Defending against Influence Operations: The Challenges Facing Liberal Democracies

Gabi Siboni and Pnina Shuker[1]

Introduction

At the end of November 2017, government ministers Gilad Erdan and Ayelet Shaked initiated the "Facebook Law," according to which the Courts for Administrative Matters may, at the request of the state, issue an order that instructs internet content providers, such as Facebook, Twitter, and Google, to remove inciteful content.[2] The bill was tabled after figures involved in the legislation's proceedings warned that the content of the law was too broad and endangered individual rights and Israeli citizens' freedom of expression.[3]

Liberal democracies[4] are open to disagreements, political competition, and oppositional organizing. These characteristics, which are the basis of democracy, provide anti-democratic forces and those hostile to the state with a convenient platform to exploit in order to undermine the existing political order.[5] While attempts by states to shape the consciousness of the population

1 Dr. Gabi Siboni is the head of the Military and Strategic Affairs Program and the Cyber Security Program at INSS. Pnina Shuker is a Neubauer research associate at INSS and a PhD candidate in the Political Science Department at Bar Ilan University.

2 Rafaella Goichman, "Facebook Law on the Way to Approval – Passes First Reading," *The Marker*, January 3, 2017 [in Hebrew].

3 Uri Berkovitz, "Netanyahu Orders Stop to the Facebook Law – Endangers Freedom of Expression," *Globes*, July 18, 2008 [in Hebrew].

4 A form of government based on free elections, separation of powers, and the limitation of the executive branch through laws and basic values in order to defend civil rights.

5 Eran Zaidise, Ami Pedahzur, and Arie Perliger, "Existential Threats to Democracies," *Politics* (Winter 2010): 39-40 [in Hebrew].

of another state and influence their opinions are not new, the information revolution has intensified them. Since the Russian interference in the US presidential elections in 2016, there has been increasing recognition that authoritarian regimes are making unprecedented use of social media both in order to suppress and rule their populations and to disrupt and harm democratic rivals in the West.[6] Defending against such actions requires counteractions, which could involve harming basic rights and freedoms. The tension between maintaining democratic values and effectively defending against foreign attempts at subversion is a significant challenge for liberal democracies.

This article seeks to examine the difficulties facing liberal democratic states in defending against influence operations by foreign entities. The article also offers possible ways of addressing these challenges.

Influence Operations

An influence operation is a coordinated, integrated, and synchronized application of diplomatic, information, military, economic, and other national capabilities during times of peace, crisis, conflict, and post-conflict. The purpose of the influence operation is to affect the behaviors or decisions of foreign target populations, so that they adopt positions that match the interests of the operation's initiators.[7] In the doctrines of states and non-state organizations, an influence strategy is seen as part of a multi-channel systemic approach, sometimes known as information warfare or cognitive warfare. This strategy aims to manipulate actors to behave in a desired way, sometimes against their interests, through actions that influence and distort their picture of reality and the use of various kinds of leverage. These actions are directed at decision makers and additional target audiences, during both peace and wartime.[8]

---

6 Clint Watts, "Advanced Persistent Manipulators and Social Media Nationalism: National Security in a World of Audiences" (Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1812, September 18, 2018), pp. 1-2, https://www.hoover.org/sites/default/files/research/docs/watts_webreadypdf.pdf.

7 Eric V. Larson and others, *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities* (Santa Monica, CA: RAND Corp., 2009), p. 2.

8 Dima Adamsky, "The Russian Approach to the Art of Cyber Operations," chapter

The manipulation of information for political or diplomatic purposes has existed throughout human history. However, the technological improvements that have occurred since the invention of the internet and the use of cyberwarfare by state and non-state actors provide new capabilities and add elements that did not exist in the past. State and non-state actors now use cyberspace in general and social media in particular as a tool for generating social and political changes and shaping cognition. Social networks enable users to create and develop connections, engage in discourse, and, in effect, turn the internet and social media from technological tools into a space where full interaction takes place on various topics, including politics and elections.[9]

In recent years, liberal democracies have been subjected to attacks of cognitive operations by a variety of actors, mainly states with authoritarian regimes, led by Russia, China, and Iran.[10] Russia is a central player in the international system that uses influence operations as one of its main non-military methods against rivals in order to achieve its objectives. Russia has a long tradition of activity in this area, and it has a coherent theory and operational capabilities for practical application.[11] Russian information warfare has a number of objectives, including undermining Western criticism of Russia; achieving legitimacy for Russian policy; reinforcing Russia's image as a major European power;[12] undermining the West's solidarity by

2, in "Cyber Operative Art: A Look from the Viewpoint of Strategic Studies and in Comparative Perspective," *Eshtonot* 11, Research Center, National Defense College (2015): 28-48 [in Hebrew].

9 Karine Nahon and Shira Rivnai, "Election Propaganda in the Context of the Internet and Social Media," background information for the Beinish Committee, January 2016 [in Hebrew]. The Beinish Committee was established in 2015 in order to examine the suitability of the Elections Law (Propaganda Methods) in the age of the internet and social media.

10 An authoritarian regime is characterized by the lack of separation of powers and the lack of limits on government through laws or basic values. The type of government in such regimes includes single-party regimes (sometimes only in practice), oligarchies, monarchies, and military regimes. Examples include Russia, China, Iran, and North Korea.

11 Adamsky, "The Russian Approach to the Art of Cyber Operations."

12 S. Hutchings and J. Szostek, "Dominant Narratives in Russian Political and Media Narratives During the Ukraine Crisis," in *Ukraine and Russia: People, Politics, Propaganda and Perspectives,* ed. A. Pikulicka-Wilczewsk and R. Sakwa (Bristol: E-International Relations, 2015), p. 185.

supporting European parties that oppose the European Union; and supporting extreme political movements in Europe.[13] Among the Russian methods of operation in the field of cognitive operations, we can see the dissemination of information on social media by fictitious profiles, along with the acquisition of news agencies in order to disseminate false and manipulative information.

In January 2017, the American intelligence community published a report on Russia's attempts to disrupt the US presidential elections in 2016.[14] The Russian operation included the dissemination of disinformation on social media with the intention of deepening existing disputes within American society and undermining confidence in Western institutions and in the democratic process using bots, trolls, and the activities of hackers.[15] That same year saw additional Russian attempts to interfere in the elections in Europe. In one instance, bots and trolls attempted to disseminate false information about French presidential candidate Emmanuel Macron on the internet.[16] Similar attempts were made a year earlier in the United Kingdom during the referendum on separating from the European Union.[17]

China also has aspirations to influence in many places in the world.[18] A classified report ordered by the Prime Minister of Australia revealed efforts by the Chinese Communist Party to influence all levels of government in Australia

13 Marcel H. V. Herpen, *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy* (Lanham: Rowman and Littlefield, 2015); P. Pomerantsev, "Authoritarianism Goes Global (II): The Kremlin's Information War," *Journal of Democracy* 26, no. 4 (2016): 40-50.

14 Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," January 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

15 A. Robertson, *Global News: Reporting Conflicts and Cosmopolitanism* (New York: Peter Lang, 2015), p. 113; Elizabeth Bodin-Baron, Todd C. Helmus, Andrew Radin, and Elina Treyger, *Countering Russian Social Media Influence* (Santa Monica, CA: RAND Corp., November 1, 2018).

16 Adam Nossiter, David E. Sanger, and Nicole Perlroth, "Hackers Came, but the French Were Prepared," *New York Times*, May 9, 2017.

17 Karla Adam and William Booth, "Rising Alarm in Britain over Russian Meddling in Brexit Vote," *Washington Post*, November 17, 2017.

18 Erica Pandey, "How China Became a Global Power of Espionage," *AXIOS*, March 23, 2018.

for over a decade.[19] Recently, there have been more reports of China's efforts to intervene in the United States too. In November 2018, President Trump announced that China sought to influence the results of the midterm elections to Congress and positions in various states.[20] Around two weeks before election day on November 6, 2018, the American administration announced that Iran, Russia, and China were trying to undermine the democratic process through an online propaganda campaign, which included the use of social media and fictitious identities, aimed at deepening ideological rifts and spreading disinformation about the candidates in order to fan the flames of disagreements on major issues.[21]

In August 2018, Twitter and Facebook erased hundreds of accounts suspected of being connected to an Iranian disinformation campaign.[22] The content posted on these accounts aimed to highlight issues and narratives that suited Iranian foreign policy and advanced anti-Saudi, anti-Israeli, and pro-Palestinian issues, as well as seeking to generate support for US foreign policy that would serve Iranian interests on certain issues, such as the nuclear deal between Iran and the world powers in 2015.[23] In addition, at the end of October 2018, a network of Facebook pages based in Iran was exposed that aimed to influence public opinion in the United States and the United Kingdom.[24]

At the beginning of September 2018, an Israeli cyber company exposed Iranian websites aimed at the Israeli public. The sites exposed are part of a worldwide disinformation infrastructure created by Iran over the years, which includes over 100 news and media websites that are active in 24 countries and

---

19 Tara Francis Chan, "A Secret Government Report Uncovered China's Attempts to Influence all Levels of Politics in Australia," *Business Insider*, May 28, 2018.

20 Abigail Grace, "China's Influence Operations Are Pinpointing America's Weaknesses," *Foreign Policy*, October 4, 2018.

21 "Concerns in the United States: Russia, China, and Iran Trying to Intervene in Midterm Elections," *Ynet*, October 20, 2018 [in Hebrew].

22 Craig Timberg, Elizabeth Dwoskin, Tony Romm, and Ellen Nakashima, "Sprawling Iranian Influence Operation Globalizes Tech's War on Disinformation," *Washington Post*, August 21, 2018.

23 Ariane M. Tabatabai, "A Brief History of Iranian Fake News: How Disinformation Campaigns Shaped the Islamic Republic," *Foreign Affairs*, August 24, 2018.

24 "Facebook Fights Fake News from Iran: 'We've Eliminated a Propaganda Network – A Million Users Were Exposed,'" *The Marker*, October 27, 2010 [in Hebrew].

29 languages, with hundreds of social media profiles supporting these sites.[25] In January 2019, Shin Bet Director Nadav Argaman warned of "intervention by a foreign state" in the upcoming Israeli elections of April 2019.[26]

The threat of influence operations extends beyond these examples. The development of technological means and the declared aspirations of Russia and China to lead research on artificial intelligence will force liberal democracies to contend with increasing threats from influence operations.

The Challenges of Liberal Democracies in Defending against Influence Operations

Sometimes there is a clash between basic democratic values and the actions and steps that democracies take out of a desire to strengthen their national security. A threatened democracy tends to see security as a supreme value, and its security needs sometimes lead it to limit democratic processes and civil freedoms.[27]

Effectively coping with influence operations in liberal democracies raises the question of what is prohibited influence and what tools can be used to cope with them within the democratic rules of the game. For example, censoring content on the internet or blocking the internet in general are inconsistent with democratic values. The critics of these methods claim that removing propaganda from the internet is undemocratic and blocking for political purposes leads to censorship, which could remain permanently in place. Secretary General of the Council of Europe Thorbjørn Jagland even expressed concerns that blocking, filtering, and removing materials from the internet could harm the freedom of expression: "Governments have an obligation to combat the promotion of terrorism, child abuse material, hate speech and other illegal content online. However, I am concerned that some states are not clearly defining what constitutes illegal content. Decisions are

25 Assaf Golan, "Iranian Propaganda Network with Fake News Sites in Hebrew Exposed," *Israel Hayom*, September 6, 2018 [in Hebrew].

26 "Shin Bet Director: A Foreign State Plans to Interfere in the Upcoming Israeli Elections," *Globes*, January 8, 2019 [in Hebrew].

27 Benjamin Neuberger, "National Security and Democracy – Tensions and Dilemmas," in *Democracy and National Security in Israel*, eds. Ilan Ben-Ami and Benjamin Neuberger (Raanana: Open University, 2007), p. 7 [in Hebrew].

often delegated to authorities which are given a wide margin for interpreting content, potentially to the detriment of freedom of expression."[28]

Liberal democracies are committed to the rules of state responsibility and activity within the framework of the law. They are characterized, in part, by the lack of internal agreement, which prevents the formulation of uniform messages, and by bureaucratic and political unwieldiness that delays learning and change processes. Liberal democracies are also exposed to leaks and subjected to oversight and supervision by the media, while the knowledge infrastructure and manpower that they devote toward handling the cognitive campaign are usually insufficient. In contrast, authoritarian regimes do not hesitate to carry out media manipulations and are hardly committed to significant public oversight. In some authoritarian regimes, influence operations and active measures are an inseparable part of their domestic and foreign policy. In contrast, democratic states have to manage their influence operations under political, legal, and media oversight.[29]

Liberal democracies are based on the principle of the nation's sovereignty. The nation's sovereignty is expressed first and foremost through free general elections at intervals determined by law. Elections are seen as the peak of the democratic process, expressing civil participation and constituting a central element of building public confidence in the state and its institutions. Due to the deep significance of elections in democratic states, damage to the election process or any external interference can have severe consequences. During the past few years, various attempts have surfaced to harm the democratic election process, using different tools in cyberspace. These include the use of technological tools to harm information systems that are used in voting processes, along with external attempts to influence the public's confidence in candidates and democratic institutions or its opinions toward them.[30] The commitment of democracies to allow their citizens free discourse poses a

---

28 Maria Hellman and Charlotte Wagnsson, "How Can European States Respond to Russian Information Warfare? An Analytical Framework," *European Security* 26, no. 2 (2017): 162.

29 Peter Mattis, "Contrasting China's and Russia's Influence Operations," *War on the Rocks*, January 16, 2018.

30 Knesset – Research and Information Center, "The Dissemination of False Information on the Internet and Cyberattacks to Influence the Elections," Jerusalem, 2017 [in Hebrew].

substantial challenge for them – coping with fake news. The current era highlights this challenge immensely, as in the current political and media reality identifying false information and removing it from the internet is considerably difficult.[31]

We can identify two central problems facing democracies in their defense against influence operations. The first is the need to identify foreign attempts to disseminate false information. There is sometimes considerable difficulty in distinguishing between internal and legitimate discourse on the internet, which includes authentic opinions and points of view, and on the other hand, discourse, opinions, and viewpoints planted by foreign entities.[32] The second problem is the limited tools at the disposal of liberal democracies in defending against influence operations. It is true that states have the ability to act immediately and forcefully, as in the case when the Chinese government blocked the use of the messaging application WhatsApp in China in 2017.[33] Nor are there disagreements about the fact that "the important right to freedom of expression can be denied, based on the public interest, when there is a 'near certainty' that the exploitation of this right in a certain situation could endanger public safety or national security."[34] Nonetheless, the question remains when the denial of the freedom of expression is justified for security reasons. In light of the difficulty in reaching conclusions on this issue, democratic states prefer not to use these methods at all.[35]

Possible Ways of Coping

The State of Israel, since its establishment, has been a "defensive democracy." This kind of democracy is defined by political scientists as "precluding the full application of the democratic rules of the game to groups whose activities or positions are seen as threatening the state or the political regime or the

31 Avshalom Halutz, "In the Post-Truth Era," *Haaretz*, November 19, 2016 [in Hebrew].

32 Todd C. Helmus et al., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe* (Santa Monica, CA: RAND Corp., 2018), p. 68.

33 Yoav Stoler, "China Completely Blocks WhatsApp," *Calcalist*, September 26, 2017 [in Hebrew].

34 Shimon Agranat, High Court of Justice 73/53, Kol Ha'am vs. the Minister of the Interior [in Hebrew].

35 Ladislav Bittman, "The Use of Disinformation by Democracies," *Intelligence and Counterintelligence* 4, no. 2 (1990): 243-61.

basic national consensus."[36] The defensiveness in the concept "defensive democracy" refers to protecting the democratic regime against internal threats by anti-democratic, revolutionary, and violent parties, movements, and groups.

Democracies can take various steps to defend themselves against subversive attempts to destroy them. These include legislative actions, legal prosecution, changing the political system, power-sharing with the dangerous groups in order to restrain and moderate them, or alternatively banning them in order to isolate and denounce them. Even though the term "defensive democracy" traditionally refers to internal threats, it can also be used in the context of external threats and as a guiding principle for democratic states when defending against the threat of foreign subversion.

The principal tool at the disposal of democracies is legislation. Since 2017, several bills have been proposed that aim to increase the transparency of election propaganda and prevent foreign funding of it. In addition, there are increasing calls for adapting the existing cybersecurity laws to enable effective handling of the issue of influence from foreign states.[37] Furthermore, in the framework of the National Defense Authorization Act[38] of 2017, the US Congress approved funding for the war against propaganda and suggested reforms to the law on the registration of foreign agents and in the committee responsible for foreign investments in the United States.[39] In addition, within this framework, a series of laws were approved, which are based on a strategic program developed by the Secretary of State and the Defense Secretary in order to contend with the threat of Russian influence in the world of social media.[40] Moreover, in September 2018, a law came into effect in California banning the use of bots.[41]

---

36 Dan Horowitz and Moshe Lissak, *Trouble in Utopia: The Overburdened Polity of Israel* (Tel Aviv: Am Oved, 1990) [in Hebrew].

37 Helmus et al., *Russian Social Media Influence,* p. 68.

38 This is the name of each of the series of federal US laws on the annual budget of the US Defense Department.

39 Mattis, "Contrasting China's and Russia's Influence Operations."

40 Helmus et al., *Russian Social Media Influence*.

41 Richard B. Newman, "California Enacts Anti-bot and IoT Laws," *National Law Review*, October 4, 2018.

During the French presidential elections in 2017, Emmanuel Macron, then a candidate and now the President, announced that he intended to pass a law regarding the conduct of social media during elections, in order to "defend democracy."[42] Canada passed a law that limits parties' expenses during a defined period of time before the elections and requires parties to mention the name of the party in election ads. The law also authorized election authority employees to prevent the dissemination of false information on the lives of candidates and on their criminal records. In addition, everyone, including social media companies, will be prohibited from distributing materials that include intentionally misleading information about their sponsor, or accepting election ads paid for by foreign entities.[43] China's increasing efforts to influence the media and academia in Australia led its former Prime Minister, Malcom Turnbull, to propose new legislation in December 2017 regarding espionage, foreign political contributions, and foreign intervention in Australia's internal affairs.[44]

In 2015, the European Union established a special task force – the East StratCom Team – which is a designated, integrated organization for defending against influence operations that aims to address Russian information warfare.[45] The task force exposes and publicizes cases of disinformation via a network, including some 400 newspapers, organizations, and academic institutions in some 30 European countries. It publishes the *Disinformation Review*, a periodical that documents instances of disinformation – so far 3,800 instances have been documented.[46] Similarly, in France, a working group has been established to explore the establishment of a joint task force for all intelligence organizations, in the wake of the Russian interference attempts during the republic's presidential elections in 2017.[47] In the United States, the FBI has

42 "Emmanuel Macron Promises Ban on Fake News during Elections," *The Guardian*, January 3, 2018.

43 Aaron Wherry, "Trudeau Government Proposes Major Changes to Elections Law," *CBC*, April 30, 2018.

44 Chan, "A Secret Government Report Uncovered China's Attempts to Influence all Levels of Politics in Australia."

45 Hellman and Wagnsson, "How Can European States Respond to Russian Information Warfare?" p. 157.

46 Sagi Cohen, "War Over the Truth," *Yediot Ahronot*, May 3, 2018 [in Hebrew].

47 Christine Schmidt, "How France Beat Back Information Manipulation (and How Other Democracies Might Do the Same)," NiemanLab, September 19, 2018.

laid the foundations for the establishment of a mechanism for fighting against disinformation, whose purpose is to create the ability to quickly respond to the threat of foreign influence operations and to conduct ongoing dialogue in order to share tactics and techniques for identifying disinformation at various levels of classification with the intelligence agencies.[48]

Cooperation between the state and the media would help encourage the media to take voluntary defensive measures and to involve social media companies in efforts to reduce potential threats.[49] After the computers of Macron's centrist party La République En Marche! were hacked during the French presidential elections in 2017, the French election committee published a press release demanding that "the media not report on the content of the information hacked, especially not on their websites." In addition, the French media received a reminder that "the dissemination of false information is a violation of criminal law." Most of the traditional media sources in France complied with the request and chose not to report on the content of the leaks. Some went even further and denounced the attempts at intervention in the elections by calling on the public not to cooperate with such manipulations.[50]

The establishment of designated bodies for countering influence operations by adversaries in special situations such as on the eve of elections is an appropriate step. These designated bodies will need to recruit the country's main intelligence organizations in the effort to identify fake accounts, discover who is behind them, and distinguish between the adversary's influence efforts and the legitimate discourse within a democratic state. The intelligence will serve as a basis for conducting efforts to thwart the adversary's efforts. These will include removing content from social networks, blocking their distribution sources where possible, and even taking offensive actions against those behind such operations. In addition, intelligence organizations will then have to work to declassify intelligence information in order to be able to place it at the disposal of the bodies responsible for cognitive warfare.

---

48 Bodin-Baron and others, *Countering Russian Social Media Influence*; Spencer P. Boyer and Alina Polyakova, *The Future of Political Warfare: Russia, The West and the Coming Age of Global Digital Competition* (Washington, DC: Brookings Institution, 2018), p. 3.

49 Boyer and Polyakova, *The Future of Political Warfare*, p. 3.

50 Schmidt, "How France Beat Back Information Manipulation."

This approach has become known as PUBINT – public intelligence.[51] It can help educate the public based on the fact that the government will need to provide guidance to its citizens in identifying external influence attempts. Educating the public will also require the assistance of the intelligence community, which can adapt some of its resources and manpower for this purpose.[52]

Official declarations can help contribute to deterring adversaries and raising public awareness about influence operations.[53] In 2017, the director of Germany's domestic security agency (BfV) publicly warned Russia not to interfere in Germany's elections, and Chancellor Merkel informed the public about the existence of this potential threat. It seems that these declarations caused Russia to refrain from leaking information collected from hacking into the German parliament in 2015.[54]

The coping mechanisms described above are in the hands of the state, while civil society should work independently in this area. At the end of September 2018, a report was published by the French Foreign Ministry's Policy Planning Committee and by a research institute of the Ministry for the Armed Forces, summarizing the ways France coped with the false information attacks during the 2017 presidential elections. The report emphasizes the central role of civil society in defending against influence operations, despite also being a source of false information: "Information is increasingly seen as a good whose defense is the responsibility of all citizens who are concerned about the quality of public discussion. Above all, the role of civil society is to develop its resilience. Governments can and should come to the aid of civil society. They should not lead, but their role is no less critical, as they cannot allow themselves to ignore the threat undermining the foundations of democracy and national security."[55]

---

51 Robert Kozloski, "Modern Information Warfare Requires a New Intelligence Discipline," RealClear Defense, February 20, 2018.

52 Ibid.

53 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.

54 Boyer and Polyakova, *The Future of Political Warfare*, p. 10.

55 Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, and Janaina Herrera, *Information Manipulation: A Challenge to Our Democracies* (Paris:

Conclusion

Defending against influence operations necessarily creates breaches that can serve as opportunities to harm basic civil freedoms. These are situations that must be avoided as much as possible. However, effective defense against the violation of democratic values sometimes requires a certain level of harm to democratic rights, as with a "defensive democracy," but we must ensure that such harm is proportional and limited. Democracies cannot abandon the basic values of openness, freedom of expression, and liberalism in order to contend with influence operations. The response to such operations, therefore, must be based on the law, on cooperation between institutions, and on civil society.

Civil society in democratic societies fulfills a series of roles, of which one of the most important is defending democracy against hostile influence operations. Civil society organizations can take action within a community or state framework to raise public awareness about disinformation and to educate the public on critical consumption of the news. Civil society should be actively strengthened by professionals providing guidance to the public on how to critically interpret visual and written media.[56] Support for civil society will also help highlight democratic values. In effect, liberal democracy cannot function without civil society.

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, 2018), p. 13.

56 Hellman and Wagnsson, "How Can European States Respond to Russian Information Warfare?" p. 162.