Disinformation Campaigns and Influence on Cognition: Implications for State Policy

David Siman-Tov[1]

The Strategic Problem

In 2018, a working group at the Institute for National Security Studies (INSS) tackled the question of the cognitive campaign and the threat it poses to Western democracies.[2] Among the participants were representatives of government ministries, the IDF, and the intelligence community. The aim was to examine the challenges and opportunities that emerge in the internet age, in light of developments in recent years that create significant challenges for the State of Israel and for Western democracies in general.

The group's discussions focused on cognitive threats, mainly covert, that exist in the age of social media, first and foremost from foreign states. The discussions examined the issue of cognitive influence on the national level, both the defensive and offensive dimensions; conceptual and theoretical issues; and the need for organizational structuring of national policy in this field.

Foreign intervention in the elections in the United States and Europe, and in Western political discourse in general, which is attributed mainly to Russia, has led many democratic states to take steps in recent years aimed at addressing the new challenges posed by this intervention. These steps can serve as an educational resource and a model for implementation in Israel.

---

1 David Siman-Tov is a research fellow at INSS, specializing in intelligence, cyber challenges, and cognitive warfare.

2 The group was headed by David Siman-Tov, assisted by Nevo Brand, Pnina Shuker, and Mor Buskila. We would like to thank the representatives of the various government ministries who took part in the discussions and contributed their experience and knowledge.

The working group examined issues connected to both the defensive and offensive dimensions of the cognitive campaign. However, its main focus and efforts were directed toward the central challenge facing the State of Israel: the need to address defensively the threat to the country's democratic processes. The decision to focus on the defensive dimension stemmed from the fact that in Israel there are almost no institutions that deal with defense against the cognitive threat. There are, however, several institutions active in the overt and covert offensive cognitive dimension, though they too could benefit from improving their capabilities by joint management of campaigns, better conceptualization of threats, and joint buildup of forces.

Threat Reference: Cognitive Subversion

The working group discussed several possible threats. Some of the threats are related to election seasons, which is a sensitive period when social processes and trends, as well as the results of the elections themselves, can be influenced. Other threats are connected to periods between elections, which are generally easier to influence.

The potential threats to Israel include:

a. *Influencing the election process* with the insertion of particular contents, technological attacks, or a combination of the two, thereby attempting to deepen existing social rifts. As part of such a threat, one possibility is to promote a certain candidate or party in the elections. Another way is to encourage certain sectors to participate in the elections, or alternatively, to refrain from participating in them. These activities use contents and messages in a carefully designed language that make them seem authentic and influential on a certain well-defined target audience that may make a difference on the election results.
b. *Undermining public confidence in democratic institutions*: Liberal democracies depend on the existence of governing institutions and civil society. The dissemination of false information regarding the behavior of figures in the democratic system can damage public confidence in democratic institutions and in the democratic process in general, and undermine the very existence of democracy. Non-participation in elections is one possible expression of such damage to public confidence.
c. *Influencing the public's positions on strategic issues*: The dissemination of false and biased information on strategic issues can undermine citizens'

perceptions of these issues. Distorting the public's perception of reality in the democratic system can influence decision making processes in democratic regimes, in light of the need to receive public legitimacy for these decisions. For example, fake Iranian news sites have aimed to influence Israeli discourse and the way the Israeli public sees Hezbollah. This could be just the tip of the iceberg that indicates a comprehensive effort by Iran, Hezbollah, or Hamas to influence the discourse in Israel. Similarly, Russia's interest in influencing the way the Israeli public sees its standing in the region must be considered, especially when it has many tools for realizing these interests.

d. *Influencing the Israeli economy*: It is possible to influence the Israeli economy through rumors, combined with offensive cyber operations. These could harm various economic interests and targets.

Main Concepts

Cognition / *Consciousness* – public opinion and beliefs, or the opinions of decision makers, that a certain party wishes to influence. There are many ways to influence cognition, from psychological warfare to public relations and advocacy, as well as public diplomacy and kinetic actions. Cognition is also shaped by exposure to unplanned processes and mindsets.

Cognitive campaign – a set of actions using overt and covert methods to influence broad target audiences and decision makers. These actions are united by their shared goal of influencing cognition, and can be achieved simultaneously or gradually. Actions intended to influence cognition generally distinguish between different target audiences: for example, intelligence agents operate among external targets; the Ministry of Foreign Affairs operates within the international system; the IDF Spokesperson operates mainly within the Israeli public. At the same time, messages permeate and pass through different audiences, and different parties operate within several target audiences simultaneously. This situation requires systemic understanding of all of the parties, central management of campaigns, and coordination between the bodies engaged in influencing cognition or preventing such influence.

Strategic Communications (SC) entails the long term shaping and shifting of significant discourses, adoption of a holistic approach to communications aimed at changing the attitudes and behavior of targeted audiences to achieve

strategic effects, and the use of words, images, actions, and non-actions in pursuit of national interests. On the one hand, there is little new in the phenomenon of SC as an activity designed to achieve political aims. On the other hand, the information revolution, which led to the proliferation of the internet and the subsequent rise of social media, has completely reshaped the information environment, creating new challenges and threats for national security apparatuses in general, and strategic communications in particular.

Cognitive subversion – covert and classified information operations carried out against a sovereign state in order to widen existing rifts, undermine public confidence in society's institutions, and increase tensions with different societies and entities in the international arena. Such operations attempt to influence the nature of the state and its society, its stability, and its decision making processes.

Western Countries in the Face of Attempts to Disrupt the Democratic Process

Western democracies have come to understand that the threat of cognitive subversion in the information domain must be addressed. As a result, counter efforts have begun, mainly but not only surrounding the threats attributed to Russia, and these efforts are relevant to threats from other countries and domestic threats as well.

Examples of such efforts can be found in different actions taken or considered by states, social media companies, and even civil society. The lessons learned in the West following attempts at intervention and influence over elections in recent years have led countries to prepare both to defend the public discourse on the eve of elections and to defend the voting systems themselves. At the same time, concerns in the West are not limited to influence over elections; they are broader, and connected to the understanding that efforts to undermine Western democracies are not limited to election processes, but include ongoing efforts to expand social rifts in order to undermine public confidence in the state's institutions and in the democratic system as a whole.

State Organizations

The following are among the most prominent examples of international organizations established to deal with cognitive influence efforts.

The *United States* established the Global Engagement Center within the State Department to lead, synchronize, and coordinate the administration's efforts to expose propaganda activities by foreign states that attempt to undermine US national security. By encouraging activity that integrates governmental organizations and private sector organizations, the organization focuses on technology, interpersonal involvement, the involvement of partner organizations in the exposure process, and content production.[3] For example, in 2017 and 2018 the Department of Defense transferred $60 million to the Global Engagement Center, and also allocated $5 million in grants to private and public organizations through the Information Access Fund. In addition, there are collaborations between the United States and Europe, for which $1.3 billion were budgeted by the State Department in 2017 to help strengthen European resilience in the face of Russian intervention.[4] The FBI has also established a mechanism for fighting against disinformation, to create the capability to respond quickly to foreign influence operations and to conduct ongoing dialogue with the rest of the organizations active on this issue, in order to integrate tactics and techniques from different clearance levels.[5]

United Kingdom: In March 2018, the UK's National Security Council announced in its *National Security Capability Review* that it intends to expand its National Security Communications Team significantly and make it a government-wide team. The team will take an inter-ministerial approach to implementation of objectives, as an integral part of the British government's approach toward the issue of national security in communications. The team

---

3 Global Engagement Center, US Department of State, https://www.state.gov/r/gec/.

4 Nicole Gaouette, "US State Department Yet to Spend Funds Allocated to Fight Russian Meddling," *CNN*, March 5, 2018, https://edition.cnn.com/2018/03/05/politics/state-russia-counter-propaganda-funds/index.html.

5 Elizabeth Bodine-Baron, Todd C. Helmus, Andrew Radin, and Elina Treyger, *Countering Russian Social Media Influence* (Santa Monica, CA: RAND Corp., 2018), https://www.rand.org/pubs/research_reports/RR2740.html; Alina Polyakova and Spencer P. Boyer, *The Future of Political Warfare: Russia, The West, and the Coming Age of Global Digital Competition* (Washington, DC: Brookings Institution, 2018), p. 3; Kara Fredrick, "How to Defend against Foreign Influence Campaigns: Lessons from Counter-Terrorism," *War on the Rocks*, October 19, 2018, https://warontherocks.com/2018/10/how-to-defend-against-foreign-influence-campaigns-lessons-from-counter-terrorism/.

will also address the issue of disinformation and the challenges involved in the transition from the world of traditional media to the internet age.[6]

Australia: Following repeated warnings from the Australian intelligence community regarding expected intervention by China in the federal elections of July 2018, the Electoral Integrity Task Force was established with the purpose of taking action against cyber risks to the country's election process. The task force is led by the Department of Home Affairs and includes representatives of Australian intelligence and the Australian Federal Police.[7]

Belgium: In early May 2018, the Belgian Minister of Digital Agenda announced two initiatives whose objective is to prevent the spread of disinformation on the internet. The first is the establishment of a committee comprising journalists and academics to formulate solutions to the threat; the second is the establishment of a site that can update and inform citizens regarding actions to counter disinformation and create a mechanism for expressing support or opposition to ideas for coping with disinformation through the use of upvoting and downvoting buttons. This aims to help citizens express their satisfaction with various suggestions for coping with the phenomenon of disinformation.[8]

Denmark: In its 2017 public report, the Danish intelligence community presented the threat of Russian disinformation as a significant and developing threat.[9] Following the report, an inter-ministerial task force was established that synchronizes between the branches of the Danish government and intelligence organizations, as part of an effort aimed at preparing all systems for the 2018 elections. To this end, the Danish government formulated an 11-stage plan aimed at addressing the threat. [10]

---

6 *National Security Capability Review*, HM Government, March 2018, https://bit.ly/2HnHafL.

7 "Anti-Meddling Task Force Set Up Ahead of Australian By-elections," *SBS News*, June 9, 2018, https://www.sbs.com.au/news/anti-meddling-task-force-set-up-ahead-of-australian-by-elections.

8 "How to Stop Fake News? – Debate," May 2018, https://monopinion.belgium.be/processes/stopfakenews/f/81/?locale=fr [in French].

9 *Intelligence Risk Assessment 2017*, Danish Defense Intelligence Service, FE, November 2017, https://bit.ly/2TcGW5l.

10 "Strengthened Safeguards against Foreign Influence on Danish Elections and Democracy," Ministry of Foreign Affairs of Denmark, September 7, 2018, https://bit.ly/2U0aHmR.

Legislation

Various legislative processes related to addressing the threat of disinformation have taken place in several countries.

In *Canada*, a bill was passed that designates a certain period of time before each federal election in which restrictions are placed on the amount of spending by political parties and interest groups that are part of the election process. These bodies will be required to include an identifying tagline that reflects the identity of the advertiser in published advertisements. Election officials will be entitled to block the dissemination of false information. During this period, it will also be prohibited to disseminate misleading information on sponsors and to accept election advertisements paid for by foreign entities.[11]

In the *United States*, Congress passed a law to improve the ability to address false information by preventing propaganda and disinformation by foreign entities. The law went into effect in late 2016, and it is part of the national effort to address foreign influence on consciousness.[12] In addition, the California Senate formulated a bill prohibiting the use of online bots, which went into effect on July 1, 2019.[13]

Germany: In June 2017, a law was passed to fight against the spread of disinformation and hate speech on the internet. The law states that companies that are active on social media are obligated to remove disinformation that foments hatred and other criminal content within 24 hours. The fine for this crime is approximately 50 million euros.[14] Note that this is very unusual and highly controversial legislation.

---

11 Aaron Wherry, "Trudeau Government Proposes Major Changes to Elections Law," *CBC*, April 30, 2018, https://www.cbc.ca/news/politics/trudeau-elections-scott-brison-legislation-1.4641525.

12 Craig Timberg, "Effort to Combat Foreign Propaganda Advances in Congress," *Washington Post*, November 30, 2016, https://wapo.st/2fOuXTU.

13 "Bots: Disclosure," Senate Bill No. 1001, September 28, 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001; Richard B. Newman, "California Enacts Anti-Bot and IoT Laws," *National Law Review*, October 4, 2018, https://www.natlawreview.com/article/california-enacts-anti-bot-and-iot-laws.

14 "Germany Starts Enforcing Hate Speech Law," *BBC News*, January 1, 2018, https://www.bbc.com/news/technology-42510868.

In *France*, President Macron announced that he intends to pass a law that would prevent the spread of fake news on the internet, especially during elections.[15]

Civil Society and Public Education on Digital Awareness

Various bodies that are part of civil society have taken a series of actions connected to addressing the phenomenon of disinformation and false information.

DFRLab (Digital Forensic Research Lab) is an organization that operates on behalf of the Atlantic Council and is composed of a network of forensic researchers, whose purpose is to identify, expose, and explain disinformation activities, advance "objective truth," and prevent digital subversion of democratic institutions and norms. The organization exposes false narratives and stories in cooperation with the technology journal *Medium*.[16]

First Draft News is an organization in the Shorenstein Center at Harvard University, which initiated the CrossCheck project, whose purpose was to monitor information surrounding the presidential elections in France in 2017 and to report nonfactual or unreliable information to the public.[17] The project included a joint effort by 37 traditional media and digital media organizations, including Facebook, Google, and *Le Monde*. In this context, there was also a report by the strategic research institute of the French Ministry of the Armed Forces that summarizes ways of coping with disinformation attacks waged during the 2017 French presidential elections. The report emphasizes the centrality of civil society in defending against influence operations.[18]

IREX initiative is an initiative designed to provide Ukrainian citizens with tools to distinguish between true and false information in order to enable them to form their opinions without falling victim to manipulations. The

15 Angelique Chrisafis, "Emmanuel Macron Promises Ban on Fake News during Elections," *The Guardian*, January 3, 2018, https://bit.ly/2COmWvj.

16 The Atlantic Council, 2018, https://www.digitalsherlocks.org/about.

17 "CrossCheck, A Collaborative Journalism Project," https://crosscheck.firstdraftnews.org/france-en/.

18 Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, and Janaina Herrera, *Information Manipulation: A Challenge to Our Democracies*, Report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, 2018, p. 13.

initiative operates in collaboration with the Academy of Ukrainian Press and with the StopFake organization, and has put together a study program for media literacy so that the public can consume information in a clear-eyed and critical manner.[19]

Cooperation with Existing and New Media Companies

The processes pursued by different countries have also led to a series of steps with regard to the role of media companies, including cooperation with governments, to prevent the spread of false information and disinformation on the internet:

France: Ten days before the first round of the presidential elections in 2017, Facebook took action, in cooperation with the French government, to remove 30,000 accounts. This cooperation was due to increased pressure and threats by European governments to legislate laws and set regulatory standards against media companies in case they would fail to take action to remove disinformation and inciting content from the internet.

In the *United States* the administration issued a reminder to the media that "the dissemination of false information is a violation of criminal law."[20]

Germany: German legislation against disinformation and incitement on the internet led Facebook to join forces with the German media in order to assess jointly information dissemination on the internet. In addition, the company created a mechanism that enables the media to identify false stories spread on the internet, based on reports made by the public.[21]

---

19 Mehri Druckman, "Media Literacy: Defeating Disinformation through Education – Ukraine on the Global Fake News Frontlines," *Business Ukraine News*, August 12, 2018, https://bit.ly/2BMp5Z2.

20 Polyakova and Boyer, *The Future of Political Warfare*, p. 3; Erik Brattberg and Tim Maurer, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks," Carnegie Endowment for International Peace, May 23, 2018, https://bit.ly/2QdjD6Z; Fredrick, "How to Defend Against Foreign Influence Campaigns."

21 Laurens Cerulus, "Germany's Anti-Fake News Lab Yields Mixed Results," *Politico*, July 17, 2017, https://www.politico.eu/article/fake-news-germany-elections-facebook-mark-zuckerberg-correctiv/.

The Challenge of Foreign Influence on Israel: A Defensive Perspective

Over the past 15 years there has been extensive attention in Israel to the challenges of cognition and consciousness, evidenced by the establishment of the Center for Cognitive Operations (Malat) in the IDF; the strengthening of the IDF Spokesperson's Unit; the establishment of a national center for public diplomacy within the Prime Minister's Office; the political campaign against Iran's nuclear program, which was based mainly on intelligence; the systemic activity by the Ministry of Strategic Affairs and civil society organizations against the threat of BDS; and public diplomacy to prepare the home front for a conflict. At the same time, preparations have not been made for the possibility of hostile influence on the public discourse and on democratic processes in Israel, most importantly the Knesset elections. This is despite the fact that there is greater awareness of cognitive subversion and possible intervention in elections.

In this context, the IDF Chief of Staff raised concerns in the Knesset about foreign intervention in Israeli democratic processes[22] and even presented it as a central challenge, noting two related phenomena: possible attempts to influence the results of general elections by falsifying them through cyberattacks; and waging campaigns to influence the consciousness of voters through mass manipulation via posts on social media and websites.[23] A Knesset discussion in June 2017 emphasized the need to deal with content distributed on such sites and networks and to address the planting of false information (and not just the technological aspects), and noted that Israel needs to take into consideration foreign intervention that attempts to influence the election results.[24] Former head of the Mossad Tamir Pardo likewise stated that the

22 Amos Harel, "Eisenkot Warns MKs of Foreign Intervention in Israeli Elections," *Haaretz*, July 9, 2017, https://www.haaretz.co.il/news/politics/.premium-1.4236932 [in Hebrew].

23 Amos Harel, "Cyber Directorate Formulates Plan for Defending against Foreign Intervention in Israeli Elections," *Haaretz*, July 13, 2017, https://www.haaretz.co.il/news/politics/.premium-1.4255146 [in Hebrew].

24 "The Dissemination of False Information and Cyberattacks to Influence the Elections," Meeting of the Science and Technology Committee, Protocol no. 118, June 12, 2017; "Meeting with Representatives of Information Security and Cyber Companies," Meeting of the Foreign Affairs and Defense Committee's Subcommittee for Cyber Defense, Protocol no. 20, May 2, 2018 [in Hebrew].

central danger facing states is "disintegration from within," and it could occur in light of efforts by foreign entities to influence the public discourse.[25]

In contrast, figures connected to the National Cyber Directorate have underscored that this organization should not deal with content connected to the elections and that it does not intend to take action to thwart cognitive campaigns by dealing with content. Nonetheless, in a discussion held in the Knesset, the National Cyber Directorate reported on cooperation with Facebook to remove fake profiles. This cooperation met with criticism on the part of the President of the Israel Internet Association, in which it was claimed that the National Cyber Directorate is not authorized to address this issue, even indirectly.[26]

State-level efforts to address false information and attempts to influence people's perceptions in advance of the Knesset elections are reflected in the establishment of a "special elections committee" led by the National Cyber Directorate, with the participation of security officials and the Ministry of Justice. The committee meets regularly, learns from the experience of foreign countries, formulates responses, and conducts exercises with relevant bodies, such as the Central Elections Committee and additional bodies within the political and civil system (for example, polling companies). The committee's activity is a significant improvement in the State of Israel's preparedness against threats of disruption to the democratic process. That said, this preparedness is only in the context of the elections, with an emphasis on technological intervention. It does not address other threats detailed above, nor does it include civil society in its responses, as is the case in other countries.

Just as Western countries see cognitive subversion as a strategic threat and have begun efforts to counter it, Israel should follow their lead and customize the right solution for itself. The desire to preserve Israeli democracy must be the aim driving the development and implementation of efforts against cognitive subversion. The way to cope with the natural tension that exists with civil society groups is to include them in the solution. Their inclusion will serve as a counterweight that restrains the state's actions against this threat.

---

25 "Countries Will Start Disintegrating from Within," *Arutz Sheva*, December 24, 2018, https://www.inn.co.il/News/News.aspx/389858 [in Hebrew].

26 Omer Kabir, "Thousands of Fake News Accounts Exposed that Tried to Influence the Israeli Municipal Elections," *Calcalist*, October 15, 2018, https://www.calcalist.co.il/internet/articles/0,7340,L-3747647,00.html [in Hebrew].

In order to address the emerging threat of cognitive subversion, the State of Israel must first define what it wants to defend (for example, democratic discourse without hostile foreign intervention), and on this basis, clarify when intervention in the public discourse is illegitimate and when it is legitimate. A possible boundary for defining these threats is when they are not visible and take place covertly. Such a boundary is important in order not to harm the freedom of expression.

Recommendations

a. *Creating a cognition committee/directorate*. Counter efforts against cognitive subversion require cooperation between a large number of bodies, as well as the inclusion of civil society. Therefore, it is recommended that a permanent inter-ministerial committee be established (perhaps within the Prime Minister's Office) that would include representatives of the intelligence community, the National Cyber Directorate, and relevant government ministries, along with representatives of civil society. The committee would carry out a risk assessment before significant events, such as Knesset elections, and formulate overall policy with government ministries, relevant companies, and civil society. It is recommended that in the initial stage the committee discuss defensive aspects of cognitive operations. In the future there could also be room to examine offensive aspects, which are not discussed in this document. In effect, this would be an expansion and institutionalization of a committee established by the National Cyber Directorate, the Israel Security Agency, and the Ministry of Justice.
b. *The integration of the intelligence community*. The intelligence community is an important component for responding to new threats, as it naturally focuses on the covert realm, which is the likely domain for foreign entities that are interested in illegitimately influencing the discourse. The intelligence community also has the ability to thwart such intervention. Currently, the intelligence community barely sees the threat of influencing cognition as its responsibility, which creates difficulties in identifying the threat (if it exists) and understanding it in depth. Recruiting it to identify and thwart threats is a critical element of the state's response.
c. *Examining the need for legislation against the new threat*. There is currently difficulty in determining which law (if any) is necessary in

order to defend against the new threat, and whether legislation is indeed the solution. In any case, it is important to learn from the experience of others and examine this possibility, with the requisite caution.

d. *Involving civil society*. Groups within civil society naturally have concerns about the state's involvement in the content of discourse and about harm to freedom of expression and civil rights. On the other hand, it is important to enable democracy to defend itself. One of the ways to deal with this tension is by involving the public in coping with the challenge. This can take place by encouraging the engagement of civil society organizations (for example, by identifying false news). Maintaining a constant dialogue with civil society groups can help calm the tensions and reduce possible opposition to necessary steps.
e. *Educating the public and relevant sectors within it* (such as journalists and opinion leaders in social media) to address the attempts to manipulate the discourse. In this framework, it is important to raise awareness about the phenomenon of attempts to influence consciousness and to develop ways to cope with them, through public education and developing civilian digital competence.
f. *Increasing cooperation with media companies*. New media companies have control over the content provided on their platforms, and they can monitor and screen suspicious users. A mechanism needs to be created for sharing information that will enable media companies to implement preventive measures at an early stage, instead of dealing with influence efforts after they have been posted on the internet and disseminated on it.[27] In addition, dialogue should also be developed with regular media networks in a way that encourages controlling the entry of illegitimate information into the public discourse.
g. *Carrying out a market survey of technologies that can prevent foreign interference in the discourse*. Israel, as a technology giant, can lead in this area too and make a global contribution.

27 Bodine-Baron, Helmus, Radin, and Treyger, *Countering Russian Social Media Influence*.