and individual rights and supervision and intervention; expanding the circle of potential targets of influence, in such a way that viral distribution serves as a force multiplier; difficulty in locating and assessing the damage of the influence; tension between the use of

---

69 In this regard, the Institute for Intelligence Methodology and the Institute for National Security Studies (INSS) published joint collections of articles dedicated to the topic of foreign influence: in April 2019, a collection of articles was published on the topic of "The Campaign for Consciousness, Strategic and Intelligence Aspects"; in 2020, an in-depth study was published on the topic of "The Role of Intelligence in the Face of Foreign Influence on Democratic Processes"; in December 2024, a collection of articles was published on the topic of " Foreign Influence and Intervention as a Strategic and Intelligence Challenge." The collection noted that the purpose of the publication is a systemic analysis of the threat to Israel, which was prominently expressed in the multi-sector war that began on October 7, 2023, which also includes efforts by various actors to weaken the Israeli state and society, among other things by undermining cohesion and strengthening narratives that support the interests of foreign elements, which masquerade as authentic Israeli discourse. Among other things, a foreign influence campaign was presented on social media that supported Hamas during the Iron Sword War.

70 It should be noted that in the context of the elections, the Shin Bet began operating on the issue in 2017. It should also be noted that various bodies monitor social networks in Israel in various contexts. Activity that does not constitute foreign influence was not examined within the framework of this report.

Legitimate in a tool of influence or consciousness for illegitimate use; difficulty in identifying "soft" actions that add up to a cumulative effect.

Following the work of the staff carried out in the Cyber Division and the directive of the Head of the National Security Council from November 2017 on the subject of dealing with foreign influences, the National Security Council held discussions in March and July 2018 on the subject of initiating inter-organizational staff work on the subject of foreign influence, in which the Cyber Division, the Ministry of Justice, and various security bodies participated, among others. The discussions noted that there is broad agreement regarding the seriousness of the potential threat of foreign influence, and that nevertheless, the organization at the national level and in the various bodies is only in the initial stages. In these discussions, the Ministry of Justice emphasized the inherent tension between the need to protect the state, citizens, and public opinion from improper foreign influences and individual freedoms and freedom of information, a tension that characterizes a democratic regime. It was noted that in light of the threat and the challenges to dealing with it, national inter-organizational preparedness is required, and it is appropriate for each of the bodies to act and develop knowledge within its areas of authority and capabilities, while decentralizing areas of responsibility and action on the one hand and a broad national vision and coordination between the bodies on the other. It was noted that decentralizing treatment to various entities provides part of the response to the sensitivity inherent in treating the issue.

It was also noted that the issue would continue to be addressed on several levels simultaneously and on an ongoing basis: formulating a policy at the national level for enforcement and thwarting foreign influence; increasing the collection, preservation of the issue, and the development of a defensive-attacking discourse; monitoring, thwarting, removing, and enforcing objectionable content in Israel; 71 In the IDF, cooperation with research entities, civil society, and technology entities; liaison with the Central Elections Committee, including the preparation of "cases and responses" and preparations for the elections; it was also suggested that consideration be given to establishing an internal coordination forum between the various entities (a kind of internal "organ").

In September 2018, the Ministry of National Defense issued an update on the subject to various bodies (including the Cyber Directorate, security bodies, the Ministry of Justice, and the Ministry of Public Security), in which it detailed several examples from around the world of attempts at foreign influence in the digital space and the actions taken in their regard. The Ministry of National Defense stated in the document that each of the bodies is required to increase the level of awareness of improper foreign influences in the context of election campaigns and in general; and to act in accordance with its areas of authority and roles to define the CIAH, increase monitoring, information sharing, and resistance to foreign influences, in a way that will increase the overall level of resilience from a national perspective.

In 2017, the head of the National Security Council insisted that the State of Israel is a target for foreign influence from both superpowers and adversaries and instructed to examine gaps in the field. At the same time, in the staff work carried out by the Cyber Directorate on the threat posed by foreign influence in the digital space, he suggested that the national response to the issue was lacking and that it was necessary to formulate an interdisciplinary response involving various bodies, while harnessing civil society bodies and research institutes, as well as to initiate critical information and education activities intended for the general public. The staff's work was presented in discussions held at the National Security Council in 2018, and the need to formulate a national policy for enforcing and thwarting foreign influence in the field was emphasized, while coordinating between the bodies. At the same time, an attempt was made to initiate inter-organizational staff work. However, it was raised that after these discussions, the National Assembly did not continue to promote the handling of the issue with the various government agencies, and the work of the inter-organizational headquarters was not advanced (except on t

2. Discussions in the 2022 National Security Council and the 2023 National Security Council

A. In a discussion held in February 2022, headed by the Cyber Command of the National Defense Security Force, with the participation of representatives of security bodies and the cyber system, on the subject of reviewing the threat of influence in the digital space and ways to deal with it, it was noted that an enemy state is investing resources in the field on an increasing scale, in order to

71 Specifying essential information.

to create chaos and deepen the divisions in Israeli society in order to weaken it; that it is active on the vast majority of social platforms, and through them, conflicting and incendiary messages are echoed between different groups or messages whose purpose is to undermine the legitimacy of the government (for example, against coronavirus vaccines, against the government), and that foreign involvement reaches the point of actually organizing demonstrations and protests. It was further noted that activity in the field of influence is foreign hostile activity for all intents and purposes. A representative of the Cyber Directorate noted in the discussion that the regulation regarding dealing with the issue of hostile content has not been resolved and it was recommended to clearly define the areas of authority and responsibility for handling influence activities online. In conclusion of the discussion, it was recommended to examine ways of cooperation between the various organizations to deal with the threat.

In June 2022, the NSC held a discussion on the subject with the Ministry of Intelligence, which also began to deal with the issue of foreign influence. The discussion revealed that the Ministry of Intelligence had identified a gap in the handling of the issue of foreign influence online and was examining ways to understand and assess the threat, as well as technological tools for identifying attempts at foreign influence online. The conclusion of the discussion emphasized both the lack of coordination and synchronization between the various bodies dealing with the issue and the need for coordination between them and for promoting an effective response to the threat.

In July 2022, the National Security Council formulated a document on the topic of "National Handling of the Cyber Dimension - Insights." The purpose of the document is to point out the main gaps in handling [72] and recommendations for issues for consideration and handling by the National Security Council. the cyber dimension at the national level in national security contexts and, as a result, to define an up-to-date list of issues required for examination, monitoring and handling by the National Security Council. In light of which, the issues required for monitoring, monitoring or the criteria detailed in the document will be defined. [73]
Involvement of the NSC in accordance with its powers and role according to law and, as a result, the list of topics recommended for examination and monitoring by the NSC for the years 2022-2023, which constitutes the NSC's two-year work plan in the field of cyber.

· One of the issues that surfaced in this framework concerns hostile foreign influence activity on networks (CNI) (74)
It was noted that social media is a convenient and accessible platform for hostile influence activities. It was also noted that Iran is carrying out influence activities in Israel as part of an overall campaign, and that it is using
On social networks for the purpose of echoing messages whose purpose is to incite between different groups and undermine the legitimacy of the government, to the point of actually organizing demonstrations and protests.

The document also states that this influence activity is focused during an election period, but it is necessary to assess its scope and impact and examine the handling of the threat during routine periods and times of emergency. The document noted that: Many bodies are involved in addressing the threat, but it emerged that additional bodies are working on the issue without coordination, and that this activity requires support and synchronization. The NSC noted that he will continue to lead, together with the relevant bodies, staff work aimed at coordinating activity in the field among all bodies and examining gaps in treatment, if any, to bring recommendations to the political echelon for policy and legislative changes and to formulate recommendations for directing the necessary resources for this purpose.

In discussions held at the National Security Council in 2022 with the participation of a number of parties, including: the Cyber Directorate, security agencies, and the Ministry of Intelligence, and in the National Security Council document intended to point out gaps

---

72 The document stated that it was written with the assistance and coordination of many elements within and outside the National Security Council, and parts of it were coordinated and reviewed with various bodies, as well as with elements within the National Security Council.

73 It was noted that the criteria were examined in light of the National Security Staff Law and the definition of its role and powers in the law, and in light of its designation and central role in shaping and maintaining the national security of the State of Israel. It was noted that this is by virtue of Section 2(a)(4) of the National Security Staff Law 5768-2008, which mandates the National Security Staff to propose to the Prime Minister an agenda and topics for discussion for the Ministerial Committee on National Security, Foreign Affairs and Defense, and by virtue of Section 2(a)(5) of the National Security Staff Law, 5768,2008, which mandates the National Security Staff to be responsible for the work of the inter-organizational and inter-ministerial staff on foreign and security matters, including alternatives, differences and implications, and to present its recommendation to the Prime Minister on policy in these matters.

74

Central to handling the cyber dimension at the national level in national security contexts within the framework of the NSC's duties according to law, the threat of foreign influence in the digital space, the lack of coordination between the various bodies dealing with it, and the need to deepen cooperation in handling the issue have resurfaced. Following this, the NSC noted in the document that it will continue to lead, together with the relevant bodies, staff work aimed at coordinating activity in the field among all bodies; examining gaps in handling, if any; and bringing recommendations to the political echelon for policy and legislative changes, including with regard to allocating the necessary resources for this. However, the audit revealed that

The issue has not been addressed before.

B. In accordance with the National Security Staff Law, 2008, the NSC is required to prepare and submit to the Ministerial Committee for National Security Affairs (hereinafter referred to as the Cabinet), at least once a year, an annual and multi-annual assessment. Annual assessment of the political-security situation . 75 The law adds that assessments of the situation will be submitted to the Prime Minister and discussed in the Cabinet, at least once a year. In the assessment of the national security situation for 2023 formulated by the National Security Council (in December 2022), key recommendations for policy were formulated, including in the field of cyber, including "deepening the handling of monitoring and thwarting foreign influences through social networks."

The National Security Assessment, which was defined by law as one of the key tasks of the National Security Council, is intended to assist decision-makers in shaping policy in the face of existing challenges. The assessment details the overarching goals and political directive; examines the strategic balance of the State of Israel; presents potential policy alternatives, and finally presents an overall concept and individual recommendations for Israeli policy in each of the areas of operation and core issues. It was raised that as of October 2023, the 2023 National Security Assessment, which included key policy recommendations, including in the field of cyberspace, including deepening the handling of monitoring and thwarting foreign influences through social networks, had not been discussed in the Cabinet. The lack of a discussion in the Cabinet on the aforementioned issue entails various risks, including harm to the ability to manage risk strategically and from a national perspective.

2021 - 2024: As stated, the Ministry of Intelligence also dealt with the issue of foreign influence, and within this framework, it initiated and supported a series of studies that dealt with this issue, and in particular, it has worked since 2021 to identify technological tools for monitoring this issue regarding foreign influence in the digital space and foreign influence on social networks. In a meeting held in 2023 between the Prime Minister and the Minister of Intelligence, the areas of responsibility of the Minister of Intelligence and the Ministry of Intelligence were determined, including leading activities on the subject of foreign influence and creating intelligence for this purpose. It should be clarified that the activities of the Ministry of Intelligence focused on accumulating knowledge, creating a methodological infrastructure, and identifying technological tools to deal with the threat, but the ministry was not authorized to deal with the operational side of dealing with the issue. In 2023, the ministry emphasized that it sees the issue of foreign influence as a threat to Israel's national security and a significant strategic challenge, and that one of the most important components in the ability of foreign countries to influence the State of Israel is influence operations on social media, and even emphasized the need for future cross-sectoral cooperation between the various parties involved in the matter, in order to better deal with

3. ACTIVITIES OF THE MINISTRY OF INTELLIGENCE, [76]

The threat.

It was noted that the ministry recognized that Israel is [77] The main points of the Ministry of Intelligence's work plan for 2023 facing attempts at foreign influence, and that it will work to promote intelligence monitoring of foreign influence.

---

[75] It should be noted that the June 2025 amendment to the law requires the Ministry of National Security to prepare and submit to the Cabinet, at least once a year, an annual assessment of the political-security situation, which was approved according to the National Security Strategy Law, 5785, 2025, as well as to prepare situation assessments regarding matters related to them, as needed and with the approval of the Prime Minister. This includes the Institute for Intelligence Methodology and the Institute for National Security Studies (INSS), joint collections of articles: " The Role of Intelligence in the Face of Foreign Influence on Democratic Processes" (2020); "Intelligence in Practice and Law - Foreign Influence and Intervention as a Strategic and Intelligence Challenge" (2024) (the contract was transferred to the Ministry of Innovation, Science and Technology after the closure of the Ministry of Intelligence).

[76] Book of Main Work Plans for 2023 - Government Ministries and Units of Authority, 2023.

[77]

and foreign interference in relation to the State of Israel and to formulate a national strategic plan to raise awareness and promote operational activity on the subject of foreign influence. Also, in 2023, the Ministry of Intelligence promoted a dialogue with a security body on the subject of foreign influence in the digital space.

In a government decision of March 2024, the Ministry of Intelligence was closed, while it was decided to transfer the area of operation of the Ministry of Intelligence, including the National Intelligence Directorate, which deals with foreign influence. In April 2024, another government decision was made in which the area of operation of the National[78] Within its framework, the Prime Minister's Office Intelligence Directorate was transferred from the Prime Minister's Office to the Ministry of Innovation. The decision stated that the five manpower standards that were used by the Prime Minister's Office for the benefit of the said area of operation would be transferred to the Ministry of Innovation, as well as all previous obligations of the Intelligence Directorate in the Prime Minister's Office.

In December 2024, the Ministry of Innovation informed the State Comptroller's Office that the issue of foreign influence on social media was not related to its activities. In February 2025, the person who served as the head of the National Intelligence Administration at the Ministry of Intelligence stated that the position of head of the foreign influence department had not been filled for several months at the Ministry of Intelligence and the tender for its replacement had been terminated due to the closure of the ministry, and that the issue of foreign influence had not been transferred to the Ministry of Innovation. He added that in parallel with the processes of closing the ministry, the Cyber Directorate announced that it was beginning to deal with the issue of foreign influence in the digital space, and knowledge was transferred between the two entities. It should be noted that even after the closure of the Ministry of Intelligence and the transfer of the Intelligence Administration to the Ministry of Innovation, the professional entities that dealt with the issue continued to promote various projects that had already been invested in. 79 of them resources.

In 2023, the Prime Minister determined in a meeting with the then Minister of Intelligence that the issue of foreign influence and the creation of intelligence for this purpose would fall under the purview of the Ministry of Intelligence. The Ministry emphasized that one of the most important components of the ability of foreign countries to influence the State of Israel is influence operations on social media, and also emphasized the need for inter-sectoral cooperation t with the threat in a better way and on the need to promote monitoring of foreign influence on the Internet. It was raised that the position of Head of Foreign Influence Department was not filled for several months in the Ministry of Intelligence, and the tender for its appointment was stopped due to the closure of the ministry in 2024. It was also raised that although the National Intelligence Administration, under whose responsibility the issue of foreign influence was, was transferred to the Ministry of Innovation, the issue of foreign influence was not transferred, without a responsible person being designated to har

3 2 0 2 - , 4. Cyberattacks in Brazil

024 :2 The Cyber Directorate documents indicate that with the outbreak of the Iron Sword War in October 2023, alongside the intensification of attacks against organizations in Israeli cyberspace, the Israeli public was targeted for influence efforts and the spread of disinformation in the digital space, among other things to widen the existing social divide and undermine social stability. The Directorate stated that it believes that these efforts have not been adequately addressed, and that they are a strategic tool used by Israel's enemies. A July 2024 document from the Directorate detailed a series of gaps in dealing with the threat.

The IDF has a plan of action: In light of the gaps raised by the Cyber Directorate, in August 2024 the head of the Cyber Directorate presented the threat to the Prime Minister and noted that attempts to influence in the digital space could undermine public trust in the veracity of information in official systems and institutions; sow division - harming social and national cohesion and fueling conflicts; influencing public opinion and public positions; strengthening extremist positions and groups. The head of the Directorate requested the approval of

78 Government Resolution 1521, "Transfer of area of operation, abolition of the Ministry of Intelligence, change in the division of roles between ministers and amendment of government resolutions" (17.3.24); Government Resolution 1678, "Transfer of area of operation from the Prime Minister's Office to the Ministry of Innovation, Science and Technology" (7.4.24).

79 Among other things, the Ministry completed joint studies with MLAM on the topics of "Foreign influence and intervention - conceptualizing the terms" and "Weapons of mass disruption: social networks, messages and manipulating public sentiment" (January 2024).

Prime Minister to lead staff work that will focus on protecting against coordinated influence attempts in the digital space
Which are carried out with foreign involvement.

The Prime Minister instructed the head of the cyber division to promote and formulate a proposal for organizing, including requirements for allocating resources, and to bring it to his approval, while emphasizing "the risks in this occupation in relation to the possibility of achieving 'takeover' of such a discourse or representation," and therefore noted that "it is necessary to manage the organization "Carefully and wisely."

In September 2024, the Head of the Cyber Directorate submitted to the Prime Minister's Military Secretary a proposal for an inter-organizational action plan for 2025 to deal with foreign influence in the digital space and requested progress as soon as possible (hereinafter - the Action Plan). The proposed action plan included actions to deal with the threat on three levels:

Figure 8: **Components of the action plan to deal with the threat of foreign influence in the digital space**

Source: National Cyber Directorate, processed by the State Comptroller's Office.

The action plan also emphasized the need to institutionalize three state coordination mechanisms: (a) an intelligence and operations desk - which will centralize the intelligence picture from all agencies, and integrate them for the purpose of assessing the situation - which will coordinate the interagency activity and the formulation and execution of the operational response; (b) an information and awareness desk for increasing public resilience through education and information efforts during routine times; (c) a "soft" information policy desk - which will coordinate government activity for examining and promoting regulation, including the manner of activity vis-à-vis digital platforms.

It was noted that the action plan will provide an initial response in the immediate term, each body within the framework of its existing powers, and in the medium-long term, an orderly and systematic state response will be provided. It was further noted that its implementation will make it possible to significantly reduce the scope of foreign influence content appearing on the various platforms, while implementing a technological and operational process to locate and remove it, and that at the same time, information and advocacy activities will be carried out to increase public resilience in order to reduce the effectiveness of influence campaigns.

The plan detailed the main milestones for 2025, along with the resources required for the various bodies for this purpose for the years 2024-2025.

In a discussion held by the Cyber Directorate in October 2024, the head of the Directorate emphasized that the threat of consciousness is a significant threat that must be dealt with as part of the Directorate's vision for a reliable, available and secure digital space, and noted that as of that date, there had been no organized national effort. He added that in order to deal with the issue, a holistic view is required, which is not only security-based, while involving civil society. Head

80 With the participation of representatives of these bodies: the National Information System, the Ministry of Education, the Ministry of Defense, the Home Front Command, the police spokespeople, the IDF spokesman.

81 With the participation of representatives of these bodies: the Ministry of Justice, including the Cyber Department in the State Attorney's Office, and the Ministry of Communications.

The system instructed to proceed as approved in principle by the Prime Minister, and noted that in order to deepen the treatment
This threat will require dedicated resources.

In June 2025, the State Comptroller's Office contacted the Prime Minister's Office and asked whether the Prime Minister or a representative on his behalf had sent the Cyber Directorate a reference to the action plan proposed by the Directorate in September 2024. On 15.7.25, the Prime Minister's Chief of Staff stated that an inspection that was carried out revealed that the plan had not been submitted to the Prime Minister and had not been brought to his attention, and that at that time the plan had been submitted to the National Security Council for the purpose of examining it and providing a reference to
the Head of the Cyber Directorate.

After the outbreak of the Iron Sword War, the Cyber Directorate stated in July 2024 that the Israeli public is a target for influence efforts and the spread of disinformation in the digital space, and that this is a strategic tool used by Israel's enemies. The Directorate stated that it believes that these efforts have not been adequately addressed and detailed a series of gaps in dealing with the threat.

It therefore appears that although in August 2024 the head of the Cyber Directorate presented to the Prime Minister the threat of foreign influence in the digital space and its implications, and, in accordance with his instructions in September 2024, submitted to him a proposal for an action plan for a national inter-ministerial deal with the issue, about a year later, as of mid-July 2025, the proposed plan had not been examined by the Prime Minister or anyone on his behalf. It was only following a request from the State Comptroller's Office to the Prime Minister's Office that the plan was forwarded to the National Security Council in July 2025 for its examination.

The audit also revealed that in the absence of approval from the Prime Minister for the plan and in the absence of approval for the budget required for its implementation, the Cyber Directorate promoted activities mainly in the areas of education and outreach to deal with the threat, alongside initial activities to examine technological options for expanding monitoring capabilities, in collaboration with additional entities (see below). Key gaps that the Cyber Directorate had covered remained intact.

As mentioned, in 2017, the Cyber Directorate carried out staff work on the issue of dealing with influence operations in cyberspace. In February 2025, the Cyber Directorate informed the State Comptroller's Office that until the outbreak of the Iron Swords War, it had not dealt with the issue of foreign influence in the digital space. Following the significant increase in influence activity against Israel by foreign entities and the connection to cyber defense activity, the Directorate worked to coordinate comprehensive inter-ministerial staff work, within the framework of which, in cooperation with the relevant entities, an orderly process of characterizing the threat, measuring the arena, and defining the attribution threat will be carried out. The Directorate added that after examining the matter holistically, it will be possible to define the options for action and the entities responsible for carrying them out.

In April 2025, the National Security Council informed the State Comptroller's Office that it dealt with the issue with the understanding that the threat of influence in the digital space is increasing, and that "promoting national preparedness and resilience against foreign influence operations" was included in the work plan of the Cyber Division in the National Security Council for the years 2025-2026. The National Security Council also stated that since the Prime Minister directed the National Cyber Directorate to promote an ecosystem and formulate a proposal for national organization to deal with the threat of foreign influence, the National Security Council decided not to deal with the issue. The National Security Council added that it would continue to update and monitor the activities of the Cyber Directorate and would assist in this in the future if the need arises. The National Security Council added that it believes that at the national level, additional resources should be provided to the Cyber Directorate in order to deal with the issue and its challenges in terms of national security. It also believes that the cooperation of the various relevant bodies with the Cyber Directorate should be improved.

In August 2025, the Cyber Directorate updated the State Comptroller's Office that upon the head of the Cyber Directorate taking office in May 2025, he examined the issue and decided that, in light of the range of tasks facing the Directorate and in accordance with its powers, the Directorate would focus its efforts with regard to foreign influence only in cases where it stems from cyber attacks that are leveraged for the benefit of achieving influence, such as sending text messages on a large scale to the public in order to achieve a public awareness achievement. It should be noted that in the past, the Cyber Directorate also emphasized

And not a job [82] So the mandate given to it is to protect computer and communication systems from cyber attacks by regulating the content aspects of activity in cyberspace, if these do not arise from cyber attacks. [83]

From the above, it appears that in light of the entry of the Cyber Division into the field, the National Intelligence Service decided not to advance the handling of the issue as planned within the framework of its work plan. This is while in practice, in the absence of approval of the action plan by the Prime Minister and provision of budget for its implementation, the Division promoted only specific actions to deal with the threat and address the gaps that were raised on the issue. Furthermore, in August 2025, as stated, the Cyber Division updated the State Comptroller's Office that upon the head of the Cyber Division taking office in May 2025, he examined the issue and decided that in light of the full range of tasks facing the Division and in accordance with his authorities, he would focus his efforts with regard to foreign influence only in cases where it stems from cyber attacks that are leveraged for the benefit of achieving influence. It therefore follows that as of August 2025, the National Intelligence Service and the Cyber Division stopped dealing with the issue.

In February and March 2026, the State Comptroller's Office informed the State Comptroller's Office that in the near future (an exact date has not yet been set), a discussion headed by the Prime Minister with all relevant parties is planned, the purpose of which is, among other things, to examine how the Israeli government is expected to deal with the threats facing it on the issue of delegitimization, including foreign influence in the digital space. The State Comptroller's Office also stated that, in his opinion, there is currently no responsible party to lead the fight against the threat of foreign influence, including in the digital space, and therefore it is appropriate to promote a government decision to establish a dedicated headquarters body with a dedicated budget, under the Prime Minister's Office. The dedicated body will lead the examination and will integrate and synchronize the handling of the issue of foreign influence between all relevant ministries and bodies. The State Comptroller added that he will be prepared to assist the aforementioned dedicated body according to the need and within its areas of expertise. His responsibilities and powers.

Mafat informed the State Comptroller's Office in March 2026 that in various works it has carried out over the past two years, the absence of a comprehensive national factor was identified as a significant gap in dealing with the issue of foreign influence. Mafat added that the activity of foreign influence against the State of Israel also includes an influence on public opinion and decision-makers around the world, shaping their consciousness and directly affecting the activities of all state agencies, from security activities to political cooperation, trade, research and culture. In light of the above, Mafat believes that a comprehensive, inter-ministerial systemic view is required in addressing the issue in its broad context.

The (former) head of the National Intelligence Directorate in the Ministry of Intelligence, within whose framework foreign influence in the digital space is dealt with, stated in February 2026 that he agrees with the findings raised in the report regarding the existence of a gap in the government's handling of this threat and the need for a coordinated policy to deal with it.

In this context, it should be noted that the National Emergency Authority (NEA) informed the State Comptroller's Office in January and February 2026 that it is committed to the continued functional continuity of the economy during an emergency, and that there is a possibility that foreign influence in the digital space will disrupt the continued supply of services and products to the population. In light of this, the prevailing opinion in NEA is that the issue of dealing with foreign influence in the digital space should be included in the State of Israel's national threat map. It was also noted that it recommends that the issue be addressed by a security factor (comparative advantage and enabling normative infrastructure), including research and prevention mechanisms. NEA added that it will take part in national organizing in elements that could pose a challenge and threat to national functional continuity, and noted that the issue of dealing with foreign influence in the digital space is very important, and its intensity will increase in the coming years.

82 It was noted that a cyber attack in this regard is a hacking or intrusion using information technology (or attempts to do so) to gain unauthorized access to information systems or computerized information, as well as their disruption or attempted disruption remotely through the use of information technology.

83 The Ministry of Justice also noted in a discussion on the subject held in 2018 that if the foreign influence in the cyber field concerns hostile content, there is a prohibition on the cyber department from engaging in the matter, in accordance with its definition and purpose.

ÿ

Similar to the identification of the threat worldwide, starting in 2017, several elements in Israel, including security bodies, the National Intelligence Service, the Cyber Directorate, the Ministry of Intelligence, as well as research entities and civil society entities, have focused on the threat posed by foreign influence in the digital space and the intensification of attempts at foreign influence. Starting in 2020, certain actions are being taken to detect and monitor attempts at foreign influence in th

Over the years, the need for holistic, inter-organizational coordination to deal with the threat of foreign influence in the digital space has been raised time and again, and various factors have led several initiatives to launch it:

Figure 9: **Failure to promote an inter-organizational response to deal with the threat of foreign influence in the digital space in the years 2017 - 2026**

* Except in cases where these are cyber attacks that are leveraged to achieve influence.

It should be noted that the actions regarding elections began even earlier (see below in the chapter that relates to the issue of elections).

The sequence of events indicates a recurring pattern of putting the threat on the agenda, and taking initiatives to deal with it inter-organizationally - however, these initiatives were abandoned and did not get on a track of actual implementation. As of March 2026, about nine years after the threat of foreign influence in the digital space was identified, there are significant gaps in dealing with it at the national level - there is no national policy on the subject and no government entity leading the inter-organizational dealing with the threat. In the absence of a directive and systematic direction, there is no fit between the threat and its intensification and the government response given to it, and the government's handling of this threat is deficient.

Leaving the gaps raised in this report unanswered will leave the Israeli public exposed to foreign influence in the digital space without an adequate response.

The role of the National Security Council is, among other[85] According to the National Security Headquarters Law, 5768-2008 things, to propose to the Prime Minister an agenda and topics for discussion on foreign and security matters. In light of the increasing threat in the field of foreign influence, including in the digital space, given that for years no regular policy has been formulated regarding leading the issue at the national level, and since the National Security Council itself believes that a government decision is required to establish a dedicated headquarters body to deal with the threat of foreign influence - it is recommended that the National Security Council propose to the Prime Minister an outline for handling the issue that will serve as the infrastructure for receiving a government decision on the issue, and within this framework, it will consider the policy, resources, and res

Assessing damage from foreign influence

In the research literature, various tools have been proposed for assessing the effectiveness of exposure to foreign influence and exposure to disinformation (which, as mentioned, is one of the tools used to carry out foreign influence operations). 86

A complex subject, partly due to the need for accessibility to data, and due to the difficulty in isolating the impact of exposure to certain information on the individual's attitudes or behavior 87

In a discussion held at the National Security Council in 2022, the threat of foreign influence and its objectives were reviewed, and it was noted that there is difficulty in assessing the extent of damage caused by foreign influence activity in Israel. The National Security Council insisted that influence activity against Israel entails great potential damage in light of the increasing concern of foreign countries on the subject. However, it is difficult to make a quantitative assessment of the extent of damage caused by influence activity and its scope. In light of this, it was noted that there is a need to examine ways to assess the damage and its impact. As a result of assessing the direct and indirect damages of hostile influence activity in Israel, it will be possible to assess whether the inputs devoted to addressing the threat are sufficient and appropriate to the scope of the phenomenon and the severity of the threat.

In 2024, as stated, the Cyber Directorate addressed the existing gaps in the subject, including the inherent difficulty in assessing the threat and measuring the impact and effectiveness of its treatment. In February 2025, the Cyber Directorate informed the State Comptroller's Office that research on the subject of assessing the damage from foreign influence is still in its infancy, and there is still no accepted assessment model at the state or academic level. The Directorate added that from the international media it is possible to learn about events around the world in which foreign influence operators attempted to influence state activity and that it identified the involvement of foreign elements seeking to act to deepen the divisions in Israeli society.

In February 2025, one of the security officials told the State Comptroller's Office that, given the polarizing and explosive discourse currently taking place online, he estimated that the damage that could be caused by foreign influence online was low relative to the potential, except during an election period when the potential for damage is high. Moreover, from an analysis by one of the influence operators

---

85 See Section 2(a)(4) of the Law.

86 Influence-to-action Model Development: A Tool to Assess the Impact of Foreign Influence Operation, 2021 Various studies focus on alternative metrics,

87 such as exposure to content and engagement in discourse through clicks and shares.

It emerged that it is difficult to indicate the effectiveness of the influence activity and its cognitive contribution to inciting the events. It was noted that in the long term, there is an aspiration on the part of the adversary to exploit the accessibility created on the basis of the platforms to strengthen operational infrastructures in Israel in order to advance its objectives.

In recent years, attempts at foreign influence in the digital space against Israel have intensified, and technological progress has also been made that allows for the improvement of the quality, scope, and distribution of campaigns.

: On the cognitive level - instilling a certain perception[88] Influence operations can have goals at three levels: of reality and certain events; On the emotional level - to arouse and intensify emotions such as anger, fear, and anxiety; On the behavioral level - motivating the target audience to act in a certain way - a threat that, as the documents show, has already been realized. Therefore, it is appropriate to examine the issue of harm also with regard to these three levels.

In 2022, the NSC emphasized the difficulty in conducting a quantitative assessment of the extent and scope of the damage caused by the impact activity and the need to examine ways to assess the damage and its impact.

It should be noted that even if there is still no accepted assessment model at the state or academic level for assessing the damage, given the events in Israel and around the world, this is a threat that cannot be ignored. Assessing the threat will make it possible to assess the actual damage caused and the potential for damage, as well as to identify target audiences where efforts should be focused to increase resilience against foreign influence.

As stated, as of March 2026, there is no designated body dealing with the issue of foreign influence, and the National Security Council believes that it is appropriate to advance a government decision that will establish a designated headquarters body to deal with the threat of foreign influence, including in the digital space. It is recommended that, in the context of thinking about establishing the designated body, consideration be given to the need to formulate indicators to assess the threat in

Furthermore, it should be noted that in June 2025, the National Security Strategy Law, 5775, was passed. The law stipulates that upon the establishment of a new government, the NSC will formulate the proposed state-security strategy of the State of Israel to promote the political and security interests in order to strengthen the national resilience of the State of Israel, which will include the threats, challenges and their ranking, as well as the means and ways to deal with them, including in the cyber information space. The law stipulates that the proposed strategy will be made in consultation with relevant bodies such as the Ministry of Defense, the Ministry of Foreign Affairs, the Ministry of National Security, security bodies and other government ministries as necessary, and that it will be approved by the government.[89] It is recommended that, within the framework of formulating the national security strategy, the NSC also examine the threat of foreign influence in all its aspects, including the threat of foreign influence in the digital space, and that the ways to deal with it will be detailed.

As part of the examination, it is recommended to examine the impact of influence operations in both the short and long term. It is also recommended to consider that even if the impact of a foreign influence campaign appears limited in the short term, such campaigns may have a broader impact in the long term. Narratives promoted by foreign influence operations may be present in the digital space for a long time and may reappear in new forms, gradually permeating public discourse and influencing perceptions among the public.

88 Gabi Siboni and Kobi Michael, **Influence Operations: The Complementary Tool for Combating Terrorism Has Not Yet Been Put into Use, Center for Greater Israel Strategy** (2024).

89 Or by the Ministerial Committee for National Security Affairs, if the government has delegated the authority to it.

Monitoring foreign influence in the digital space

The digital space in general and social networks in particular are a breeding ground for activity that can harm the state and the public in various ways. To deal with these threats, various bodies are working to monitor the digital space for the purpose of protecting the public, for example by detecting attempts to recruit, deceive, activate, and incite terrorism using various tools.

It should be noted that monitoring foreign influence in the digital space involves significant challenges, relating to the protection of freedom of expression; to the enormous scope of content distributed daily on the Internet and its characteristics, including anonymity and sometimes the difficulty of attributing a particular expression to a foreign entity. While attempts to incite terrorism or violence, for example, are inherently illegal, and the very expression of the subject is prohibited, attempts at foreign influence can include the use of legitimate content for an illegitimate purpose, such as creating anxiety and fear, widening divisions in society, and attempting to influence attitudes. For example, a call to participate in a legal demonstration is legitimate when it originates from an internal factor but is illegitimate when it originates from a foreign factor that presents itself as an internal factor in order to deepen the division in society. This difficulty is exacerbated because in many cases, attempts at influence mix with internal discourse and echo each other's mes

Below are details about the monitoring operations:

Shin Bet: Shin Bet began working on dealing with foreign influence in the context of the Knesset elections in September 2017, and not in the context of the elections in mid-2020. According to Shin Bet documents, the influence activity carried out by foreign countries and powers occurs, among other things, in the online environment, due to the lack of physical accessibility and the advantages that exist on the Internet, such as anonymity, virality, ease of creation and copying of messages and ideas.

Civil **society:** Alongside the monitoring activities carried out by the Shin Bet, elements in civil society also Engage in activities to identify foreign influence campaigns (for more information about civil society activities, see below).

PLATFORMS AND CORPORATE MEDIA: To complete the picture, it should be noted that some platforms prohibit "inauthentic coordinated activity" or activity carried out through fake accounts that aim to influence public discourse, and within this framework, attempts at foreign influence are also monitored. In periodic reports published by some platforms, they refer to the actions they take in this context. It should be noted that the scope of monitoring and removal of content varies from platform to platform, depending on its considerations.[91]

For example, one company prohibits coordinated activity using fake accounts, which aim to influence public discourse for a strategic purpose. The company's policy focuses on user behavior and not on the content of the posts or the identity of the users (whether foreign or local). In particular, the policy prohibits misleading conduct by foreign entities: foreign entities that use its assets in an inauthentic manner to falsely represent a voice that is perceived to be local, in order to mislead users about the identity, purpose, or source of the . According to documents published by the company, it conducts automatic and manual monitoring to locate the entity they represent. 92 .of coordinated inauthentic behavior and removes accounts and pages found to be such 93

---

90 For example, the organization "Fake Reporter" is engaged in identifying foreign interference campaigns on social networks. For more information on this topic, see Assaf Wiener, "National Preparation Against Foreign Influence and Intervention Through Social Networks: Global Findings and an Israeli Situational Picture," **Intelligence - Halacha and Practice** 10 (2024), pp. 243-257, commissioned by the Ministry of Intelligence.

91 /https://transparency.meta.com/en-gb/policies/community-standards/inauthentic-behavior

92 Meta, Adversarial Threat Report, May 2025

93

Gaps and challenges in the field of monitoring

Over the years, various parties have repeatedly raised the need to improve digital space monitoring capabilities in order to detect attempts at foreign influence, and attempts have been made to develop technological tools and create collaborations for this purpose.

Shin Bet: Shin Bet documents revealed various difficulties in extensive monitoring of the Israeli digital space and challenges in attributing attempts at influence to a foreign entity, due to the network's characteristics that allow anonymity for users.

MINISTRY OF INTELLIGENCE: Along with the Shin Bet, the Ministry of Intelligence also tried to promote monitoring of attempts at foreign influence in the digital space: In addition to its support for several studies on the subject of influence, the ministry worked from 2021 to 2024 to locate technological tools for collecting online intelligence on the subject of foreign influence and analyzing it. Initially, an attempt was made to build a tool independently, but it became clear that from a technological point of view and in terms of the required knowledge, it was not possible to promote the treatment of the issue independently and it was decided to turn to companies with knowledge and expertise in the field. During these years, contracts were examined with about ten companies and options for carrying out various collaborations were also examined.

Following a study commissioned by the Ministry of Intelligence on the subject, the ministry stated in 2023 that it intended to establish a monitoring center for attempts at foreign interference in social networks in Israel, which would operate on a permanent basis, combining experts in the subject and advanced technologies with research institutes, civil society organizations, and relevant companies. As mentioned, in March 2024, it was decided to abolish the Ministry of Intelligence without appointing a responsible entity to handle the matter (see more on this matter above in the chapter on “Identifying the Threat of Foreign Influence in the Digital Space” 94). In Israel, gaps and deficiencies in providing an inter-organizational government response to deal with it.

CYBER DEPARTMENT: The Cyber Directorate noted that there are gaps in the detection and monitoring of attempts at foreign influence in the digital space. In July 2024, the Cyber Directorate stated that Israel does not have a comprehensive and continuous up-to-date national picture of foreign influence efforts on the Israeli public.

In light of the technological gaps raised by the Cyber Division in the field of monitoring and further to the proposed action plan it formulated after the outbreak of the Iron Sword War, it promoted inter-organizational coordination, within the framework of which a technological pilot was carried out to improve monitoring capabilities of foreign influence on the network. In October 2024, a meeting was held with the participation of representatives of the relevant bodies and it was agreed to embark on a technological pilot. Following this, in December 2024, cooperation on R&D issues for protection from covert foreign influence was agreed upon and a document of understanding and principles on the subject was formulated. The document noted that an initial examination indicates that deep-cover foreign "users" are operating in the Israeli cyberspace, some with a wide distribution of thousands of followers, who are systematically operating for the purposes of intimidation, demoralization, undermining public trust, sowing chaos, deepening polarization, misleading and biasing positions. Against this background, the Cyber Directorate initiated an inter-organizational organization with the participation of various entities to examine the national response to protection from covert foreign influence.

The document also stated regarding this pilot that the Head of the Cyber Division will hold an inter-ministerial steering committee headed by him, with the participation of representatives from various bodies, to examine the progress of the project and the manner in which resources are allocated and utilized, and that during 2025 the Head of the Cyber Division will make a decision on the continued involvement of the Cyber Division and the required headquarters work.

In February 2025, the Cyber Directorate informed the State Comptroller's Office that, as of this date, the activity within the pilot is in the R&D stages, and within the framework of which suspicions have been raised regarding foreign campaigns operating in the State of Israel.

94 Government Resolution 1521, "Transfer of area of operation, abolition of the Ministry of Intelligence, change in the division of duties between ministers and amendment of government resolutions" (17.3.24); Government Resolution 1678 "Transfer of area of operation from the Prime Minister's Office to the Ministry of Innovation, Science and Technology" (7.4.24).

In August 2025, the Cyber Directorate informed the State Comptroller's Office that the incoming head of the Directorate had determined that, given the Directorate's powers, it would focus its efforts regarding foreign influence in the digital space only in cases where the foreign influence stems from cyber attacks. The Cyber Directorate noted that it had informed its partners in the pilot regarding the aforementioned focus.

Mafat informed the State Comptroller's Office in August 2025 that it identified the need for protection against foreign influence in the digital space in 2016, and that in the years that followed, the said need intensified. The work plan for 2020 included the issue as a focus for R&D activity.

Mafat added that, in his understanding, the main gap that exists on the issue of foreign influence whose purpose is to harm national resilience or create division and deepen rifts in society is that there is no operator for whom this task has been clearly defined (except during an election period), and the issue lies in headquarters work, thinking, and planning for joint organization by various bodies.

The following was raised in the review:

1. The Shin Bet detects and monitors attempts at foreign influence on the Internet. However, as of February 2025, It faces certain challenges in the field of monitoring and prevention.

The Shin Bet informed the State Comptroller's Office in July 2025 that in the past year, internal changes were made in the area of force building in the face of foreign influence, and as a result, several actions were taken, including conducting a pilot, within the framework of which, among other things, emphasis was placed on providing a response to the widest possible variety of social networks. It also noted that it had made a significant technological leap in the matter.

The Shin Bet's response indicates that although as of July 2025, some of its difficulties and challenges in the field of monitoring and thwarting foreign influence operations have been addressed, certain difficulties and challenges still remain as a gap and an examination is underway regarding how to deal with them.

2. In light of the gaps raised by the Cyber Directorate in the field of monitoring and further to the proposed action plan it formulated, the Directorate promoted inter-organizational coordination, within the framework of which a technological pilot was carried out regarding improving the monitoring capabilities of foreign influence on the Internet, with the participation of various parties. As of July 2025, the pilot products were under review, and the Cyber Directorate decided not to engage in the subject any further.

3. The action plan proposed by the Cyber Directorate in September 2024 detailed the resources required for its implementation in 2025, including the budget required for research and technological strengthening. As of July 2025, the plan submitted to the Prime Minister for consideration had not yet been examined, and the resources required for its implementation had not been allocated.

Due to the challenges and difficulties in detecting and monitoring attempts at foreign influence online, the picture of the situation regarding foreign influence efforts in the digital space is lacking and there is a certain difficulty in correctly assessing the scope of the phenomenon.

It is recommended that the Shin Bet continue its efforts to improve the detection of attempts at foreign influence on the Internet, including as part of the pilot. It is also recommended that the Shin Bet give its opinion on additional directions for action that have been raised regarding improving monitoring capabilities.

In January 2026, the Shin Bet informed the State Comptroller's Office that it had begun carrying out various actions on the matter.

In March 2026, Mafat informed the State Comptroller's Office that this is a developing field, and therefore constant and ongoing research and development efforts will be required to develop building blocks and maintain capabilities to deal with

Foreign influence activity. MAFAT added that effectively dealing with the issue will require significant investment. He further added that monitoring and warning tools are not sufficient in themselves and that a holistic response to influence efforts will be required, including technological tools for dealing with, thwarting influence, and even advocacy. In addition, MAFAT noted that given the large number of national bodies dealing with foreign influence efforts, it sees the importance of pooling resources to build a common technological infrastructure for all parties involved in this context, and noted that despite the lack of a comprehensive national body, it is working on the issue.

Civil society's contribution to monitoring foreign influence, research, and strengthening digital literacy

In efforts to deal with foreign influence [95] Over the years, the need to integrate civil society into the digital space has resurfaced. For example, in 2017, the Cyber Directorate noted that efforts should be made to harness civil society bodies and research institutes to deal with the issue, and in a subsequent discussion at the National Defense Council, it was noted that for this purpose, it was necessary to cooperate, among other things, with civil society and research entities. In 2024, the Cyber Directorate again noted that in order to deal with the issue, a holistic view is required, which is not only security-based, while involving civil society.

Civil society and research bodies are dealing with the issue from various aspects. For example, research bodies have engaged in many studies in recent years on the subject of foreign influence, including in the digital space. Some of the studies were conducted with government support. Alongside this, civil society elements are working to increase resilience against foreign influence and disinformation. In this regard, a joint project has been launched by the Israel Democracy Institute, the Internet Association, and the Mofet Institute that deals with media literacy, including identifying deception and misinformation. [97]

Another area of activity in which civil society actors are engaged concerns monitoring: Meetings held by the State Comptroller's Office with civil society actors involved in monitoring foreign influence campaigns indicate that it is difficult to identify with certainty, using the tools at their disposal, that a foreign entity is indeed behind the influence attempts they have detected. One of the means they use to identify foreign influence is various indications that it is a foreign entity, such as language disruptions, different time zones, and recurring patterns that they have identified from other cases. It also emerged from the aforementioned meetings that sometimes information about campaigns suspected of being attempts at foreign influence is brought to the attention of the public, and sometimes it is brought to the attention of the relevant entity for further processing - through unregulated reporting channels.

The Shin Bet informed the State Comptroller's Office that part of its activity to detect foreign influence activities online also includes examining inquiries from citizens and civil society organizations regarding suspicions of foreign influence activities. Shin Bet documents indicate that the activities of these entities helped, for example, in exposing a set of Twitter profiles operated by a foreign entity during the elections for the twenty-fifth Knesset. The Shin Bet noted that the interface with that entity in civil society, which it claims has produced valuable products for it, should be maintained.

It was raised that although civil society actors monitor attempts at foreign influence and even bring attempts they have detected to the public's attention, and benefit is derived from their actions, there is no mechanism or official body that civil society actors can contact to report suspicions of these attempts and to forward relevant materials to them.

---

[95] This report refers to the entire range of non-governmental entities that contribute to dealing with the issue. For example, the Institute for Intelligence Methodology (INSS) and the Institute for Security Studies (ISS) have published collections of articles.

[96] Joint publications dedicated to the topic of foreign influence: In April 2019, a collection of articles was published on the topic of "The Campaign for Consciousness, Strategic and Intelligence Aspects"; in 2020, an in-depth study was published on the topic of "The Role of Intelligence in the Face of Foreign Influence on Democratic Processes"; in December 2024, a collection of articles was published (in collaboration with the Ministry of Intelligence and Malam) on the topic of "Foreign Influence and Intervention as a Strategic and Intelligence Challenge."

[97] Fakeornot.org.il

The Shin Bet informed the State Comptroller's Office in January 2026 that it recommended that the communication channel not be operated by it, but by another security agency.

Over the years, the importance of integrating civil society in the holistic fight against foreign influence in the digital space has re-emerged.98 Since the Shin Bet detects and monitors attempts at foreign influence online, and since there are only a few elements in civil society involved in monitoring suspicions of these attempts, it is recommended that it consider establishing a communication channel (directly or through another government entity) that would serve as an official and regulated address for transmitting reports on the subject.

It should be noted in this context that in March 2026, Mafat informed the State Comptroller's Office that in order to reduce the potential harm to privacy, it is proposed to examine the regulation of the involvement of civil society entities in monitoring public discourse in Israel, and their empowerment with appropriate technological tools.

It should be noted that the Cyber Directorate operates a reporting center (telephone or online) that allows reporting of a cyber incident in order to receive an initial response. The Directorate's website states that cases such as hacking into social networks, phishing and phishing messages, ransomware attacks, and spoof pages can be reported. The State Comptroller's Office contacted the Cyber Directorate and requested details about reports concerning attempted foreign influence. In September 2025, the Cyber Directorate stated that in 2025, a number of reports were forwarded to it that it classified as "foreign influence." The Directorate added that in cases where there is evidence that foreign influence is involved, the information is forwarded to the Cyber Prosecutor's Office to examine the possibility of requesting removal of the publication, and, as necessary, is also forwarded to the relevant security agencies. A review of the list forwarded by the Cyber Directorate revealed that it includes various reports that do not necessarily constitute foreign influence as defined in this report.

Foreign influence campaigns are directed at the public, and their distribution extends across all social networks, and therefore elements in the public can assist in locating and identifying campaigns. Although the Cyber Directorate has received reports from the public regarding foreign influence in the digital space, it informed the State Comptroller's Office in August 2025 that it had decided to focus its work on the issue of foreign influence only in cases where it stems from cyber attacks. As a result, a situation has been created in which there is a lack of clarity regarding the entity to which the public can turn to report concerns regarding attempts at foreign influence in the digital space.

In light of the recommendation that the National Security Council propose to the Prime Minister an outline for leading the handling of the issue at the national level, which will also serve as a foundation for receiving a government decision on the issue, the aforementioned decision may lay the foundation for carrying out staff work in additional aspects, including a response to

Dealing with foreign influence in the digital space - content removal

After detecting foreign influence activities, one of the steps is to forward a reasoned request to the Cyber Department of the State Attorney's Office (hereinafter - the Cyber Department), for further processing of the matter. The department handles offenses committed in the online space through two channels: handling criminal cases and "alternative enforcement." As a rule, alternative enforcement is used in circumstances where handling through the criminal channel is not possible. For example, when the advertiser is anonymous or resides outside of Israel and cannot be brought to justice through an effort.

reasonable.

Activity in the alternative sphere is regulated by a work procedure that deals with handling illegal content published in the online space . 99 The department examines whether the accounts, pages, or content collected or

98 For more information on the role of civil society, see: David Siman Tov and Amos Harvitz, **The Role of Civil Society Organizations in Curbing Covert Foreign Intervention in Democratic Processes,** INSS (2021).

99 Work Procedure - Cyber Department at the State Attorney's Office, Handling Illegal Content Published in the Online Space - Update No. 2

Received from the investigative and security authorities or other elements in government ministries, depending on the areas of responsibility, three cumulative conditions are met: 100

1. **The content constitutes an offense under Israeli law:** According to the procedure, among the offenses in which the department will act is an offense relating to false information as stated in Section 3 of the Computer Law, 1995-

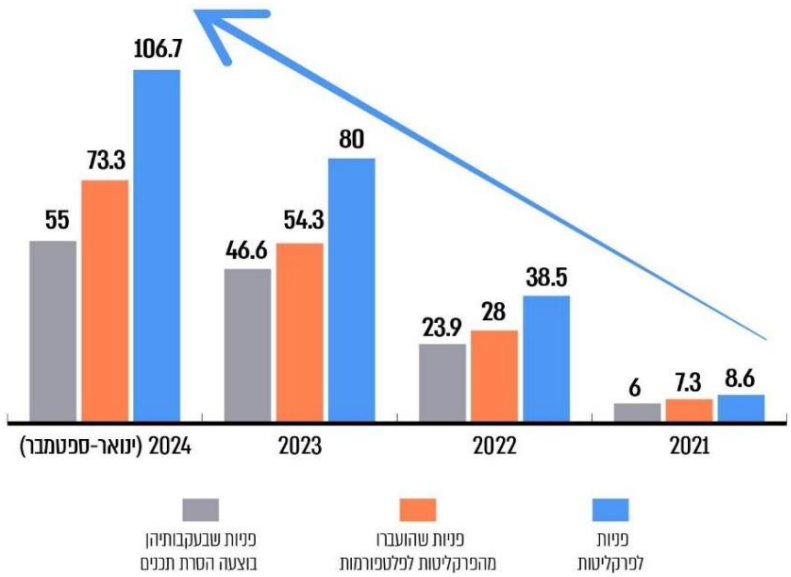
2. **The content violates the terms of use of the online platforms or internet access providers.**

3. **The existence of additional considerations** that justify reporting the prohibited content to the online platforms or Internet access providers, including the actual distribution of the advertisement, the target audience, the seriousness of the advertisement, the date of publication, the potential for virality of the advertisement, and the manner in which the advertisement was interpreted by its readers. In addition, at this stage, the tension between the public interest and rights such as the right to a good name, the right to privacy and the dignity of the person harmed by the advertisement on the one hand, and other rights at stake: freedom of expression, the right to access information, and the freedom to surf the Internet on the other hand, is considered.

If the conditions specified in the procedure are met, the department reports this content to online platforms and Internet access providers, so that they can consider removing it.

Regarding requests to remove content, below is information regarding requests submitted to the Attorney General's Office on all topics in the years 2019 - 2024:

Figure 10: **Data on requests for voluntary removal of content from social media, 2019 - 2024 (in thousands)**



According to data from the Cyber Department at the State Attorney's Office, processed by the State Comptroller's Office.

The data shows that in the years 2021-2024, there was a significant increase in the number of requests transferred from security agencies and various government ministries to the Cyber Department at the Prosecutor's Office for the removal of content in the voluntary track, including - against the backdrop of the Iron Swords War: from approximately 8,600 requests to more than 106,000 requests, and that approximately 15%-25% of the requests transferred from the Prosecutor's Office to platforms for the removal of content in these yea

100 The department does not engage in monitoring or tracking in the online space.

The audit revealed that the department does not have data segmentation by category of attempts at foreign influence, and these were sometimes counted under another category, such as "other" or "cyberterrorism organization activity," and the Cyber Department noted that it was not even possible to classify them with reasonable effort.

One way to deal with foreign influence online is by contacting the Cyber Department at the State Attorney's Office, so that it can contact the online platforms about the matter, but in the absence of detailed data regarding requests for removal in the area of foreign influence, it is not possible to know the extent of the platforms' responsiveness in this area.

In order to be able to examine in depth the effectiveness of handling this channel, it is recommended that the Cyber Department from now on segment the data on the number of requests forwarded to the department regarding foreign influence on the network, including the number of requests forwarded and responded to and the number of requests that were refused, including indicating on which platforms they were received or rejected; and that it should state the circumstances in which it was determined that the information in the requests was insufficient to forward them to the platforms; and what is required to promote their response to the requests. This need is exacerbated, among other things, since the Cyber Department informed the State Comptroller's Office in December 2024 that no criminal proceedings relating to foreign

In December 2024, the Cyber Department at the Ministry of Justice informed the State Comptroller's Office that there are barriers and difficulties in handling the issue and that there is a need to determine who are the responsible parties for collecting relevant information, locating, identifying, analyzing, intelligence gathering, and finally - forwarding a request for consideration of the channel for removing content by the Cyber Department; the Cyber Department further stated that working procedures should be established with the various bodies; controls should be established on the effectiveness of the treatment and the benefit derived from it; and the national priority order for activity on this issue should be determined, both for the bodies responsible for locating and identifying the activity of consciousness and for the State Attorney's Office responsible for requests for the removal of content.

As stated, as of March 2026, there is no designated body leading the fight against the threat of foreign influence. In light of the recommendation that the National Security Council propose to the Prime Minister an outline for leading the handling of the issue at the national level, which will also serve as an infrastructure for receiving a government decision on the issue, the aforementioned decision may lay the foundation for performing staff work in additional aspects. In this regard, it is proposed that consideration be given to the difficulties and barriers raised by the Ministry of Justice regarding the entities responsible for locating and identifying foreign influence content in the digital space and transferring it to the content removal channel, as well as to the manner in which requests for content removal are handled. This is done while considering the efficiency of the handling and the benefit derived from it. It is also recommended that the State Attorney's Office give its opinion on the need to develop a p

Examining existing regulation regarding social networks

Unlike television or radio broadcasts, platforms developed on the Internet are not subject to state regulation in the field of content distribution.101 The main legal rules applicable to the distribution of content in this space are largely determined and enforced by the platforms themselves within the framework of their terms of use (community rules), which outline the rules of conduct for their users. Within this framework, the platforms define the permitted and prohibited content or harmful use ,102 such as violence or disinformation, illegal or dangerous content (such as cyberbullying).

101 A series of digital content platforms, in much broader contexts than foreign influence, but as in the past, this has been examined Regulation has not been advanced for 2025. In this context, see also Tehila Schwartz Altshuler, Assaf Wiener and Eyal Zilberman, **A blueprint for regulating social networks in Israel.** (2023).

102 On this matter, see Amit Ashkenazi, “Proposal for Guidelines for Israel’s Dealing with Foreign Influence in Cyberspace and Social Networks,” **Intelligence – Law and Practice ,** 10, Institute for National Security Studies, Ministry of Intelligence (Ministry of Innovation, Science and Technology) and the Institute for Research on Intelligence Methodology (2024), pp. 219-230.

In addition to rules regarding the substance of the content, some platforms establish rules regarding the identity of the publisher or the mechanism for distributing the content. For example, the Community Guidelines of some platforms prohibit the performance of “coordinated inauthentic activity” or “covert influence operations” and in particular when they are carried out through multiple accounts to influence public opinion, while misleading the responsible party. The platforms use technologies and human review to enforce their Community Guidelines 103 and to detect content and accounts that violate them. The Community Guidelines and the scope of monitoring and removal of content that violates them vary from platform to platform according to their considerations, and they may change from time to time. In the periodic reports published by some platforms, they indicate the actions they take in this regard.

Given the centrality of online platforms and the existence of illegal and harmful content distributed on them, countries and organizations around the world have begun to examine ways to regulate and supervise the activities of online platforms. The models adopted around the world are diverse in terms of the level of intervention and the way they deal with the challenges inherent in the use of platforms . 104 For example, the European Union enacted the Digital Services Act (DSA). The law imposes obligations on very large platforms and search engines regarding the need to conduct an annual risk assessment and implement a plan to minimize them, to publish annual risk assessment reports, which detail, among other things, the measures taken to identify the risks related to the services they provide, to analyze these risks and to deal with them. The law requires the large platforms and search engines to publish transparency reports that include data on the scope of requests for removal of content submitted by different countries, and on the number of contents removed; The law also defines various obligations that apply to those platforms and large search engines, for example regarding cooperation with warrants; the need to provide means of contact for authorities; reporting and transparency obligations regarding content management activities; and the creation of warning mechanisms for users.

In Israel, too, a review has begun regarding the regulation of digital content platforms, and various committees in the Ministry of Communications and the Ministry of Justice have examined the issue and submitted their recommendations in 2022. It should be noted that this is a complex regulation (which concerns much broader contexts than the issue addressed in this report), which raises, among other things, challenges regarding freedom of expression and the right to privacy.

Within the framework of the gaps that the Cyber Directorate mapped in 2024 regarding foreign influence in the digital space, he insisted that there is no regulation in Israel that requires a platform to manage risks, report transparently, and manage efforts to remove content (except in the enforcement route, where the mere publication is presumed to be a violation of the law), and within the framework of providing a national response, this issue should also be addressed, including examining the possibility of "soft regulation."

Furthermore, the documentation shows that one of the challenges in thwarting attempts at foreign influence concerns the cooperation of the platforms, and that removing content is based on the "good will" of the social networks to shut down those campaigns, and that there are social networks, such as "Telegram", which, even through the Ministry of Justice, have significant difficulty in thwarting the content distributed on them.

---

103 For more on the subject, see Assaf Wiener, “National Preparedness Against Foreign Influence and Intervention Through Social Networks: Global Findings and an Israeli Situational Picture,” **Intelligence - Law and Practice ,** 10, Institute for National Security Studies, Ministry of Intelligence (Ministry of Innovation, Science and Technology) and the Institute for Research on Intelligence Methodology (2024), pp. 243-257. For a

104 review, see Appendix F of the report of the team advising the Minister of Communications to examine the regulation of digital content platforms (2022).

105 See, for example , the Committee for Formulating Measures to Protect the Public and Public Service Officials from Harmful Activities and Publications (2017); the Report of the Committee for Adapting the Law to the Challenges of Innovation and the Acceleration of Technology on the Subject of Illegal Content in the Digital Space, headed by the Director General of the Ministry of Justice, Adv. Eran Davidi (2022); the Team Advising the Minister of Communications to Examine the Regulation of Digital Content Platforms (2022). In this context, see also Tehila Schwartz Altshuler, Assaf Wiener, and Eyal Zilberman, **An Outline for Regulating Social Networks in Israel** (2023).

The Ministry of Communications informed the State Comptroller's Office in this regard in February 2025 that although it has dealt with issues related to the operation of social networks in recent years, it is not directly responsible for regulating the operation of social networks, including aspects related to foreign influence. The ministry also stated that the main obstacle to promoting regulatory activities concerned achieving broad government agreement to advance a legislative process on the subject.

The Ministry of Justice informed the State Comptroller's Office in January 2026 that regulating digital content platforms in general, and on the issue of foreign influence in the digital space in particular, raises weighty questions in other areas, and in particular in aspects of freedom of expression and the right to privacy, areas that are the responsibility of the Ministry of Justice.

In February 2026, the Ministry of Communications informed the State Comptroller's Office that it does not currently regulate the activity of social networks. The Ministry of Communications added that in recent months it had established a new department dealing with the field of television broadcasting on the Internet, and that the field of the digital space and social networks is very close in terms of content to the field of broadcasting. Therefore, it believes that it would be right for the aforementioned new department to be responsible for the activity of the digital space.

Although the Ministry of Communications and the Ministry of Justice have previously dealt with the issue of regulating digital content platforms, regulation has not been advanced. The scope of monitoring and removal of content carried out by each platform regarding content that violates its community rules in general, and those relating to foreign influence in particular, varies from platform to platform according to its considerations, and may change from time to time. Accordingly, the platforms' response to requests from the Ministry of Justice in the voluntary track, civil society, or the public to remove content is also subject to the discretion and cooperation of each of the platforms. As part of the mapping of gaps carried out by the Cyber Directorate in 2024, the need arose to examine the existing regulation vis-à-vis online platforms. As of March 2026, in the absence of a body entrusted with handling the issue of foreign influence, no coordinated policy had been formulated for activity vis-à-vis the platforms in this regard.

It is recommended that, as part of the examination to be carried out regarding the need for a responsible entity to outline the handling at the national level, consideration be given to the policy that should be maintained with respect to the platforms and that the matter be promoted in coordination with the Ministry of Justice and in consultation with the Ministry of Communications. In this regard, consideration should be given to the need to examine ways and tools to deepen the cooperation of the platforms regarding requests addressed to them and to examine the possibility of "soft regulation". It is also recommended that, as part of this examination, consideration be given to the various models that have been adopted around the world in this contex . 106 (Digital Services Act) DSA

Dealing with foreign influence in the digital space - education and public outreach

Education - Promoting information, media and digital literacy

Promoting information, communication and digital literacy is considered one of the components of increasing civic resilience against disinformation and foreign interference in information.107 These concepts have different emphases and definitions ,108 but it can be said that they refer, among other things, to the multitude of skills related to access, analysis,

106 An outline for regulating social networks in this regard. See also: Tehila Schwartz Altshuler, Assaf Weiner and Eyal Zilberman, "M. in Israel", The Israel Democracy Institute and the Israeli Internet Association, 2023.

107 https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf

108 In this context, see Ministry of Education, **Digital Literacy - Definitions and Models, Digital Literacy** (2022). https://meyda.education.gov.il/files/LishcatMadaan/Ogdanim/digital-literacy.pdf

To evaluate and create content in a variety of contexts and to develop the ability to take a critical approach to assessing the reliability of information and making informed decisions (for convenience, in this report, these skills will be referred to as digital literacy). People with developed digital literacy possess skills that help them evaluate the source of information, distinguish between facts and opinions, identify false and misleading content, and avoid various threats such as online grooming , online bullying, and personal information theft . [109]

The importance of digital literacy is increasing in light of the rapid development of artificial intelligence and the use of technologies such as DeepFake, which makes it difficult to distinguish between truth and falsehood, combined with the ability to widely and rapidly distribute its products on social networks.

Many countries and organizations around the world see the importance of promoting digital literacy in order to deal with disinformation in the digital space, which, as mentioned, is one of the main tools used for foreign influence purposes.

In 2020, the Council of the European Union stressed the need to strengthen citizens' skills to deal with disinformation and called, among other things, for systematic action to raise public awareness of the importance of digital literacy; to develop a digital literacy learning approach for all ages; and to improve the capabilities of professionals from various fields who play a role in imparting digital literacy. The European Parliament has addressed the issue over the years, and in a March 2021 resolution, it emphasized the need for the public to develop digital literacy to deal with various online threats, including disinformation . [110] [111]

In 2022, the European Commission formulated guidelines for teachers and educators to promote literacy, and in 2023, the Council of the Union recommended promoting the use of digital tools to combat disinformation. [112] [113]

The OECD also addressed the issue and noted in a 2024 report on dealing with disinformation that one of the key state goals is a systematic and long-term effort to increase social resilience to disinformation through digital literacy. [114]

In 2025, the World Economic Forum also addressed the importance of imparting media literacy, noting that it is not only a set of skills essential for individuals and information to cope in the age of disinformation, but also a fundamental pillar for protecting democratic discourse, social cohesion, and public trust. [115]

Various countries have also addressed the issue. For example, Ireland published a strategy document in April 2025 that included, among other things, reference to aspects related to FIMI, the national use of artificial intelligence against disinformation and the integrity of elections. The strategy defined several courses of action, including raising awareness of the issue and implementing national digital literacy strategies in the population. [116]

Also within the framework of Ireland's national strategy in the fields of literacy, computational and digital literacy for the years

---

109 https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/772886/EPRS_BRI(2025)772886_EN.pdf

110 Council conclusions on media literacy in an ever-changing world https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2020_193_R_0006 (C 193/06/2020)

111 https://www.europarl.europa.eu/doceo/document/TA-9-2021-0095_EN.html

112 European Commission, Directorate-General for Education, Youth, Sport and Culture Guidelines for teachers and educators on tackling disinformation and promoting digital

113 https://data.consilium.europa.eu/doc/document/ST-15740-2023-INIT/en/pdf

114 OECD (2024), Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity, OECD Publishing, Paris, https://doi.org/10.1787/d909ff7a-en

115 /https://www.weforum.org/stories/2025/07/disinformation-media-and-information-literacy

116 https://assets.gov.ie/static/documents/20250416_National_Counter_Disinformation_Strategy_-EN_-Final.pdf

The need to develop digital literacy skills was emphasized that would allow students and teachers [117]2033 - 2024
to navigate the digital space responsibly and critically, among other things, for the purpose of dealing with disinformation.

Another example is the National Digital Literacy Policy, published by the Ministry of Education and Culture in Finland in 2019, which aims to improve the ability of the entire population - from children to the elderly - to develop digital literacy. The policy document noted that in recent years the need for digital literacy has [118]
been emphasized in the context of societal threat scenarios, for example, the systematic and targeted dissemination of disinformation and anti-democratic messages, and that a higher level of literacy could help citizens protect themselves against these threats.

,[120]), which was formulated within the framework of the European Union[119]Digital Skills Framework for Citizens (DigComp)
Provides a common understanding for identifying the key areas of digital literacy and addresses five areas of "digital competence" and the skills required in relation to them.121 One of the areas relates to information and data literacy:

Figure 11: **Digital competencies required according to DigComp**

Source: DigComp 2.2 - The Digital Competence Framework for Citizens, 2022, Office Reviewer in Translation
The country.

Each of the areas is divided into sub-areas. The area of information and data literacy refers, among other things, to the evaluation of data, information, and digital content.

117 https://assets.gov.ie/static/documents/irelands-literacy-numeracy-and-digital-literacy-strategy-2024-2033-every-learner-from-.pdf

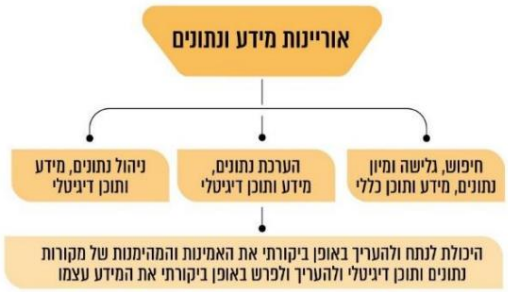
118 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162065/OKM_2019_39.pdf?sequence=1&isAllowed=y

119 DigComp - The European Digital Competence Framework DigComp,

120 established by the European Commission's Joint Research Centre for Science and Knowledge, provides definitions and tools for developing digital citizenship - see https://joint-research-centre.ec.europa.eu/projects- for more information. and-activities/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp_en

121 DigComp 2.2 - The Digital Competence Framework for Citizens, 2022

Figure 12: **Detailing the sub-domains of information and data literacy according to DigComp**



DigComp 2.2 - The Digital Competence Framework for Citizens, 2022, Ministry in Process:

State Comptroller.

The report addresses the level of proficiency of each sub-domain, from basic to highly specialized. As for the sub-domain related to the evaluation of data, information and digital content, at the basic level the user can identify in a guided manner the credibility and trustworthiness of common sources of data, information and digital content; at the highest level of specialization the user can formulate solutions to complex problems with multiple factors, related to the analysis and evaluation of reliable and trustworthy sources of data, information and digital content and propose new ideas and processes in the field.

The DigComp was first published in 2013 by the European Commission, and has been updated from time to time since then. The 2022 version noted that emerging technologies such as artificial intelligence, virtual reality and augmented reality, as well as new phenomena such as disinformation and misinformation, have created new and expanded demands for digital literacy. The report includes examples of the knowledge and skills required for the different dimensions, and in 2022, examples were given for the first time regarding awareness of the existence of incorrect and misleading information; the importance of identifying the source of the information; possible information biases; DeepFake products and the difficulty that sometimes exists in identifying them; and the ability to critically evaluate search results and social media activities to identify their sources, distinguish between factual reports and opinions, and determine whether they are true or biased; And recognize that some artificial intelligence algorithms, for example on social networks, may reinforce existing opinions in digital environments by creating "sounding boards."[122]

In light of developments in the field of digital technologies, such as the rapid and extensive spread of generative artificial intelligence systems and the implications this has for the scope of citizens' digital skills, an updated version of the Digital Skills Framework was published at the end of 2025, which, among other things, gave further expression to aspects related to artificial intelligence and dealing with disinformation.[123]

He suggested that Israel [124]A 2025 report by the Israeli Internet Association conducted as part of the DRI project Particularly vulnerable to deception and disinformation, partly due to low levels of digital literacy. The report noted that political and security instability, both domestic and regional, also contribute to creating fertile ground for local and foreign actors to exploit social divisions and undermine public trust in democratic institutions. Certain groups, such as ultra-Orthodox Jews, Arabic speakers, Russian speakers, and the elderly, are particularly vulnerable due to low media literacy, limited access to testing resources, and limited access to information security.

122 DigComp 2.2 - The Digital Competence Framework for Citizens, 2022, https://publications.jrc.ec.europa.eu/repository/handle/JRC128415

123 DigComp 3.0 - European Digital Competence Framework, 2025,

124 With the support of the European Union. ,Disinformation Resilience Israel (DRI) Project

Facts and lack of public service programs and civil society initiatives tailored to their unique needs. 125

Similar to various countries around the world, the importance of imparting digital literacy in the education system has become increasingly important in Israel. In particular, in 2021, the Ministry of Education published the "Learning Concept - Skills of the Education System 2030-2031", in order to outline an applied educational vision to challenge student readiness in a changing world, in line with the OECD Vision 2030. The concept presents a renewed and updated definition of the set of skills, disciplinary knowledge and values required for an individual to thrive and fulfill his or her destiny. The document proposes a conceptual and applied framework to structure learning and teaching processes according to the expressions of skills at different ages, to establish a set of learning and training processes for educational and support teams, and to help create measurement and evaluation processes. The concept presents four clusters: cognitive, emotional, social, and physical, divided into 13 skills, including digital literacy and information literacy. 126

For each of the skills, core competencies and actions were defined. One of the core competencies determined regarding digital literacy is "consumption and creation of content in digital media", among the actions defined within it is "evaluating the quality and credibility of messages in digital media by identifying the characteristics of the information provided", divided by age, and in the upper grades, this involves showing skepticism about information distributed in digital media and the ability to criticize messages and identify the motives of those distributing the information and messages on social networks 127
.

In July 2025, the Ministry of Education informed the State Comptroller's Office that it considers promoting safe and secure online behavior and preventing risky behaviors to be an important and central goal. To this end, an interdisciplinary team operates in the Ministry that promotes the issue in various educational spaces, while coordinating between the various departments and administrators. The Ministry operates in various ways to promote safe and secure online behavior, both through information and prevention programs for students, education teams and parents, and through providing assistance by Ministry of Education professionals in situations of risk and harm, in partnership with the National Headquarters for the Protection of Children Online - Unit 105.

The ministry noted that it offers programs to promote online protection and safety and prevent situations of harm and risk, alongside lectures on the subject in collaboration with the National Headquarters for Child Protection Online - Unit 105, and addresses the issue during National Safer Internet Access Week and in preparation for the summer vacation. It also produces informational materials for various target audiences (education teams, students and parents).

The ministry added that it integrates digital literacy skills across the curriculum, while adapting to the various fields of knowledge, and that recent literature reviews from around the world indicate that digital literacy is seen as a necessary area that all teaching staff must know, master, and integrate into teaching.

The Ministry of Education detailed its plans to promote online protection and safety and prevent situations of harm and risk, including the new life skills program "Powers on the Road." Which deals, among other things, with developing skills for safe and secure online behavior among students, the content of which was adapted to the needs raised during the ongoing emergency period, while developing resilience in the age of artificial intelligence. The program includes, among other things:

---

125 https://www.isoc.org.il/files/docs/disinformation/Disinformation-Resilieance-Israel- Stakeholder-Analysis-Report-April2025.pdf

126 Digital literacy is defined in the concept as "the ability to use information and communication technologies for a variety of personal, group, and social needs and goals, educational and in everyday life, in an appropriate, efficient, and responsible manner, and to adapt quickly to technological changes and developments." Information literacy is defined as "the ability to define the required information, locate it, organize it, evaluate it, and present it in an informed manner."

127 Ministry of Education, The image of the adult (in lecture). https://boger.openfox.io/%D7%9E%D7%99%D7%95%D7%9E%D7%A0%D7%95%D7%99%D7%95%D7%AA:%D7%90%D7%95%D7%A8%D7%99%D7%99%D7%A0%D7%95%D7%AA_%D7%93%D7%99%D7%92%D7%99%D7%98%D7%9C%D7%99%D7%AA

Lessons on identifying and dealing with false information, intended for elementary, middle, and high school students, as well as the Not or Fake128 project·

The ministry added that the Not or Fake project is the product of cooperation between the Film and Media Supervision Authority, the Israel Democracy Institute, the Mofet Institute, and the Internet Association. The program aims to strengthen the issue of civic media literacy in light of the increasing exposure to false information following the events of October 7, 2023. The proposed lesson plans include an explanation of false information online, in both normal and wartime periods, and tools for identifying it, and they also include activities according to the various subjects of study. The Ministry of Education stated that from January 2024 to May 2025, there were approximately 9,000 visits to the project's website, and 45,000 views of its content.

Fake or Not Project : 12 photos

Source: The project website.

The ministry also stated that since the Corona period and even more so since the outbreak of the Iron Sword War, in light of the ongoing period of emergency, there has been an increase in the consumption of information on various media channels, including social networks, including the viewing and distribution of difficult videos, the dissemination of information and false news, and the publication of posts of distress and vulnerability online in the shadow of the war. The ministry added that the education system has an important role in developing critical thinking skills, in balanced consumption of content, identifying risky situations online, and seeking help. The ministry also stated that during the Iron Sword War, the Ministry of Education was exposed to the phenomenon of foreign influence on social networks, and that the issue is also being studied in the face of education systems and organizations around the world, and accordingly, it will develop content for education staff, parents, and students.

Disinformation has been defined by the World Economic Forum as one of the key risks in the coming years, and various organizations around the world have highlighted the threat inherent in this risk, including the use of disinformation by foreign actors to undermine public trust in state institutions and increase social polarization. These organizations have also stressed that promoting digital literacy, developing critical thinking, and improving the ability to assess the reliability of information and the reliability of its sources, are key tools for dealing with this risk. For example, some European Union institutions have emphasized the need to develop digital literacy to deal with various online threats, including disinformation, and guidelines have even been formulated to promote digital literacy to deal with the issue; the OECD has set a national goal of increasing social resilience to disinformation through digital literacy; and the World Economic Forum has noted the importance of imparting Disinformation.

A 2025 report by the Internet Association found that Israel is particularly vulnerable to deception and disinformation, due in part to low levels of digital literacy and a lack of political and security stability, domestically. State and regional, contribute to creating fertile ground that allows local and foreign actors to exploit social divisions and undermine public trust in democratic institutions.

The review pointed out that the Ministry of Education offers lesson plans related to disinformation and critical thinking. However, the content offered is a matter of permission and is at the discretion of the school.

128 /https://www.fakeornot.org.il

and the educational staff. For example, within the framework of the life skills program "The Forces on the Road", which is a mandatory program, one of the chapters deals with optimal conduct on the Internet and preventing harm. However, the individual content conveyed within the framework of this chapter, including the choice of whether to deal with the issue of disinformation, is not defined as mandatory for schools, and each school is entitled to choose content according to its own discretion. It was also raised that the Not or Fake project website , **which the Ministry of Education operated, in collaboration with various parties, in light of the increasing exposure to false information following the Iron Swords War and with the aim of offering lesson plans and activities, recorded only about 9,000 visits in a period of about a year and a half, and the number of views on the website content was 45,000. It therefore follows that defining the content of the subject as only public education is not consistent with the risk inherent in disinformation for the individual**

The Ministry of Education responded to the State Comptroller's Office in February 2026 that it is leading three initiatives to advance the issue: (a) the "Skills on the Road" program (the new life skills program), which is a mandatory program in the education system and includes a chapter dealing with optimal online behavior and preventing harm. The lessons within the program are adapted to different developmental characteristics and age stages and to the cultural characteristics of the different sectors. In the past two years, the lessons have been adapted to the needs that arose during the ongoing emergency period, while emphasizing developing resilience in the era of artificial intelligence and dealing with false information online; (b) promoting media literacy - a program that provides students with tools to cope in a media-rich environment, with the aim of identifying false information and disinformation as part of the learning process in various fields of knowledge. As part of this, a dedicated "Not or Fake " website was built, which contains recommendations for lesson plans and learning and training materials in Hebrew and Arabic. The program is being updated These days, and will include lessons that provide tools for identifying foreign influence and DeepFake, mainly in preparation for the elections; (c) The National Plan for Integrating Artificial Intelligence in Education - a program within the framework of which the Ministry of Education developed an artificial intelligence competency model that combines knowledge, skills, values, and attitudes required for responsible conduct in a digital space saturated with artificial intelligence. The model is intended to strengthen students and education staff's critical understanding of information creation processes, the ability to identify manipulations, and the ability to assess the reliability of sources. The Ministry of Education noted that in this way, the model connects technological education, civic responsibility, and democratic values, as part of the education system's preparation for the challenges of foreign influence and disinformation. The Ministry of Education added that it will study the conclusions of the State Comptroller's report and carry out a process of learning, accuracy, and improvement of ministerial measures, in order to provide a comprehensive and holistic response to

It is recommended that the Ministry of Education define content related to disinformation as mandatory content in the education system in all its streams, starting at a young age. The application of education on the subject of disinformation and critical thinking regarding content in the digital space as mandatory studies is of crucial importance, especially in light of the definition of the risk of disinformation by a number of factors as one of the main risks in the coming years; in light of the increasing exposure to disinformation, including its dissemination by hostile foreign elements, especially after the Iron Sword War; and considering the technological development that blurs the ability to distinguish between truth and fiction.

In this context, it should be noted that the Digital Division is operating a national initiative to promote digital literacy in local authorities - "Project 100 in Digital Literacy." The initiative focuses on populations 129 which are characterized by with low digital literacy and provides them with training and guidance in all aspects of basic digital use. The goal of the project is to provide these populations with digital skills and competencies as a means of improving the quality of life, improving the ability to receive services in an advanced digital world, and encouraging the civic integration of disadvantaged populations, using government, municipal, and community digital platforms. As of January 2026, the project operates in 169 local authorities, and more than 12,000

129 Target population - residents of local authorities where the project operates, over the age of 18, lacking digital literacy or with low digital literacy, with an emphasis on the core population; Core population - Haredim over the age of 18, members of minorities over the age of 18 and senior citizens lacking digital literacy or with basic digital literacy.

Kashrut, in which 190,563 participants took part (of whom 67,859 were senior citizens, 35% of the total participants).

In January 2026, the Digital Division informed the State Comptroller's Office that training courses are being held as part of the project that include content dealing with disinformation, identifying misleading content, and critical thinking in the digital space. The Digital Directorate added that in training for adults, and in particular for senior citizens, there is systematic reference to the issues of safe browsing, identifying fraud attempts (phishing), identifying misleading content and false information, and maintaining privacy and securing personal information. This content is included both in dedicated workshops, such as the Fake News and False Information Workshop, the Safe Online Consumerism Workshop, and the Online Safety Workshop in the Age of AI, and as an integral part of the digital literacy course and training programs. In addition, the Digital Directorate noted that it has begun developing a dedicated digital course on the topic of "Digital Resilience," which will include, among other things, reference to topics such as digital fraud, risks and challenges on social networks; fake news, manipulations
Advertising and identifying incorrect information online.

The State Comptroller's Office positively notes the activity of the Digital Division in all matters relating to the provision of training for adults that includes content dealing with disinformation, identifying misleading content, and critical thinking in the digital space. The implementation of this training is of great importance, especially in light of the findings of the Israeli Internet Association's 2025 report, which revealed that Israel is particularly vulnerable to deception and disinformation, due, among other things, to low levels of dig

Public information

Raising awareness among the general public, and in particular decision-makers, about disinformation and foreign influence campaigns is one of the tools for increasing national resilience to these phenomena. 130 For example, the EEAS operates the EUvsDisinfo project to increase public awareness of foreign influence and disinformation attempts by publishing articles, studies and identified foreign influence attempts. Similarly, the French organization VIGINUM publishes, among other things, reports aimed at raising public awareness and enriching public knowledge on the subject. 131

.

The need for public awareness activities arose in Israel as part of the Cyber Directorate's staff work in 2017, which noted that critical awareness and education activities should be initiated for the general public. The issue was raised again in the Cyber Directorate's July 2024 initiation document. The document raised the need to strengthen the population's civil resilience through awareness and education activities, including the preparation of ongoing and sustained campaigns for emergencies, continuous content uploads, including tips, examples, and guides for identifying influence attempts, establishing a knowledge center for reporters on the subject, and publishing periodic reports on the subject. In the proposed Cyber Directorate's 2024 action plan, it was proposed that the institution establish an awareness and awareness "desk" that would coordinate international activity.
Ministry and civil society to increase public resilience through education and outreach efforts during routine times.

As part of the work of the headquarters to examine dealing with foreign influence online, the Cyber Directorate formulated an outreach concept in September 2024 that aims to reduce the effect of the threat of foreign influence by increasing public resilience and awareness of the issue and equipping the public with appropriate tools to identify the threat and deal with it. The concept included a review of literature on outreach and education on the subject, as well as a review of education activities, campaigns, and outreach activities on the subject carried out in various countries. Based on these, the Spokesperson's Division developed

130 https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf

131 https://www.sgdsn.gouv.fr/files/files/Publications/RA-Viginum-Annee1-32p-V20_EN_LQP-1.pdf

and advocacy in a set of recommendations and an advocacy model for dealing with the phenomenon in Israel among various target audiences.[132] The concept included reference to potential partners for carrying out advocacy and education activities.

The concept addressed, among other things, the need to create an orderly process for making decisions regarding cases in which information on the subject of foreign influence should be provided and the need to provide information in cases where there is concern that the influence operation will cause harm to human life; create widespread panic that will disrupt public order; harm the resilience of the population or involve psychological warfare aimed at inciting widespread panic or false news that affects cyberspace.

This included distributing dedicated publications on the subject.[133] At the same time, the Cyber Division conducted outreach activities on the subject of identifying fake news (some in collaboration with the Israel Police, the Israeli Defense Forces, and the Home Front Command), identifying bot activity as part of foreign influence campaigns, publishing a glossary on the subject of foreign influence, and reporting to the public on some of the foreign influence activities that were detected (such as sending text messages to the public from foreign entities). In addition, in December 2023, the Division launched a public campaign called "Overcoming Involvement."[134]

Image: 13 **"Overcoming Involvement" campaign**

Source: Cyber Directorate, Summary for the year 2023.

In addition, a follow-up campaign to the "You Participated" campaign was published in February-March 2025. The follow-up campaign was published on television, radio and digital, and according to data from the National Cyber Directorate, it reached 63 million digital impressions and more than 2 million households on television. The campaign focused on raising awareness of the threats of phishing, fake accounts, online misinformation and suspicious links.

In August 2025, the Cyber Directorate informed the State Comptroller's Office that it had decided to focus its efforts on the issue only in cases involving cyber-based foreign influence. The Directorate added that this focus would also be implemented in the Directorate's public outreach activities.

In February 2025, the Shin Bet informed the State Comptroller's Office that it attaches importance to creating resilience and awareness on the subject, and therefore, in cases where possible, it publishes information in the media about campaigns that have been detected. As stated, in January 2024, the Shin Bet published information to the public about several online platforms that are suspected of being operated by

132 Among them: the National Information System, the PFM, the Internet Association, the Ministry of Education and the Ministry of Foreign Affairs. https://www.gov.il/he/pages/cyber_dictionary_foriegn_influence

133 https://www.gov.il/he/pages/bots_activity_foreign_influence_campaign
https://www.gov.il/he/pages/identifying_and_dealing_with_foreign_influence

134 https://www.gov.il/he/departments/topics/psychological_warfare/govil-landing-page

Including the "Second Israel" and "The Avengers" campaigns - which Iranian security elements operated undercover on various platforms[135] to inflame political discourse and deepen the divide in Israel. The importance that the Shin Bet attaches to increasing awareness of the threat is also evident in its documents. It was noted that, given the existing gaps in dealing with the issue, it is right to focus efforts on increasing awareness of the threat among the general public and among decision-makers, both to reduce the effectiveness of similar moves and to encourage additional campaigns to flood in from below.

Increasing public awareness of attempts at foreign influence in the digital space is one of the tools for dealing with them and strengthening national resilience in the face of them. On the other hand, official attention to foreign influence operations may lead to their increased spread and thus assist the foreign entity behind them. This therefore requires the formulation of a regulated public information concept regarding the cases in which it would be appropriate to inform the public about detected attempts at influence, the entity publishing the information on the subject, and the channels through which the attempts were carried out.

After the outbreak of the Iron Sword War, the Shin Bet published information to the public about several campaigns in the digital space that were suspected of operating covertly to inflame political discourse and deepen divisions in Israel. Alongside this, the Cyber Directorate pointed out a gap in the issue of information and began to act on the issue, including formulating an information concept and carrying out information activities among the public. However, in August 2025, the Directorate decided to focus its efforts only on cases involving cyber-based foreign influence. As a result, the gap regarding strengthening national resilience through information activities and increasing public awareness remains, and there is no entity leading the information on this issue.

In February 2026, the Cyber Directorate informed the State Comptroller's Office that, in addition to the campaigns it had published in the past two years, it had distributed warnings and refutations to the public in real time regarding attempts at intimidation, demoralization, and deception, when these were messages that were distributed to the public on a large scale. For example, in 2024, 42 warnings were distributed, and in 2025, 51 warnings were distributed. The Cyber Directorate added that outreach efforts on the subject of foreign influence in the digital space are continuing, including in aspects that are not cyber-focused.

As stated, as of March 2026, there is no responsible entity for the issue of foreign influence in the digital space, including the aspects of information. Therefore, in light of the recommendation that the National Intelligence Service propose to the Prime Minister an outline for leading the handling of the issue at the national level that will serve as a basis for the headquarters' work on additional aspects, it is recommended that consideration be given to the issue of information to the public. It should be noted that although the Cyber Directorate conducts information activities on the issue, these activities are carried out voluntarily. The need to provide a response to the issue of information takes on added importance during wartime, when information activities and the rapid i Foreign influence.

In this context, it should be noted that security bodies also see importance in strengthening public awareness, increasing resilience, and providing a holistic response that includes informational activities.

Foreign influence during an election period

An election campaign is considered a particularly sensitive time in a democratic society with regard to foreign influence. The US are a particularly attractive target for foreign influence campaigns because[136] Department of Justice (DOJ) has argued that elections they provide an opportunity to undermine trust in one of the key components of democracy. The US Department of Homeland Security noted in its National Security Threat Assessment that

135 Shin Bet website, ,Shin Bet reveals several online platforms suspected of being operated by Iranian security officials .15.1.24

136 Department of Justice, Evaluation of the US Department of Justice's Efforts to Coordinate Information Sharing About Foreign Malignant Influence Threats to US Elections, 2024; https://oig.justice.gov/sites/default/files/reports/24-080.pdf

Because before the 2020 US presidential election, Iran tried to empower the homeland for 1372025
Divisive narratives to incite violence, influence the American electorate, and undermine confidence in the electoral process. He added that foreign actors with hostile influence will almost certainly attempt to influence democratic processes at all levels of government - federal, state, and local - in order to influence the preferences of US voters, exacerbate social tensions, and undermine confidence in democratic institutions and electoral processes. It was assessed that these actors will increase their overt and covert use of media and networks of fake social media accounts, as well as operate through influence agents to spread their desired narratives and work to advance their goals.

From 2024 identified [138]In the risk picture of the European Union Cybersecurity Agency (ENISA)
Some key cyber threats include information [139]manipulation and interference. The report noted that information manipulation could affect electoral processes in various ways, such as setting the agenda on key issues, encouraging voter abstention, or harming political opponents.

A study commissioned by the European Parliament's Committee on Civil Liberties and Constitutional Affairs, which aims to identify the challenges threatening the resilience of democracy ahead of the 2024 European Parliament elections, noted that disinformation campaigns are probably the most common type of foreign interference, and are particularly effective during election periods. They aim to sway votes in favour of certain candidates or parties, reduce voter turnout It was also noted that [140]and raise doubts about their validity and fairness.
although in many cases the impact of attempts at foreign influence is limited, they may have a cumulative long-term impact on trust in democracy, the social fabric, and the international order.

It was [141]In a June 2025 European Commission report on the 2024 European Parliament elections, noted that the EEAS identified attempts by Russia to interfere in the elections, focusing on social media aimed at creating divisions and divisions in society by spreading false information, defaming political leaders, and sowing distrust in public institutions.

A study conducted at the UK's National Institute for Data Science , 142 and Artificial Intelligence examined the impact of false and misleading content generated using artificial intelligence on the 2024 US election. The study found no conclusive evidence that such content significantly influenced the election results, but identified indirect effects on the broader democratic system, such as confusion about the authenticity of election content. It was noted that this jeopardizes voters' ability to receive reliable information. It was also noted that DeepFake could be used to attempt to undermine the legitimacy of election results, for example through fake videos or images depicting ballot tampering, ballot theft, or other election offenses.

---

137 Homeland Threat Assessment, 2025. https://www.dhs.gov/sites/default/files/2024-
See also: 10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf
https://www.fbi.gov/news/testimony/worldwide-threats-to-the-homeland-091720

138 European Union Agency for Cybersecurity, **Enisa threat landscape 2024** (2024) Risks identified in the report: ransomware, malware, social engineering, threats to information, threats to information availability,

139 manipulation and interference with information, and attacks on the supply chain.

140 European Parliament, **Resilience of Democracy and European Elections against New Challenges,** 2024 European Commission, **Report on the 2024 election to the European Parliament 2024,** (6.6.25)

141

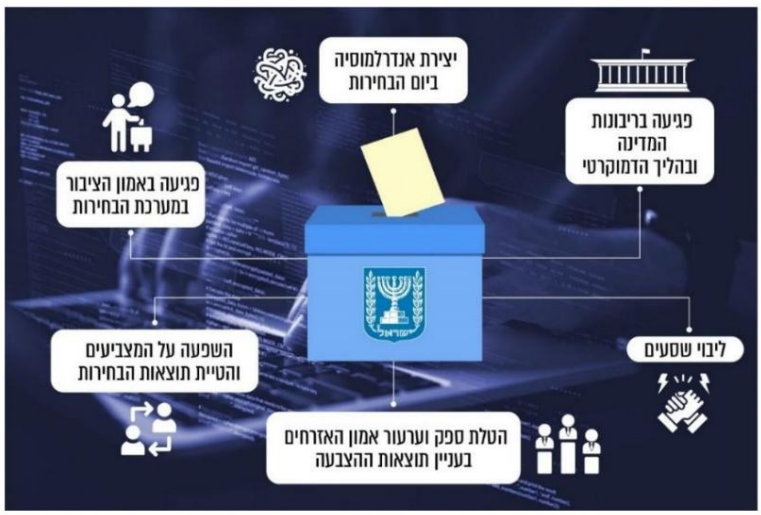
142 The Alan Turing Institute, **AI-Enabled Influence Operations: Safeguarding the Future Elections,** 2024

On 6.12.24, the Romanian court annulled the first round of the presidential election held on 24.11.24. The court ruled that information presented before it revealed voter manipulation and distortion of equal opportunity for candidates in the elections, through the non-transparent use of digital technologies and artificial intelligence in the election campaign, in violation of election laws, as well as through the financing of the election campaign. The decision noted that voters received misleading information from unreported sources, including on the Internet [143]
Through an election campaign in which one of the candidates was aggressively promoted, bypassing the provisions of the law and exploiting the algorithms of social media platforms. [144] [145]

The European Commission, operating within the framework of the European Union, announced a follow-up to this, on 17.12.24. [146]
Opening of an official investigation against one of the platforms for suspected violation of the Digital Services Law (DSA) regarding its duty to assess and minimize systemic risks related to the integrity of the elections. The Commission President stated in the announcement that the investigation was opened following significant indications that external parties interfered in the Romanian presidential elections through this platform.

A 2025 report by the French service for monitoring and protection against digital foreign interference (VIGINUM) noted that the elections appeared to be the target of a campaign that dealt with the manipulation of information in the Romanian elections. [147]
A sophisticated digital campaign that was based on manipulating the algorithm of one of the platforms, which is a particularly popular platform in Romania, and included the pre-activation of account sets and the recruitment of influencers. It was also noted that the analysis of the campaign highlights, among other things, the relative ease with which it is now possible to force users to expose themselves to a particular topic on a social network such as the aforementioned platform, without the system recognizing the action as inauthentic or performing filtering; and the vulnerability of influencers, who are increasingly exposed to the risk of activation and manipulation by malicious actors, operating in disguised ways. The report noted that one of the main damages caused by the campaign was the damage to voters' trust in the credibility of the electoral process.

Figure 13: **Potential Damages from Attempts to Influence During an Election Period**



143 RULING No 32 of 6 December 2024 on the annulment of the electoral process for the election of the President of Romania in 2024
https://www.ccr.ro/wp-content/uploads/2025/02/RULING-No-32-2024.pdf

144 Article 11 of the decision.

145 Article 14 of the decision.

146 European Commission, "Commission opens formal proceedings against TikTok on election risks under the Digital Services Act", Press Release, 17.12.4
https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487

147 Manipulation d'algorithmes et instrumentalisation d'influenceurs Enseignements de l'élection .présidentielle en Roumanie & risques pour la France, VIGINUM, Février 2025

The above indicates that an election period is perceived by countries and organizations around the world, such as the European Union, the World Economic Forum, the United States, and the United Kingdom, as a particularly sensitive period with regard to foreign influence. This period may serve as a fertile ground for attempts to influence the agenda, the perception of reality, and decision-making, in a way that could skew the election results (without directly disrupting them) or sow doubt about the purity of the elections and the credibility of their results. For example, true, biased, or false information can be published in order to influence public opinion and divert it in a certain direction that will be reflected in voting patterns or to undermine public confidence in the election results; to act to resonate messages on a large scale; or [148] on social media to shape the discourse in a certain direction to influence voting rates among the population as a whole or part of it. There have been indications of attempts at intervention in several election campaigns in recent years. The cancellation of the elections in Romania in December 2024, among other things due to suspicions of foreign interference through the digital space, is the most prominent case. Which illustrates the potential harm inherent in foreign influence and manipulation of inf

Identifying the threat in Israel

Similar to other countries, in recent years, concerns have been identified in Israel about foreign influence in the digital space during election periods. Below are the details:

CENTRAL ELECTIONS COMMITTEE: The Elections Committee is an independent statutory body established under the Knesset Elections Law [Consolidated Version], 1969. This committee is responsible for ensuring that there is a proper and reliable election process in all its stages, reflecting the will of the voters in Israel. The Elections Committee is entitled to seek assistance from state authorities in fulfilling its duties, and they are obligated to assist it, pursuant to Section 150 of the Law. Following the 2016 US presidential election campaign and other election campaigns around the world, in which the connection between content in the online space and the ease of distribution and impersonation inherent in this space and the potential for diversion involved, was revealed, the Elections Committee raised concerns in 2018 that there may be attempts to influence voters in order to harm democratic institutions.

The Central Elections Committee informed the State Comptroller's Office in October 2024 that it had identified three major potential harms in this context: (a) **Harming public trust in the electoral system and in Israeli democracy,** such as publications that the purity of the elections is being harmed; (b) **Harming the voter's ability to vote and creating chaos on election day,** such as falsely publishing that the elections have been canceled or that a particular polling station has been closed; (c) **Harming the voter's ability to vote freely by misleading or diverting him,** such as publishing that a particular candidate has withdrawn, publishing DeepFake as if they were the opinions of a particular candidate.

Regarding DeepFake, the chairman of the Central Committee for the Twenty-Fourth Knesset noted that the use of files produced with this technology as part of election propaganda "could undermine the public's belief that there is truth in elections in general: if everything can be faked, why believe in anything? Hence, they pose a danger to the very existence of the election process and the survival of the democratic system." [149]

It should be noted that in the framework of the lessons learned document by the Chairman of the Central Elections Committee, Supreme Court Justice Yitzhak Amit, after the elections to the Twenty-fifth Knesset, which took place in 2022, the Chairman of the Committee referred to the distribution and echo of election propaganda through means that are deceptive . 150 The Chairman of the Committee noted that the amendment to the Elections (Propaganda) Law, 5719-1959, which requires transparency in sponsored propaganda messages or on behalf of an election candidate, was a first step in dealing with illegitimate means.

148 Dganit Peikovsky and Eviatar Matanya, **"Cyber Influence Operations - Characteristics and Insights",** The Campaign for Consciousness - Strategic and Intelligence Aspects, Intelligence Halacha and Mease (2019); Dudi Siman Tov, Gabi Siboni, Gabriel Erel, "Cyber Threats to Democratic Processes", Cyber, Intelligence and Security, Volume 1, Issue 3, December 2017, pp. 59-69.

149 TBA 9/24 **Yesh Atid v. "Yes to Peace" Association** (18.1.21), published on the Central Elections Committee website.

150 Twenty-five (November 2022). Lessons from the Chairman of the Central Elections Committee following the 2022 Knesset elections

Chairman of the Committee [151]. To sway the voter's mind and spread propaganda or misleading messages in a disguised manner, he added that in his opinion, additional steps are needed to expand the duty of transparency and regulate phenomena in the digital space that are designed to manipulate public opinion, such as the use of DeepFake technologies ; the creation of influence networks to resonate messages and amplify them among voters by using fictitious accounts operated by bots, including for sharing and "likes"; fake profiles under pseudonyms or even the names of others (fake); "disguised" groups designed to run a party or politicians; the establishment of a network of fake accounts and phenomena of inauthentic behavior on social networks.

[152]

Shin Bet: The Shin Bet informed the State Comptroller's Office that it began operating in the area of foreign influence during the 2017 election period. Shin Bet documents revealed that attempts at foreign influence were identified in previous election campaigns, and in preparation for the election campaign for the twenty-fifth Knesset, it was preparing to intensify attempts at foreign influence online, with an emphasis on social networks. In a discussion with the Central Elections Committee that took place in preparation for the election campaign for the twenty-fifth Knesset on the subject of cyber threats to the election campaign and dealt, among other things, with the issue of influence and false information, the Shin Bet noted that from observing events in the world, one of the greatest challenges is casting doubt among citizens regarding the results of the vote.

A Shin Bet document from June 2023 revealed that it had identified several foreign online campaigns and assessed that these campaigns constituted platforms through which covert foreign interference would be carried out during the elections.

The Shin Bet informed the State Comptroller's Office in February 2025 that during the election period the threat of foreign influence increases considerably and the potential for damage is high, and that in the elections for the twenty-fifth Knesset, several campaigns suspected of being foreign influence operations online were located and thwarted.

NATIONAL **CYBER SYSTEM:** In a discussion on preparations for the elections to the Twenty-Third Knesset that took place in January 2020, the head of the National Cyber System noted that one of the main threats that must be addressed in cyberspace in the context of the elections is influencing public opinion, for example by sowing divisions.

In the discussions of the Cyber Division in preparation for the elections for the twenty-fifth Knesset, the Division emphasized that the use of cyber as a means of influencing electoral systems in countries around the world has gained momentum over the years, and that the elections in Israel are a significant target for intervention by various elements in the space, both in the desire to influence the results of the elections and for the purposes of creating awareness of harm to governance. The Division noted that in recent election campaigns, parallel activity by several attack elements was identified, in order to create activity to influence the electoral system in Israel, and, among other things, to reduce the voter turnout, damage the image of the parties, and undermine the credibility of the process. The Division emphasized that awareness activity is the most common and widespread, and its assessment was that it is highly likely that such attempts will be made, such as the dissemination of false information in preparation for the elections.

The National Security Council: In discussions held in the Elections Committee in preparation for the elections to the Twenty-fifth Knesset, the National Security Council emphasized the threat of foreign influence on the networks and noted that at that time there were already efforts to influence from various elements, and the assumption was that the election process would be their target.

MINISTRY OF JUSTICE: The Ministry of Justice informed the State Comptroller's Office in December 2024 that an election campaign period is a particularly sensitive time for influence operations, as they have the potential to influence voters and skew the election results. Influence operations originating outside Israel constitute a core violation of the state's sovereignty and its democratic process.

---

151 In this context, see also TBAK 8/21, which determined that the provisions of the law relating to the need to indicate the identity of the person behind election propaganda also apply to publications on the Internet, including on social networks, and noted that this will assist, among other things, in exposing the interference of foreign entities that usually operate anonymously.

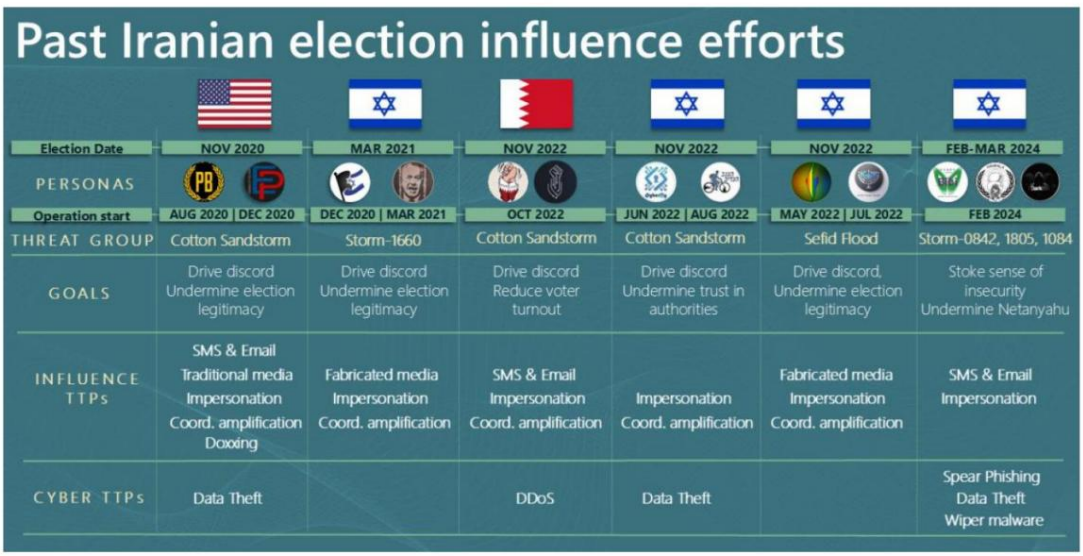
152 For more information, see Tehila Schwartz Altshuler and Guy Luria, “Digital Propaganda and the Threat to the Elections,” Israel Democracy Institute (2020).

The Ministry of Justice added that influence operations during an election period raise unique challenges, including: the need for urgent action as the election date approaches ("there is no second date"); there is the potential for greater motivation for hostile elements to launch awareness operations; there is the potential for particularly serious damage in the form of biasing the election results or discrediting the election results and creating an acute legitimacy crisis; there is a need to exercise extreme caution in order not to harm protected political content in terms of the expression of all network users, which is of utmost importance during an election campaign and as Election Day approaches.

A study conducted for the State Comptroller's Office to identify and analyze [153] **REPORT FROM THE CITY** official and unofficial activity on social media used to promote the factions and lists running in the elections revealed that in the run - up to the elections for the twenty-first, twenty-second, and twenty-third Knesset, there were indications that sponsored propaganda activity was carried out for factions through the purchase of Facebook and Twitter accounts, as well as through the operation of fictitious accounts. In light of this, the State Comptroller raised concerns that there is a wide-ranging discourse on social media that purports to be authentic, which could mislead the public and even sway public opinion in favor of or against factions. The study's authors were unable to determine who was responsible . 154 Thus, it could affect the election results.

A 2024 Microsoft report on Iranian foreign influence during the US election period includes examples of attempts at foreign influence during elections, including towards Israel. The report indicates that attempts at foreign influence were made by Iran during elections, to stir up controversy and to undermine the legitimacy of the elections and trust in ·government institutions. 155

Image: 14 **Attempts at foreign influence by Iran during an election period**



·Source: Microsoft Report (2024)156

153 State Comptroller, **Report on the Results of the Audit of the Faction Accounts and Candidate Lists for the Election Period to the Twenty-Second** Knesset (2021); **Report on the results of the audit of the accounts of the factions and candidate lists for the election period for the Twenty-Third Knesset** (2022). The aforementioned factions and lists claimed that they did not purchase party promoter accounts or operate fictitious profiles for payment.

154 Microsoft, Iran steps into US election 2024 with cyber-enabled influence operations 2024 https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/5bc57431-a7a9-49ad-944d-b93b7d35d0fc.pdf

155 Microsoft, Iran steps into US election 2024 with cyber-enabled influence operations 2024

156

Elections are the culmination of the democratic process and serve as a central component in building public trust in the country and its institutions. An election campaign period is a particularly sensitive time for attempts at foreign influence. Similar to international organizations and countries around the world, in Israel, several factors, including the Central Elections Committee, Shin Bet, the Israeli Secret Intelligence Service, and the Ministry of Justice, have identified the serious potential damage that could be caused by foreign influence during an election period, to the point of skewing the election results and undermining public confidence in the results. At the same time, foreign online campaigns were identified that were carried out during an election period in Israel, as well as campaigns that were assessed to be platforms through which covert foreign intervention would be carried out during the ele
The elections.

Dealing with foreign influence during an election period

Taking note of the risks raised by various bodies regarding foreign influence during election periods, the State Comptroller's Office examined what actions were taken in recent election campaigns to deal with the issue.

In October 2024, the Central Elections Committee stated that although it is not the body responsible for dealing with foreign elements seeking to influence the Israeli voter, after identifying the threat, it acted to motivate security forces to use their powers to deal with it. In this context, in 2018-2022, in preparation for the elections for the twenty-first to twenty-fifth Knesset, the committee held several discussions on the subject with the participation of various entities in order to examine how they were dealing with the issue and to coordinate their activities.

The Election Commission's attribution threat

In light of the potential harms identified by the Elections Commission, it determined that the core focus of election protection would expand to also focus on cyberspace impact. Subsequently, in 2019, the Commission included this issue in its reference threat and reference scenarios.

The threat attribution is intended to direct defense efforts according to the threats identified, their severity, and the likelihood of their realization. A gap has emerged in this regard.

The importance of the threat of attribution is also heightened in light of the reference made by the Chairman of the Elections Committee, Supreme Court Justice Yitzhak Amit, in the document on drawing lessons after the elections to the twenty-fifth Knesset held in 2022, according to which additional steps are required to expand the obligation of transparency and regulate phenomena in the digital space that are intended to manipulate public opinion, such as the use of fictitious accounts operated by bots, the use of fake profiles, the establishment of a network of fake accounts, and phenomena of inauthentic behavior on social networks.

As for the steps proposed by the Chairman of the Elections Committee for the Twenty-fifth Knesset in the document on drawing lessons after the elections, in order to regulate phenomena in the digital space that are intended to manipulate public opinion, the Elections Committee stated that expanding transparency obligations and regulating the digital space are not "parked" under the field of elections, but rather require significant and substantial legislative amendment. However, the best way to implement the changes is through legislative amendment. According to the Elections Committee, these steps will contribute to the ability of the Dealing with threats.

It is recommended that the Elections Committee act to correct the gap that was raised. Furthermore, to the extent that the Committee believes that there is a need to implement specific legislative amendments to eradicate phenomena in the digital space during an election period, it may do so.

and submit a proposal to amend the law to the Constitution Committee, Law [157], To act, subject to the approval of the committee plenary and a Knesset trial.[158]

Monitoring influence operations during elections

As stated, the Shin Bet is involved in monitoring foreign influence on social networks, including during election periods, and during this period there has been a change in the working method and various operations are carried out.

Shin Bet documents summarizing the election campaign for the twenty-fifth Knesset in 2022 indicate that its working assumption was that the main state adversaries would attempt to intervene and influence the election process in accordance with their interests. Accordingly, the Shin Bet acted on the issue. At the same time, it received information from various sources about suspicious profiles or unusual activity online, including from civil society, and these were examined for suspicion or incrimination. Suspected profiles were transferred to the Cyber Department of the State Attorney's Office for further processing (see below).

The Shin Bet informed the State Comptroller's Office in February 2025 that in the elections for the twenty-fifth Knesset, several campaigns suspected of exerting foreign influence online were located and thwarted. The profiles that were located were, among other things, engaged in creating negative discourse about certain candidates and legitimizing the avoidance of voting at the ballot box. All of the identified campaigns were transferred to the Attorney General's Office for closure.

As part of the lessons learned process carried out by the Shin Bet after the elections for the twenty-fifth Knesset, it was noted that there is room for improvement in several aspects, including improving work interfaces with the Attorney General's Office; creating a joint intra-organizational forum to streamline the work process for developing tools and methods.

In July 2025, the Shin Bet informed the State Comptroller's Office that, in furtherance of the lessons learned, it had recently made a significant technological leap. The Shin Bet added that within the framework of the pilot (on this matter, see above in the chapter on monitoring foreign influence in the digital space) emphasis was placed on providing a response to as wide a range of threats as possible. Social networks.

It emerged that as the election period approaches, the intensity of Shin Bet activity in the field of monitoring foreign influence in the digital space is increasing, and, among other things, various actions are being carried out. However, as of July 2025, the Shin Bet has not yet begun preparations for the elections for the Twenty-sixth Knesset.

As stated, the Shin Bet informed the State Comptroller's Office in July 2025 that the change in the working method for the elections is being implemented a certain period before the date of the elections. In view of the high potential for damage from foreign influence during an election period, the intensification of the threat in recent years, and the gaps that still exist in the field of monitoring and prevention, it is recommended that the Shin Bet examine, in cooperation with the Central Elections Committee, whether preparations for this period of time before the election date are sufficient. This is all the more true in light of past experience, which shows that elections have been brought forward more than once, and have not been held on the date originally set, and in light of the campaigns that have already been identified around the world and in particular in Israel.

In January 2026, the Shin Bet informed the State Comptroller's Office that it had begun focused activity in preparation for the 2026 elections.

The Elections Committee announced in February 2026 that the committee and security agencies had begun preparations for the elections to the Twenty-sixth Knesset, which are scheduled to be held according to the provisions of the law in about ten months, in October. .2026

157 See details on this matter on the Elections Committee website, in the section describing the activities of the Elections Committee's Legal Bureau and the activities of the Legislation Subcommittee.

158 If it was not submitted to the Knesset as a bill by a member of Knesset in the manner prescribed for this purpose in the Knesset regulations.

Removing foreign influence content during an election period

When foreign influence activity is identified in the digital space, a request is forwarded to the Cyber Department at the State Attorney's Office so that it can take action to remove the relevant content.

In 2019, the Ministry of Justice established the main principles of action for dealing with phenomena in cyberspace in the context of elections, including foreign influence (hereinafter - the Principles of Action Document). The Ministry of Justice insisted that the special characteristics of the Internet and social networks allow them to be abused by many parties. However, at the same time, the development of these tools allows everyone to have free discourse, and is important for freedom of expression and democracy. Therefore, in general, caution should be exercised in all matters concerning government intervention that affects platforms for online discourse, and sensitivity is increasing in the context of political expressions, and especially during election periods.

The Ministry of Justice added that, however, the threats to the purity of elections through the exploitation of the characteristics of the Internet, which have been discovered in various countries in recent years, require the design of an arrangement to address these phenomena, and that such an arrangement must ensure that freedom of expression and public trust in freedom of discourse in all matters related to elections are not unduly harmed by interference from the incumbent government or another governmental entity.

Accordingly, the Attorney General determined that, as a general rule, there is no room for enforcement agencies to take action regarding the content of publications on the Internet, including regarding the reliability or accuracy of an advertisement. On the other hand, it was determined that action must be taken to reduce the misuse of the Internet in the context of elections in all matters relating to actions not related to content. It was noted that with regard to offenses under election law that fall within the powers of the Chairman of the Elections Committee, the best course of action is to file a request for a restraining order.

It was further noted that, in addition to examining the appropriate cases of criminal enforcement, it is also possible to examine a route of contacting service providers with a request that they prevent abuse of the features of the platforms they offer to the public in all matters relating to elections (hereinafter - the voluntary route), which may bring immediate benefit, preventing the continuation of the danger of unfair influence on the voter.

The document detailed guiding principles for applications to the Cyber Department in the voluntary track to reduce unfair influences on the elections, and given the sensitivity of the issue and the importance of maintaining public trust, it was noted that such an application would be made in coordination with the Chairman of the Central Elections Committee. The document detailed possible scenarios for interference or influence on the elections via the Internet and social networks, as well as the methods of action that were approved by the State Attorney and the Attorney General.

In a discussion held at the Central Elections Committee in 2022, the Cyber Department pointed out the possible difficulty in defining the source of the threat, and noted that in this case, the assumption will be that it is an internal threat, and due to the concern of affecting the protected discourse that deserves protection during an election period, this will be discussed at senior levels in the State Attorney's Office, and this will be decided in accordance with the criteria detailed in the Attorney's Office procedure.

In February 2026, the Central Elections Committee informed the State Comptroller's Office that the Chairman of the Committee has the authority to issue orders under the Elections (Propaganda) Law, 5719, 1959, provided that several conditions are met: an initiated petition is submitted to the Chairman of the Committee; the requested order is to prevent or terminate the commission of the offense; the offenses for which a petition can be filed are offenses under the provisions of the Propaganda Law or under Chapter 11 of the Knesset Elections Law; the representative of the faction whose propaganda constitutes an offense or is likely to constitute an offense will be given an opportunity to present his claims to the Chairman of the Committee. The Elections Committee added that even if a justified report is received, without the filing of a petition by the applicant, conducting a procedure before the Chairman of the Elections Committee and issuing an order by him, it will not be possible to remove the information. Furthermore, even if the Chairman of the Elections Committee issues a restraining order, the Committee has no authority to remove the content, and the removal process is carried out through The State Attorney's Office at the Ministry of Justice, which is evacuated

to the relevant platform. The committee noted that this state of affairs leaves the committee in a "reactive" position and not in a "proactive" position, with all that this implies.

The threats to the integrity of elections through the exploitation of the characteristics of the Internet, including attempts at foreign influence, led the Ministry of Justice to formulate in 2019 guiding principles for addressing these phenomena, as well as ways to deal with various scenarios such as the activity of bots or fake accounts linked to a foreign country. It emerged that at the time of the audit's conclusion, approximately six years after these principles were formulated, and despite significant technological development, including in the area of the use of artificial intelligence tools, the guiding principles had not bee

It is recommended that the Ministry of Justice conduct a lessons-learned process and review and update the list of scenarios to ensure that the principles document includes ways to deal with all existing scenarios as of today.

The Election Committee's activities vis-à-vis online platforms

As mentioned, there is no regulation regarding digital content platforms in Israel. The scope of monitoring and removal of content carried out by each platform varies from platform to platform according to its discretion and may change from time to time.

In light of concerns about the exploitation of online platforms to influence public opinion through unfair means, some have announced their intention to use various tools to protect the elections, such as marking certain content (such as that whose source or authenticity cannot be verified), removing certain content (such as that intended to suppress voting or that could lead to violence), cooperating with fact-checkers, and restricting publications in the run-up to Election Day.[159]

Following lessons learned from previous election campaigns in Israel and around the world, in which concerns were raised about foreign influence via social media, the Central Elections Committee held discussions with several online platforms in 2019-2022 regarding their preparations for elections in Israel and the tools available to them regarding political publications. In some of the discussions, platform representatives noted that although certain tools were used around the world during election periods, given the short timelines leading up to the elections in Israel and the adjustments required to implement them, they encountered difficulty in implementing them.

In 2019-2022, the Elections Committee held discussions with several of the online platforms regarding their preparations for the elections in Israel, including regarding foreign influence in the digital space. Holding this dialogue is a significant step in advancing the fight against the issue. However, it emerged that from 2022 to August 2025, the Central Elections Committee did not hold discussions with the online platforms on the issue. This is despite the intensification of the threat and indications of attempts at foreign influence that have been noted in several election campaigns in recent years around the world, and despite the fact that since the elections were held in 2022, there have been changes in the patterns of use of platforms in Israel, in the community rules and self-regulation that the platforms apply to themselves, and it is not inconceivable that there have a

In light of this, and considering the need to adapt the tools for elections in Israel, it is recommended that the Elections Committee immediately resume dialogue with online platforms, including to ensure that all the tools used around the world to protect elections, including with respect to foreign influence, will also be implemented during the Israeli election period.

159 For more information, see Assaf Wiener and Ido Ily, **Social Networks' Preparations for National Elections Around the World: An Updated Review,** Israeli Internet Association (2022); **Social Networks and Technology Giants' Preparations for the 2024 Elections - An Updated Review,** Israeli Internet Association (2024).

The Elections Committee informed the State Comptroller's Office in February 2026 that it had initiated meetings with the major social media providers, with the aim of learning how they intend to deal with the widespread distribution of misleading content during an election period, what tools they intend to use, how they operate worldwide in this area (since this problem is not unique to the State of Israel), and which of these tools and methods of operation can be used within the framework of the providers' policy and community rules and existing legislation. The Elections Committee noted that the process and the formulation of insights began a few weeks ago and is in full swing.

Publicity during an election period

One of the key tools for dealing with attempts to distort the discourse and unfairly influence voters during an election period is to warn the public and raise its awareness of attempts to manipulate public opinion in the digital space. This is done, among other things, by providing the public with basic tools for identifying fake news and attempts at influence and increasing its awareness of their existence.

The Central Elections Committee informed the State Comptroller's Office in October 2024 that since the elections for the twenty-first Knesset, it has taken extensive actions regarding influence operations and fake news. This includes formulating a targeted message page for the public and publishing it on various platforms, including on the committee's website and on social networks; an information campaign on television, radio and digital, including on various websites and on social media. The committee's publications included, among other things, information in Hebrew and Arabic on how to identify false information; recommendations to exercise caution before sharing information and how to act if suspicions of spreading false information arise. The following are examples of the committee's publications:

Image: 15 **examples of the committee's publications regarding false information**

Source: The Central Elections Committee's Facebook page.

Public information is an important tool for dealing with attempts to manipulate public opinion, including by foreign actors. In light of the growing threat, including technological advances that enable the improvement of the quality and spread of influence attempts, such as through the use of artificial intelligence tools, and in light of the real concern that foreign actors will exploit the election period to influence voters.

and undermining public confidence in the integrity of the elections and their results - it is recommended that the Elections Committee prepare to expand its outreach, awareness, and education activities for the general public regarding the risks arising from false information, and in particular regarding the possibility that the source of the information is a foreign entity that aims to harm Israel. It should be ensured that outreach efforts are directed at all relevant target audiences, and in different languages. It is also recommended that the Elections Committee examine, in consultation with the entities dealing with the issue during an election period, and while conducting a legal review, whether and how a channel can be created to receive inquiries from the public, so that the information can be transferred to the entities responsible for handling the issue and with the

The need to prepare to deal with disinformation and fake news is also heightened in light of what is stated in the document on drawing lessons from the Chairman of the Elections Committee, Supreme Court Justice Yitzhak Amit, after the elections for the twenty-fifth Knesset that took place in 2022. The document details events that occurred on election day and highlights the enormous speed with which false news is spread on social media and from there to the established media outlets, while noting that the phrase "like wildfire" is too poor to illustrate the speed of the spread of false news. The document states that the lessons learned in this matter are that a rapid response team should be established to be at the disposal of the Central Elections Committee at critical junctures of election day until the publication of the final results, and to prepare in advance for the phenomenon of the spread of false news.

In February 2026, the Elections Committee informed the State Comptroller's Office that it believes that the main tool for dealing with the issue of malicious influence during an election period is through educating the public in digital literacy, while increasing its awareness of the possibility of attempts to manipulate public opinion in the digital space and providing basic tools for identifying false content and attempts at influence. The Elections Committee noted that in the 2026 budget proposal, the budget item designated for public information was significantly increased, in order to significantly expand information activities on the subject, including launching a campaign on this subject that will be directed at the widest possible target audience. The Elections Committee added that it intends to hold a seminar with civil society entities engaged in the detection and identification of false information in cyberspace.

In addition, the Elections Committee stated that it had approached the Minister of Education with a request that he examine the development and delivery of educational content adapted to school students, and especially to high school students, as part of school education classes or as part of community commitment hours, in which the students would serve as "mediating ambassadors" of the tools they had acquired and would disseminate them among senior citizens, and that a meeting on the subject had been coordinated.

ÿ

An election campaign is a particularly sensitive time for influence operations. International organizations such as the European Union and the World Economic Forum have emphasized that during this period, hostile actors are more motivated to launch influence operations due to the potential to influence voters' positions and undermine voters' confidence in the election results, and attempts at foreign influence have even been identified in various election campaigns around the world. The cancellation of the Romanian presidential elections at the end of 2024 due to suspicion of foreign interference illustrates the damage that can be caused by information manipulation on social media and poses another warning sign

The review revealed that despite the consensus regarding the potential for serious damage that may be caused by foreign influence in the digital space during an election period, the main focus on the issue occurs only near the elections, and as of July 2025, preparations to deal with the issue ahead of the elections for the Twenty-sixth Knesset, which are expected to be held in October 2026, have not yet begun.

The State Comptroller warned the Central Elections Committee, Shin Bet, the Cyber Directorate, the National Intelligence Organization, and the Ministry of Justice that the intensification of attempts at foreign influence in the digital space after the Iron Sword War and the serious risk posed by foreign influence during an election period require them to prepare in advance to deal with this threat and not wait until near the election period, when additional tasks are broug

In this regard, the Elections Committee must address the gaps that have arisen, formulate courses of action for dealing with various events, and examine, in consultation with the parties dealing with the issue during an election period, and while conducting a legal review, whether and how a channel can be created to receive inquiries from the public, so that the information can be passed on to the parties responsible for handling the issue and with the aim of enabling a rapid respons

The Shin Bet informed the State Comptroller's Office in January 2026 that it was taking steps to prepare for the matter.

The Elections Committee informed the State Comptroller's Office in February 2026 that the issue of foreign influence in the digital space had been on its agenda since 2019, and had received significant attention and investment of resources in all election campaigns since then. The Elections Committee noted that kick-off meetings were held with the relevant officials in the relevant bodies, in order to formulate, already in the current period, ten months before the election date set by law, the manner of cooperation between the Elections Committee and these bodies. The Elections Committee added that it was agreed to establish a special task force (STTF) consisting of representatives of the Elections Committee and each of the relevant organizations, to translate the attribution threats and attribution scenarios into a coordinated operational concept. In addition, the Elections Committee decided to establish a dedicated team, within the Elections Committee, which is currently being formed, to deal with the issue of foreign influence, and even initiated meetings with the major social media providers.

The Elections Committee noted that in addition to all of these, additional actions are planned for the elections, such as holding an administrative exercise in which situations of receiving false messages that could mislead the electorate or interfere with the election process will be practiced, and which require a quick and decisive response from the committee; the Elections Committee's preparations to establish a rapid response team that will include representatives of all relevant parties and will be part of the Election Day administration, the goal of which is to thwart false messages that could interfere with the fair conduct of the elections. The Elections Committee added that upon the announcement of the dissolution of the Knesset and the entry into the election period, the Chairman of the Elections Committee will convene all relevant security and regulatory bodies for a kick-off discussion for preparations for the elections. In this discussion, the main dilemmas, the main challenges, and the means to deal with them will be reviewed for all participants in order to coordinate the activities between the various bodies. The Elections Committee noted that it intends to advance this comprehensive meeting and hold it in the coming weeks.

The State Comptroller's Office notes the implementation of the aforementioned steps by the Elections Committee. However, given the possibility that the elections will also be held outside of their scheduled time, which has happened more than once, and since in recent years, and particularly after the Iron Swords War, there have been significant changes in the threat map and their intensity with regard to foreign influence in the digital space during an election period, including significant technological changes - a level of preparedness that will enable a rapid and orderly transition to a format that will allow immediate operation when necessary is required from all parties involved in the issue.

Summary

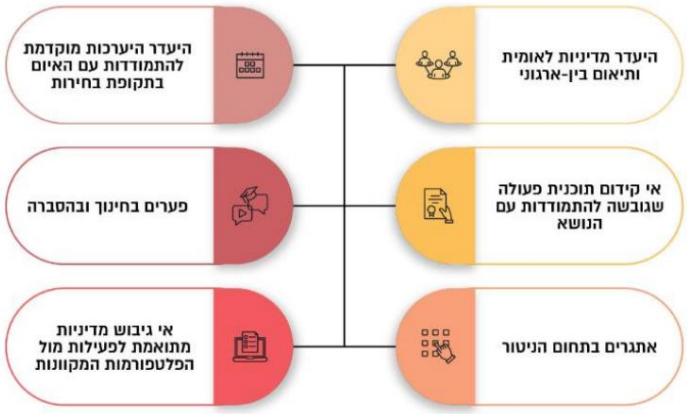
Foreign influence is the set of illegitimate actions by a foreign entity, which aim to covertly harm the interests of the state, to the point of fundamentally harming its sovereignty. In recent years, the use of the digital space for the purposes of foreign influence and the spread of disinformation by hostile entities has increased. Foreign influence poses a threat to the functioning of the democratic regime. Its purpose is to influence public opinion and decision-makers, create political instability, damage the social fabric and widen existing divisions in society, arouse panic and fear among the public, influence the results of elections and undermine public confidence in them.

Dealing with foreign influence in the digital space involves significant challenges. One of the main ones is the fear of harming freedom of expression, as sometimes discourse originating from foreign elements resonates and interferes with legitimate internal discourse.

Countries and organizations around the world have identified the threat of foreign influence in the digital space as a strategic risk. Since 2017, the need to deal with the threat of foreign influence directed against Israel in the digital space has resurfaced in Israel, as has the need for a holistic response and inter-organizational coordination to deal with t

With the outbreak of the Iron Sword War, attempts at foreign influence in the digital space intensified, but the situation reflected in this report shows that in the absence of a systematic directive and direction, there is no match between the threat and its intensification and the government response to it, and that there are significant deficiencies in dealing with the threat that have not been addressed for years. This includes initiatives that have been taken over the years to holistically deal with organizationally - were abandoned and did not embark on a real implementation path; an action plan formulated by the cyber division after the outbreak of the Iron Sword War was not examined by the Prime Minister for about a year and no decision was made on its matter; the situation regarding foreign influence efforts in the digital space is lacking - there are challenges in the field of monitoring that make it difficult to deal with the issue, and there is a certain difficulty in correctly assessing the scope of the phenomenon; there is a need to examine regulation and work interfaces with online platforms; despite the intensification of the risk and potential for damage during an election period, the bulk of the preparation for dealing with the issue takes place only near the elections; existing programs and lesson plans on the subject of disinformation in the Ministry of Education are offered as authorized content only, and there is no government entity responsible for informing and raising public awareness of this threat.

Figure 14: **Main gaps in the national struggle against foreign influence in the digital space**



The result is that the government's handling of this threat is deficient, and as of March 2026, there is no national policy on the subject and no government entity leading the fight against the threat of foreign influence in the digital space.

According to the National Security Staff Law, 2008, the role of the National Security Staff is, among other things, to propose to the Prime Minister an agenda and topics for discussion on foreign and security matters. In light of the intensification of the threat in the field of foreign influence, including in the digital space, given that for years no regular policy has been formulated regarding the leadership of the issue at the national level, and in light of the National Security Staff's position that it is appropriate to promote a government decision to establish a dedicated headquarters body with a dedicated budget to deal with the threat of foreign influence, including in the digital space, which will lead the examination of the issue and will integrate and synchronize the handling of all relevant ministries and bodies - it is recommended that the National Security Staff, in accordance with its authorities, propose to the Prime Minister an outline for leading the activity in the field of foreign influence that will serve as the infrastru

Additionally, in light of the challenges and difficulties raised regarding the detection and monitoring of attempts at foreign influence, it is recommended that the Shin Bet continue its efforts to improve the detection of attempts at foreign influence in the digital space.

Furthermore, in light of the definition of the risk of disinformation by a number of factors as one of the main risks in the coming years, and considering the technological development that blurs the ability to distinguish between truth and fiction, it is recommended that the Ministry of Education define content related to disinformation and critical thinking regarding content in the digital space as mandatory content in the education system in all its streams

Leaving the gaps and deficiencies raised in this report unanswered leaves the Israeli public exposed to foreign influence in the digital space without an adequate response, with all that this implies. In dealing with the threat, the necessary actions must be taken in advance to prevent devastating consequences for society.

This is even more true during times of crisis, war, and elections. Political and security instability, both domestic and regional, are fertile ground for local and foreign actors to exploit social divisions and undermine public trust in democratic institutions.

During this year, 2026, the State of Israel will hold an election campaign. The Knesset elections are the foundation of the democratic nature of the regime in Israel. An election campaign is considered a particularly sensitive period, in which the potential damage from attempts at foreign influence in the digital space increases significantly. This period may serve as a fertile ground for attempts to influence the agenda, the perception of reality, and decision-making, in a way that could skew the election results to the point of undermining public confidence in the election results. Given the intensification of the threat and the serious potential damage inherent in this, the Elections Committee must act to address the gaps that have been raised, formulate courses of action to deal with various events, and examine, in consultation with the parties dealing with the issue during an election period, and while conducting a legal review, whether and how a channel can be created to receive inquiries from the public, so that the information can be transferred to the parties responsible for handling the issue and with the aim of enabling a rapid response when necessary. The findings of this report, both in the context of the external and internal threat, must first and foremost be revis

Another aspect that must be taken into account is the rapid technological development, which means that attempts at foreign influence in the digital space are changing frequently, such as the increasing use of artificial intelligence. This requires monitoring these developments in order to provide an immediate response.

This report deals with dealing with foreign influence in the digital space directed against the Israeli public. However, attempts at foreign influence on Israel are not directed only at the Israeli public, but also at the international community, and this could seriously damage Israel's status, its legitimacy and its actions, and later even infiltrate Israeli discourse. The Israeli government must consider this aspect and the potential damage it entails.

It should also be noted that the digital space that this report focused on is just one of the spaces where attempts at foreign influence are being made, and the issue has only recently made headlines, including in Israel. This raises the need for a comprehensive examination of the issue of foreign influence in all its aspects and the establishment of a clear directive, while taking into account the necessary force and resource building, to ensure that the State of Israel is prepared to deal wit