INTELLIGENCE IN THEORY AND IN PRACTICE

a journal on intelligence methodology

March 2025

Foreign Influence and Interference as a Strategic and Intelligence Challenge

Intelligence: Theory and Practice" - vol. 10

INSS: Memorandum - 238

Edited by: Yossi Kuperwasser and David Siman-Tov

Israel Ministry of Science & Technology

ISRAEL INTELLIGENCE HERITAGE & COMMEMORATION CENTER (IICC)

THE INSTITUTE FOR THE RESEARCH OF THE METHODOLOGY OF INTELLIGENCE

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Edited by: Yossi Kuperwasser and David Siman-Tov
Graphic Design: Ze'ev Eldar
Translation and Language Editing: Ela Greenberg

The Institute for National Security Studies (INSS), incorporating the Jaffee Center for Strategic Studies, was founded in 2006. The purpose of the Institute for National Security Studies is first, to conduct basic research that meets the highest academic standards on matters related to Israel's national security as well as Middle East regional and international security affairs. Second, the Institute aims to contribute to the public debate and governmental deliberation of issues that are – or should be – at the top of Israel's national security agenda. INSS seeks to address Israeli decision makers and policymakers, the defense establishment, public opinion makers, the academic community in Israel and abroad, and the general public. INSS publishes research that it deems worthy of public attention, while it maintains a strict policy of non-partisanship. The opinions expressed in this publication are the authors' alone, and do not necessarily reflect the views of the Institute, its trustees, boards, research staff, or the organizations and individuals that support its research.

The Institute for the Research of the Methodology of Intelligence (IRMI) at the Intelligence Heritage Center was established in 2016 and is dedicated to developing knowledge, operational concepts, and methodologies to support the needs of the intelligence community in Israel and worldwide.
The institute serves as a platform for discourse on intelligence methodology within the Israeli intelligence community while fostering connections with relevant discussions globally—across other intelligence communities, academia, and the private sector. IRMI draws upon the extensive experience of Israeli intelligence professionals, as well as a broad body of academic and research literature in the fields of intelligence and security from institutions in Israel and around the world.The institute includes research fellows the vast majority of whom come from the intelligence community.

Institute for National Security Studies (a public benefit company)

40 Haim Levanon Street

POB 39950 Ramat Aviv

Tel Aviv 6997556 Israel

info@inss.org.il http://www.inss.org.il

Contents

Introduction

David Siman-Tov and Yossi Kuperwasser

Foreign influence and intervention have emerged as critical strategic challenges in recent years, ranging from interference in democratic processes to shaping policy, security, economic affairs, and academia. A notable milestone in raising awareness of this threat was Russia's interference in the 2016 U.S. presidential elections.

This publication is a joint project of the Institute for the Research of the Methodology of Intelligence (IRMI) and the Institute for National Security Studies (INSS), initiated with the support of the Ministry of Intelligence. The contributors include academic researchers, current and former intelligence practitioners, and independent researchers who are actively engaged in countering foreign influence in Israel.

The aim of this report is to conduct a systematic analysis of a significant threat to Israel, which became particularly evident during the war in Gaza. Various actors seek to weaken the state of Israel and Israeli society, including by undermining social cohesion and amplifying narratives that serve foreign interests while masquerading as authentic Israeli discourse. This report focuses specifically on the role of intelligence in addressing this challenge.

Defining Foreign Influence and Intervention

The opening article of this report, written by Dr. Ofer Fridman of King's College London, provides a definition of foreign influence and intervention. According to Dr. Fridman, foreign influence has always been a fundamental component of international relations, manifesting through the use of all available instruments of power by one international actor seeking to impact another in pursuit of a strategic objective.

Building on this definition, foreign intervention can be defined as a specific form of foreign influence: *"Foreign influence becomes foreign intervention when the application of all available power sources by one international actor upon another is perceived by the affected party as being contrary to its values, norms, or laws."*

Foreign influence and intervention in democratic processes are not new phenomena and were particularly prevalent throughout the 20th century, on both sides of the Cold War. However, the last decade marks a significant shift, especially with the rise of social media as a primary arena for targeting both broad and specific audiences. This trend is part of the post-truth phenomenon, which fosters widespread skepticism and facilitates the dissemination of alternative truths and competing narratives.

In recent years, generative artificial intelligence (GAI) has significantly enhanced the ability to manipulate public perception, marking the beginning of a new and complex era of influence operations.

How Western Countries Address Foreign Influence and Intervention

When examining how Western states confront the challenge of foreign influence, several key components emerge:

- Dedicated governmental organizations – Establishing specialized government agencies to oversee and counter foreign influence.
- Regulation of digital media companies – Implementing policies to prevent foreign manipulation of online platforms.
- Raising public awareness – Enhancing digital literacy to educate citizens about foreign disinformation.
- International cooperation – Strengthening alliances to counter shared threats.

Beyond state-led efforts, civil society—including NGOs and the broader public—plays a vital role in countering this phenomenon. This includes:

- Identifying and researching threats related to foreign influence.
- Engaging in proactive countermeasures such as lobbying media companies to remove inauthentic influence campaigns.
- Collaborating with the press to expose foreign manipulation efforts.
- Promoting educational initiatives to strengthen democratic resilience.

The Intelligence Challenge in Addressing Foreign Influence

The intelligence challenge in countering foreign influence is a complex issue requiring in-depth examination. To explore this, we convened a roundtable discussion with former senior intelligence officials, focusing on the unique characteristics of the threat and the challenges it presents to intelligence agencies.

The discussion proposed distinguishing between three types of influence:

1. Foreign Influence – A broad spectrum of overt efforts by one state to impact the policy of another. This is considered legitimate (e.g., foreign media, diplomatic pressure, and economic measures) and should not be restricted.
2. Malicious Influence – Covert influence efforts by domestic actors aimed primarily at shaping internal public opinion. The legitimacy of such activities is debated in democratic societies, as they may weaken national resilience while still falling within the framework of a functioning liberal democracy.
3. Malicious Foreign Influence – Covert foreign influence that seeks to advance hostile objectives against the target state by exploiting the vulnerabilities of democratic societies and amplifying internal divisions. This constitutes a severe threat that must be actively countered.

Participants in the discussion recommended that Israel formally recognize malicious foreign influence as a national security threat, particularly in the social-digital sphere. Unlike the multi-agency intelligence system in the United States, Israel lacks a clearly designated authority to lead the national response to foreign influence threats.

The discussion emphasized the need for a governmental agency with the authority to integrate efforts and coordinate national resources, serving as the central body for intelligence operations against foreign influence campaigns.

A critical concern raised was the difficulty democratic states face in countering foreign influence without infringing on fundamental freedoms. This sparked a debate on the question if the digital sphere truly justifies

state intervention, which could risk unintended consequences such as restricting free speech.

Some participants warned of a “slippery slope”, arguing that this is an ethical issue that should not be solely managed by security agencies. Instead, checks and balances should be established, and a strict ethical framework should guide all state actions in this domain.

The Role of Civil Society in Countering Foreign Influence

Given the limitations of intelligence agencies in countering foreign influence, the role of civil society becomes increasingly crucial. Many civil society organizations actively monitor and expose foreign influence campaigns and develop countermeasures.

We refer to this emerging phenomenon as “Citizen Intelligence”—semi-intelligence initiatives led by concerned citizens committed to protecting national security and democracy.

Unlike covert threats, foreign influence actors seek public impact, often operating openly yet deceptively within the information space. In many cases, civilians—who are not bound by government regulations—have a unique advantage in detecting and countering foreign influence operations. Thus, civil society serves as a critical pillar in combating malicious foreign influence, complementing the efforts of national intelligence and cybersecurity agencies.

Defining Foreign Influence and Interference[1]

Ofer Fridman *

Over the past decade, governments, private companies, expert communities, and civil society organizations around the world have invested significant efforts and resources to understand and address subversive malign activities conducted by foreign states and non-state actors. Research and policy-related initiatives and legal actions undertaken during this period have exposed significant conceptual and normative gaps not only between democratic countries and countries at odds with human rights, but among like-minded democracies as well.

When examining the state of contemporary political, professional, and academic discourse on foreign influence and interference, it quickly becomes clear that there is a significant discrepancy between different definitions and approaches. These differences can be found on all levels of analysis and conceptualization: from basic understanding of what foreign influence and interference are, how they are conducted, and what they do, to strategic frameworks for how foreign influence and interference can be used to serve political aims.

The purpose of this article is threefold. First, it reviews the state of the contemporary debate. Starting with the review of existing strategic frameworks, it focuses on the main trends in existing denotative approaches to foreign influence and interference. Second, it critically analyzes existing concepts and approaches, identifying common gaps and misconceptualizations. Finally, based on the review and critical analysis, it builds the conceptual framework by constructing separate definitions of foreign influence and foreign interference, thus offering a better understanding of the difference between these two phenomena.

*Dr. Ofer Fridman is a Senior Lecturer at King's College, London

[1] This article is part of a forthcoming memorandum on the strategic challenge of foreign influence and intervention. The memorandum includes articles that examine the challenge from the perspective pf adversaries (e.g., Russia, Iran, and China), and deals with the nature of the influence (including via human influence agents and in the economic and academic worlds). The challenge will be examined with respect to routine times, as well as with respect to times of disruptions to democratic processes, deepened social rifts, election campaigns, and war. The articles will reflect a connection between systemic insights and the policy necessary in Israel and Western states. The memorandum is the product of collaboration between the Institute for National Security Studies (INSS) and the Institute for the Study of Intelligence Methodology at the Israel Intelligence Heritage & Commemoration Center (IICC), with the assistance of the Ministry of Intelligence.

Part I: The State of the Debate

Existing Strategic Frameworks for Foreign Influence and Interference

The principle of non-intervention into internal affairs of other states has a long history.[1] Article 2.4 of the UN Charter clearly states that "all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[2] However, over the past decade, Western academic, professional, and policy-relevant discourse has been shaped by three new conceptual frameworks intended to describe foreign influence and interference below the threshold of open military confrontation: "hybrid warfare/threats," "gray zone," and "Foreign Information Manipulation and Interference (FIMI)."

Hybrid Warfare: The idea of hybrid warfare/threats has a long and complicated conceptual history, during which the definition of concept (what it is), as well as what it entails (what it does), has been repeatedly adjusted and reconceptualized.[3] Initially introduced in the US, the hybrid warfare framework gained its popularity in Europe after Russia's 2014 annexation of Crimea.[4] While the concept has no definitive definition, it is possible to group all existing approaches into two main interconnected clusters. The first cluster consists of different definitions prevalent in military discourse. The best example of these approaches is the definition adopted by the Multinational Capability Development Campaign (MCDC): "Hybrid warfare is the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergetic effects."[5] The second cluster includes definitions used by different European political institutions. The best example of these approaches is the definition introduced by the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), according to which "the term hybrid threat refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level."[6]

Gray Zone: While the concept of hybrid warfare/threats has dominated the discourse in Europe, the concept of gray zone has gained its popularity in the US. Led by the US Army, especially the special forces community, the concept of gray zone became increasingly prevalent in the mid-2010s.[7] Similar to hybrid warfare, there is no definitive definition of gray zone. After assessing different existing definitions, researchers at the RAND Corporation concluded that "the gray zone is an operational space between peace and war, involving coercive actions to change the status quo below a threshold that, in most cases, would prompt a conventional

military response, often by blurring the line between military and nonmilitary actions and the attribution for events."[8] This concept shares many core assumptions with the concept of the "campaign between wars," independently developed by Israeli strategists over the last decade.[9] As Amos Yadlin and Assaf Orion argue, the core principle of the campaign between wars is "to avoid escalation and conduct operations under the war threshold," by "reducing the enemy's sense of urgency to react with an escalatory response."[10]

Foreign Information Manipulation and Interference (FIMI): While the concepts of hybrid warfare/threats and gray zone originate from political-military discourse, the FIMI framework has entirely civilian roots. It was proposed in 2021 by the European External Action Service (EEAS) in response to the 2020 call by the EU Commission for a further refinement of the conceptual frameworks around disinformation.[11] Adopted by different strategic documents, such as the 2022 Strategic Compass for Security and Defense[12] and the 2022 Council Conclusions on FIMI,[13] the concept has become a term of art across the EU professional and policy-relevant discourse. According to EEAS, FIMI describes "a mostly non-illegal pattern of behavior that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory."[14]

Existing Approaches to Foreign Influence and Interference

Following the 2014 annexation of Crimea and the controversies surrounding the 2016 presidential elections in the United States, the terms "foreign influence" and "foreign interference" assumed center stage in discussions among different governments, private companies, expert communities, and civil society. While there is little agreement on what these two phenomena entail, a review of many definitions and approaches proposed in the last several years allows identification of five main conceptual trends in the discourse about foreign influence and interference.

Influence versus Interference: Existing approaches adopted by governments and academia vary in their understanding of the difference between foreign influence and foreign interference. The approach adopted by the Australian government clearly distinguishes between influence and interference. While it seeks to counter foreign interference, which is "coercive, corrupting, deceptive or clandestine, and contrary to Australia's sovereignty, values and national interests," it "is not concerned with foreign influence activity that is open and transparent and that respects our people, society and systems."[15] The EU stance represents an opposite

example, where the official approach does not recognize the difference between foreign influence and foreign interference, using them interchangeably.[16] Moreover, they rarely provide clear definitions of foreign influence or interference; instead they offer a nonexclusive list of examples of activities that can be considered as foreign influence or interference and avoid formal definition altogether. Finally, they frequently include different negative adjectives, such as "malign,"[17] "malicious,"[18] or "manipulative."[19]

Domain of Influence and Interference: When discussing foreign influence and interference, existing approaches vary in their focus on the domain within which these activities take place. While there is general agreement that these activities pursue political goals by interfering, subverting, or detrimentally affecting the established democratic processes, approaches differ in their emphasis on the domains in which these activities can be conducted. On the one side of the spectrum, there are approaches that focus exclusively on the information domain as the main field of foreign interference, addressing disinformation and social media campaigns, relevant cyber activities, fake news, and data misuse and manipulation.[20] In contrast, there are approaches that take a more holistic view that incorporates not only information activities, but also other actions intended to interfere in established political processes, such as trade and investment, corruption, migration exploitation, and manipulation of international organizations.[21] In other words, while some approaches to foreign influence and interference take a more holistic view and include everything that foreign actors do, others focus exclusively on information, disregarding other potential domains of influence.

Intent: Many existing approaches tie their understanding of foreign influence and interference to the issue of intent. Some approach this question in an explicit way, referring to intent as a determining element in foreign interference. For example, the US Department of Homeland Security defines foreign interference as "actions…*designed to* sow discord, manipulate public discourse, discredit the electoral system…*for the purpose of* undermining the interests of the United States and its allies."[22] On the other hand, others approach the question of intent implicitly, simply referring to foreign influence and interference as "hostile," "malicious," "malign," or "manipulative." While there is little consensus on the strategic nature of this intent beyond the maligned tactical action, the non-definitive list of most frequently mentioned include: to coerce, undermine, subvert, manipulate, and disrupt established democratic processes and/or amplify societal divisions.

Transparency: Some existing approaches explicitly refer to the question of transparency as a determinant in defining foreign influence and interference, when "the former is open and honest, whereas the latter is covert and/or deceptive."[23] Other approaches refer to this question implicitly, by approaching any foreign interference or influence as "covert," "deceptive," or "clandestine."[24] Many existing approaches assume that transparency implies legitimacy, or suggest that the question of transparency is the main difference between foreign influence and interference, as "foreign influence is open and honest whereas foreign interference is clandestine and deceptive."[25]

Legitimacy: Defining foreign influence and interference, existing approaches vary in their use of different dichotomies to discuss legitimacy. Most frequently used frameworks are "legitimate vs. illegitimate," "acceptable vs. unacceptable," "legal vs. illegal." Some approaches adopt these frameworks explicitly, acknowledging the possibility of legitimate/acceptable/legal versus illegitimate/unacceptable/illegal foreign influence and interference. For example, the EEAS uses the term "non-illegal."[26] Most approaches, however, discuss these distinctions implicitly, focusing exclusively on foreign influence and interference as something illegitimate/unacceptable/illegal. Both, however, tend to adopt dichotomous frameworks of 'either … or' and rarely see these distinctions as a continuum.

Part II: Analysis

Analysis of Hybrid Warfare/Threats and Gray Zone

While these two strategic frameworks were developed independently, according to many experts they share many common attributes.[27] Both essentially describe a mix of hostile means and methods intended to achieve desired political aims without escalating to direct armed military confrontation. In other words, both describe a strategic approach to malign foreign influence short of war.

Since the comeback of the great power competition in the early 2010s, the Western strategic vocabulary has been tainted by a large number of different terms denoting more or less the same activity – hostile international relations between political actors short of kinetic application of force. Hybrid warfare/threats and gray zone are good examples of poorly constructed strategic frameworks that lack conceptual rigor.[28] The main conceptual flaw of these frameworks is their attempt to offer an objective definition to a practice in international relations. However, no Western political or military actor would acknowledge that they conduct hybrid or gray activities.[29] Conceptualized as a set of activities pursued only by adversaries, these frameworks fail to recognize their

inherent subjectivity that ultimately undermines their rigor. For example, if hybrid warfare is "the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergetic effects,"[30] then activities of any political actor (from the most liberal democracy to the most autocratic regime) involved in a non-military confrontation can be characterized as hybrid warfare. If gray zone is "an operational space between peace and war, involving coercive actions to change the status quo below a threshold that, in most cases, would prompt a conventional military response," then it is not only China that operates in the gray zone in the South China Sea,[31] but also NATO, as it attempts to coerce the Kremlin by means and methods that would not prompt Russian military response against NATO.

Analysis of Foreign Information Manipulation and Interference (FIMI)

While hybrid warfare/threats and gray zone were intended to provide an overarching strategic framework for malign foreign influence, they came with many conceptual caveats,[32] encouraging experts and policymakers to focus on foreign influence and interference as concepts on their own. The FIMI framework has been one of the main outcomes of this shift in focus. Since the framework is relatively new (introduced in 2021), its conceptual rigor has not been subjected yet to an extensive critical assessment by the expert community. However, its exclusive focus on interference in information domain already undermines its potential as a strategic framework. In other words, since FIMI focuses on information interference only, it ultimately fails to recognize the holistic nature of foreign influence and interference that interweaves political, economic, informational, diplomatic, financial, and other activities in international relations. According to EEAS, FIMI comes to describe what is "often labeled as disinformation,"[33] and, therefore, by its very definition, it cannot offer a strategic framework for understanding foreign influence and interference in international relations.

Analysis of Conceptualizations of Foreign Influence and Interference

The exisiting strategic frameworks not only try to reinvent the wheel by offering new conceptual frameworks for something that has always been common practice in international relations, but they also focus exclusively on influence that is perceived as hostile. This leads to the failure of these frameworks to recognize that influence in international relations can be perceived in ways positive and negative and its perceived hostility is subjective to the influenced. In other words, similar to many Western countries that perceive Russian hybrid warfare/threats

as hostile influence, Russia can perceive Western soft power as a hostile influence on Russia.

An analysis of contemporary scholarly and professional discourse on foreign influence and interference shows that very little effort has been invested in trying to understand and define what these phenomena are. Moreover, foreign influence and interference have been commonly defined and discussed in a negative way (with Australia being a helpful exception), as a set of threats or activities that need to be countered or eliminated, failing to acknowledge that under certain circumstances foreign influence can be welcomed. Moreover, many existing approaches and definitions fail to conceptually recognize the inherent difference between foreign influence and foreign interference, using the terms influence and interference interchangeably.

On the one hand, in their attempts to define foreign influence and interference, existing approaches operate with relevant characteristics, such as transparency or legality. On the other hand, due to the exclusive focus on foreign influence as something conducted by malign actors with hostile intent, there is much confusion and misunderstanding what foreign influence and interference are, what they do, and how they can be addressed.

One of the main conceptual drawbacks of the existing approaches to foreign influence is their failure to recognize that influence is not a goal in and of itself, but the means in international relations to achieve a political goal. Arguably, all interactions (both deeds and words) between states (in all domains of national power: political, information, military, economy, and others) are the means of influence in pursuit of political goals in international relations.

Part III: The Influencer and the Influenced in Foreign Influence and Interference

To define foreign influence, it is important to focus on three main aspects. First, an influencing actor formulates the intent of its influence in the context of its national interests (constructed through interaction between the government, different domestic political actors and institutions, and the people) and shaped by its national values (Figure 1).[34] In most of the cases the true intent of the influencing actor will be unknown to the influenced actor. Even in the cases when foreign influence is invited and welcome, its true intent remains unknown to the inviting actor. Therefore, trying to tie the definition of influence (or interference) to the nature of influencing actor's intent is misleading and counterproductive.

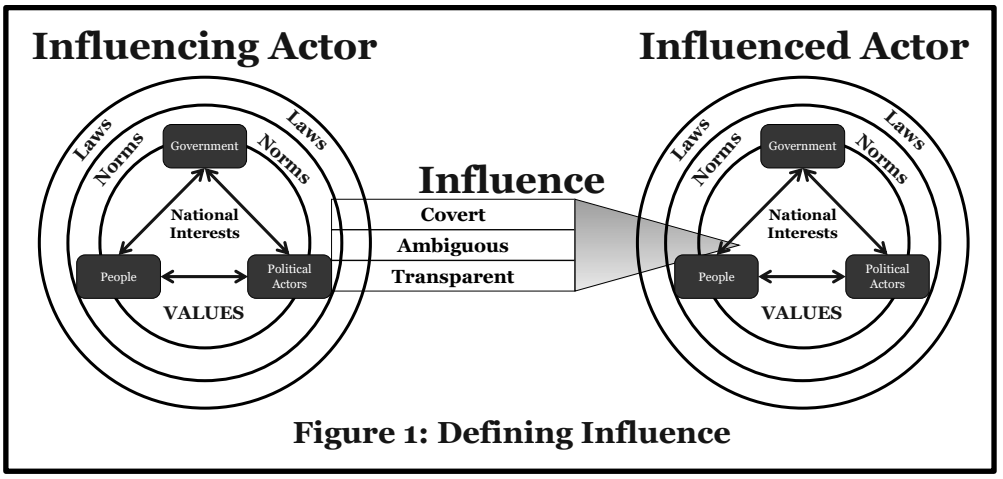


Figure 1: Defining Influence

Second, the question of transparency is determined by the influencing actor, not the influenced. Since the true intent of influence is known only to the influencing actor, it is he who decides whether the influence exercised by him will be transparent, ambiguous, or covert. Since influence is not a goal, but the means in international relations to achieve a political goal, the transparency of the actions conducted in pursuit of influence is shaped by the strategic goals (intent) behind these actions. For example, a foreign investment in national infrastructure of the influenced actor can be either a transparent influence (investment in pursuit of transparent and openly declared goals), or it can be covert (investment in pursuit of covert – other than openly declared – goals), or it can be ambiguous (investment that has a potential to be used for other than openly declared goals).

Finally, influence is characterized (as hostile or otherwise) by the influenced actor in the context of its national interests and values, as well as norms and laws intended to shape and protect them. In other words, the issue of hostility is judged by the influenced actor's perception of this influence, and the same influence driven by same intent can be perceived differently by different influenced actors.

The influence can be perceived by the influenced in three different ways. First, it can be perceived as welcomed, as it acts in consensus with national norms and values of the influenced actor. Second, it can be perceived as prohibited, as it acts against the existing national laws of the influenced actor. And finally, the nature of influence can be contested, as it is neither implicitly in consensus with the influenced actor's national norms and values nor explicitly prohibited by its legal system. Sometimes, contested influence can be tolerated in the name of values and interests (e.g., freedom of speech, human rights, etc.). On other occasions, it can be perceived as unlawful and requiring new relevant legislation. The way influence is perceived by the influenced actor will be shaped by its national norms, policies, and laws (Figure 2).

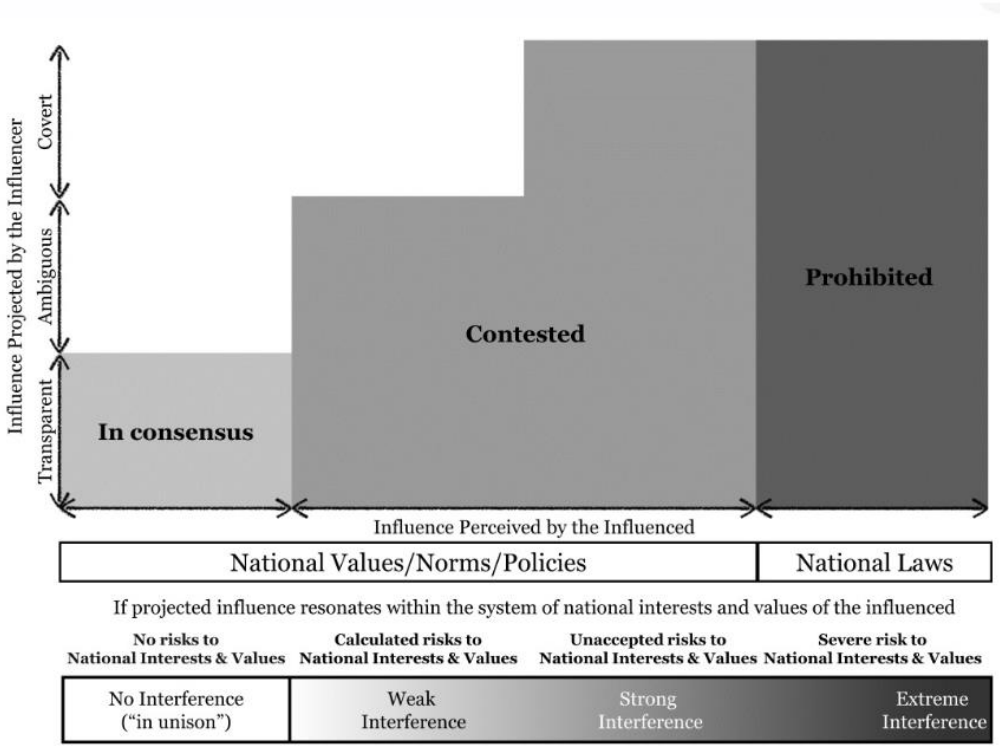


Figure 2: Perception of Foreign Influence by the Influenced

The perceived nature of influence depends more on the influenced actor's internal elements, rather than on the issue of transparency (or lack thereof). Since the issue of transparency is controlled by the influencing actor, any influence (transparent or not) will be judged by the influenced actor in the context of its values/norms/policies and laws. For example, a transparent influence can be perceived by the influenced as in consensus, contested, or prohibited, depending on its national values/norms/policies and laws. An ambiguous influence would not be welcome; however, it can still be perceived as contested or prohibited. A covert influence will usually fall in the area of already prohibited or something unlawful that requires new legislation.

Most of the existing approaches try to address the area of contested influence, as its acceptability, tolerability, and legality is contested in the context of the existing values/norms/policies and laws. The problem with these approaches, however, is that their exclusive focus on this particular type of influence (combined with the failure to acknowledge the existence of other types) undermines their conceptual rigor.

The final limitation of the majority of existing approaches is their confusion between foreign influence and foreign interference, to an extent that sometimes these terms are used interchangeably. Influence is the means in international relations to achieve a political goal. Foreign influence can achieve these goals only if it resonates within the system of the national interests and values of the influenced. Without this resonance, foreign influence is meaningless as it fails to interact with the influenced actor in any way (positive or negative). For example, an attempt to influence an Amazonian tribe through information about the Second World War would generate no resonance, as the peoples of this tribe simply have no knowledge of this war.

Since the way foreign influence is perceived and the type of resonance it can create are defined by the national interests and values of the influenced actor, there is a strong correlation between them. The resonance created by foreign influence in consensus would create no interference, as it would act "in unison" with the existing national interests and values. However, as the risk created by this resonance to these interests and values increases, the more interference it creates (Figure 2).

Conclusion: Defining Foreign Influence and Interference

Foreign influence is a core element of international relations. International actors have always sought to influence each other's affairs and decision making in pursuit of their political goal. In other words, foreign influence encompasses any type of interaction between two political actors – whether it is honest cooperation based on shared democratic values, or an act of war. After all, war is "an act of force to compel our enemy to do our will,"[35] i.e., influence. Foreign influence has always been the fundamental means in international relations, and therefore, there is no need for new conceptual strategic frameworks. Instead, it should be seen for what it has always been: *a deployment of different sources of national power (diplomatic, information, military, economic, financial, religious, etc.) by one international actor to influence another in pursuit of a political goal.*

Following this definition of foreign influence, it is possible to define foreign interference as a particular type of foreign influence: *foreign influence can be characterized as foreign interference when the deployment of different sources of national power (diplomatic, information, military, economic, financial, religious, etc.) by one international actor to influence another is perceived by the latter as in contradiction with his values, norms, or laws.*

[1] Michael Wood, "Non-Intervention (Non-interference in domestic affairs)," Princeton University, https://pesd.princeton.edu/node/551

[2] United Nations, *United Nations Charter*, https://www.un.org/en/about-us/un-charter/full-text
[3] *Ofer Fridman,* Russian "Hybrid Warfare": Resurgence and Politicization *(New York: Oxford University Press, 2022).*
[4] Ibid.
[5] *The Multinational Capability Development Campaign (MCDC),* Countering Hybrid Warfare *(2019), p. 12,* http://tinyurl.com/27zwnsc3
[6] *The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), "Hybrid Threat as a Concept,"* https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/
[7] *Donald Stoker and Craig Whiteside, "Blurred Lines: Gray-Zone Conflict and Hybrid War: Two Failures of American Strategic Thinking,"* Naval War College Review*, 73, 1, (2020): 13-48.*
[8] *Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe,* Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War *(Santa Monica, CA: RAND Corporation, 2019), pp. 7-8.*
[9] Shai Shabtai, "The Concept of the Campaign between Wars," *Maarachot*, No. 445 (2012): 24-27 [in Hebrew].
[10] Amos Yadlin and Assaf Orion, 'The Campaign between Wars: Faster, Higher, Fiercer?' *INSS Insight* No. 1209, (2019), http://tinyurl.com/3j2hn756
[11] The European Union Agency for Cybersecurity (ENISA) and the European External Action Service (EEAS), *Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape*, December 2022, p. 4, http://tinyurl.com/yjxwuf3w
[12] Council of the European Union, *2022 Strategic Compass for Security and Defence*, March 21, 2022, http://tinyurl.com/2732xzsd
[13] Council of the European Union, *Council Conclusion on Foreign Information Manipulation and Interference (FIMI)*, July 18, 2022, http://tinyurl.com/jyk8d4ye
[14] The European External Action Service (EEAS), *1st EEAS Report on Foreign Information Manipulation and Interference Threats*, February 2023, p. 4, http://tinyurl.com/ycyfcw9b
[15] Australian Government, Department of Home Affairs, *Defining Foreign Interference*, http://tinyurl.com/t4c5c29a
[16] European Parliament, *Foreign Interference in All Democratic Processes in the European Union*, March 9, 2022, https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_EN.pdf
[17] *For example: G7,* Charlevoix Commitment on Defending Democracy from Foreign Threats*, June 9, 2018,* http://tinyurl.com/mt7pb5e7
[18] *For example: European Commission,* Securing Free and Fair European Elections*, September 12, 2018,* http://tinyurl.com/ystkhc57
[19] *For example: Council of the European Union,* Complementary Efforts to Enhance Resilience and Counter Hybrid Threats*, December 10, 2019,* http://tinyurl.com/78emmdb2
[20] *For example,* The European Union Agency for Cybersecurity (ENISA) and the European External Action Service (EEAS), *Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape*; The European External Action Service (EEAS), *1st EEAS Report on Foreign Information Manipulation and Interference Threats*.
[21] *For example: Katherine Mansted, "The Domestic Security Greyzone: Navigating the Space Between Foreign Influence and Foreign Interference,"* National Security College Occasional Paper*, Australian National University, 2021; US Department of Homeland Security, "Foreign Interference Taxonomy," July 2018,* http://tinyurl.com/5h6eem7w
[22] *US Department of Homeland Security,* Foreign Interference Taxonomy *(emphasis added)*.
[23] Kate Jones, "Legal Loopholes and Risk of Foreign Interference," In-Depth Analysis requested by the ING2 Special Committee at the European Parliament, January 2023, p. 21, http://tinyurl.com/y8hhku3b
[24] *For example: Australian Department of Home Affairs,* Countering Foreign Interference*, January 27, 2022,* http://tinyurl.com/mrfrjp2x
[25] Jones, "In-Depth Analysis: Legal loopholes and the Risk of Foreign Interference," p. 21.
[26] The European External Action Service (EEAS), *1st EEAS Report on Foreign Information Manipulation and Interference Threats*.
[27] *For example, Frank Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges,"* Prism*, 7, 4(2018): 31-47; Stoker and Whiteside, "Blurred Lines," Fridman,* Russian "Hybrid Warfare*."*
[28] *Vladimir Rauta, "A Conceptual Critique of Remote Warfare,"* Defence Studies*, 21, 4(2021): 545-72; Stoker and Whiteside, "Blurred Lines"; Fridman,* Russian "Hybrid Warfare."
[29] Ofer *Fridman, "Afterword to Paperback Edition: Moving Beyond Hybrid Warfare," in Fridman,* Russian "Hybrid Warfare*."*
[30] *The Multinational Capability Development Campaign (MCDC),* Countering Hybrid Warfare*, p. 12*

[31] *Peter Layton, "Responding to China's Unending Grey-Zone Prodding,"* RUSI Commentary, *August 11, 2021,* http://tinyurl.com/mrm5nspr
[32] *For example, Fridman, Russian "Hybrid Warfare"; Stoker and Whiteside, "Blurred Lines"; Hoffman, "Examining Complex Forms of Conflict."*
[33] The European External Action Service (EEAS), *2021 StratCom Activity Report*, 2021, p. 2, http://tinyurl.com/w6abcryk
[34] While the conceptualization here is between states (i.e., national interests, government, people, etc.), it can be easily translated to non-state actors (i.e., actor's interests, actor's leadership, actor's norms and values, etc.).
[35] Carl von Clausewitz, *On War*, Ed. and trans. Michael Howard and Peter Paret (Oxford: Oxford University Press, 2008), p. 13.

Foreign Interference and Iranian Influence on Social Networks in Israel[1]

Inbal Orpaz and David Siman-Tov[2]

This article addresses the phenomenon of Iranian foreign interference in social media platforms in Israel during the years 2020–2022. Its aim is to examine and characterize the phenomenon, discuss its consequences, and propose policy addressing it. The study reveals that agents of foreign interference in the discourse on Israeli social networks do not favor a certain group or agenda in Israeli society; rather, they aim to deepen the rifts in Israeli society and weaken it. The article begins with a description of the main operations present in the Israeli discourse in recent years. We then present an analysis of the phenomenon and identify the main modus operandi of the perpetrators. Finally, we provide policy recommendations for the government, civil society, and the public.

Introduction

In the digital era, social networks have become the new "digital town square" active both in routine times and during emergencies. Over 70% of the Israeli public uses social networks for various purposes: consuming information, expressing diverse opinions, receiving purchasing recommendations, and staying in touch with friends.[3] However, it is not just Israeli citizens who use social networks in Israel. Occasionally, social media accounts that appear "Israeli" and publish content aimed at the Israeli public are, in fact, operated by hostile entities intending to

[1] This article is part of a soon-to-be-published memorandum on foreign influence and interference as a strategic challenge. Some of the articles included will address this issue from the perspective of adversaries. Some will also examine foreign influence and interference during routine times as well as during the disruption of democratic processes, the deepening of social rifts, election campaigns, and wars. The articles reflect a connection between systemic understandings and the policy needed to address it, both in Israel and in Western countries. The memorandum concludes a joint project conducted by INSS and the Israel Intelligence Heritage and Commemoration Center (IICC).

[2] Inbal Orpaz is a strategic innovation consultant and was a visiting researcher at the Institute for National Security Studies. David Siman-Tov is a senior researcher at the Institute for National Security Studies and deputy head of the Institute for the Research of the Methodology of Intelligence.

[3] Central Bureau of Statistics, "Well Being, Sustainability, and National Resilience Indicators, 2021," Part 11, "Internet and Technology," https://www.cbs.gov.il/he/publications/doclib/2022/1873_well_being_2021/prt11_5_h.pdf

interfere with and disrupt Israeli discourse in order to advance their strategic goals.

This study provides an in-depth analysis of foreign interference operations carried out on social networks in Israel in recent years, specifically from 2020 through the end of 2022. The study aims to analyze and characterize this phenomenon, discuss its implications, and propose policy recommendations to address it. Findings reveal that foreign actors engaging in Israeli social media discourse do not necessarily support any specific group or agenda within Israeli society. Rather, their primary objective is to deepen societal divisions and undermine the country's stability. While Iran is identified as being behind most of the influence operations discussed in this study, recent evidence suggests the involvement of additional actors.

The following research questions were examined:

- What are the modus operandi of foreign interference operations on social networks?
- How can suspected inauthentic activity on social networks be linked to foreign influence agents?
- What can we learn from the handling of the digital platform and the government that were exposed?
- What insights can be drawn from how digital platforms and government entities handle these exposures?
- How do networks affect national security, democracy, and national resilience?
- How do such influence networks affect national security, democratic processes, and societal resilience?

Part 1. Description of the Foreign Interference Operations

The foreign interference operations examined in this study were carried out by social media accounts exhibiting inauthentic behavior and were likely operated by foreign state actors. Later in the document we will detail the criteria used to identify each account as inauthentic, foreign, or Iranian. A report published by Meta discussing influence operations that took place during the years 2017–2020,[4]

[4] Facebook, "Threat Report: The State of Influence Operations 2017–2020," May 2021, https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf

defined influence operations as "coordinated efforts to manipulate or disrupt the public discourse for a strategic goal."

In this study, we focused on three groups of interference operations targeting specific audiences in Israel from early 2020 until the end of 2022. Additionally, we included networks active around the November 2022 election campaign.

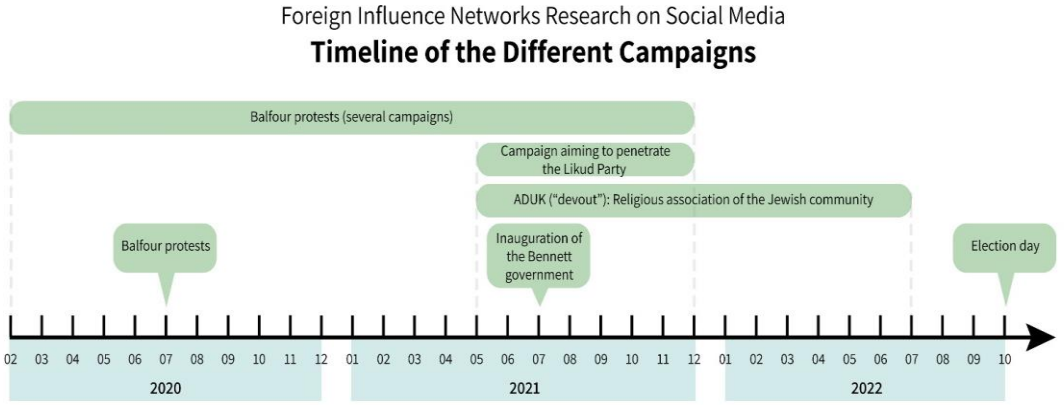


Figure 1. Timeline of Foreign Interference on Social Networks in Israel Included in This Study and Main Events in Israel During This Period

Influence Campaigns by Groups Posing as Activists in the Balfour Protests (February 2020–December 2021)

In this category, we include at least five influence operations and their affiliated accounts that were identified by Facebook and FakeReporter, which all shared similarities in terms of content and patterns of activity. The common denominator was posing as groups of activists from the Balfour protests (such as the legitimate groups of "The Black Flags" (*haDegelim haShchorim* in Hebrew) and "No Way" (*ein matzav*) groups). The operations took place from the beginning of 2020 until the end of 2021. The documentation about these groups is extremely limited, as Facebook shared information about these groups in its publications only after it had removed their accounts. Those behind these interference operations had access to a variety of platforms and tools at their disposal, including accounts on Facebook, Instagram, WhatsApp, and Twitter, websites, Facebook groups, and Telegram channels. The various operations employed multiple tactics and methods, including both Hebrew and English language accounts, impersonation of legitimate protest organizations and private individuals, and tagging tens of thousands of Instagram accounts.

The first operation—Black Flags IL—was identified by Facebook and disclosed in a report published by Meta in November 2020.[5] Facebook removed the accounts that were part of the operation, stating that Iranian agents were behind them. According to the report by Meta, a total of 12 Facebook accounts, 2 Facebook pages, and 307 Instagram accounts were identified as part of this single operation. About 1,100 accounts followed one or more of the pages, and about 9,500 people followed one or more Instagram accounts related to the operation.

A report by Graphika claimed that the operation did not allocate significant resources to creating these accounts. For example, the names "Leah" and "Ori" were selected for a dozen accounts in the operation. Instagram accounts were created with a standardized format of full name and year of birth. In addition, no effort was made to select credible profile pictures; rather, they used pictures from the Getty Images database (which included the company's watermark) or used profile pictures of Arab women wearing hijab in accounts bearing Hebrew names.[6]

Facebook stated that when it removed the accounts, those behind the operation were still in the initial stages of building their community of followers. The operation used fake accounts, most of which had been created around the same time. Over time, these accounts changed their names and worked to promote various goals that served the aims of the Iranian influence operations. The accounts published pictures, memes, and content in Hebrew and Arabic. In some cases, different accounts published identical content, such as the same picture. The content revolved around current events, including anti-Netanyahu demonstrations and criticism of his policy on the COVID-19 pandemic.

According to Graphika's report, the content changed at each stage of activity. The content addressed various issues based on public discourse in Israel and aimed to create social or political divisions. In the first few months of 2020, after the outbreak of the COVID-19 pandemic, the content primarily focused on criticizing Netanyahu's policy in addressing the pandemic. Specifically, it centered on the tensions between the government and its citizens, as well as the significant impact caused by the pandemic. In July of that year, the accounts affiliated with this operation started to publish content associated with the Black Flag movement—a legitimate Israeli protest movement that started during that period to oppose Netanyahu.

---

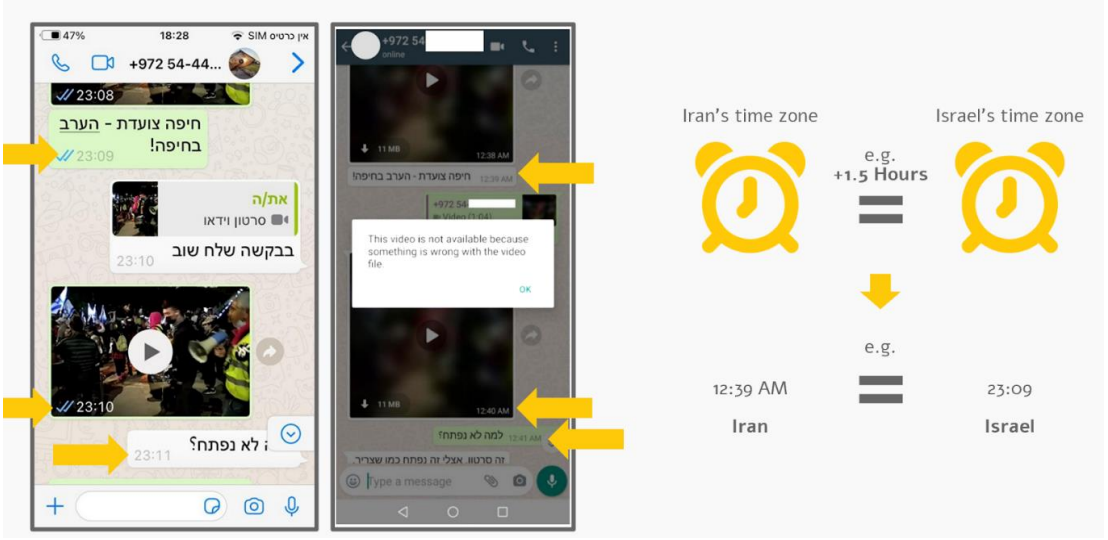
[5] Meta, "October 2020 Coordinated Inauthentic Behavior Report," November 5, 2020, https://about.fb.com/news/2020/11/october-2020-cib-report/

[6] Graphika, "Capture the Flag: Iranian Operators Impersonate Anti-Netanyahu 'Black Flag' Protestors, Amplify Iranian Narratives," November 2020, https://public-assets.graphika.com/reports/graphika_report_capture_the_flag.pdf

According to Graphika's report, in one case, one account published the details of a PayPal account to which money could be transferred for donations to the operation. According to Facebook, the operators of these accounts attempted to hide their identities, but the company discovered links between them and entities connected to EITRC, an IT company based in Tehran.

In December 2020, the team that eventually developed into FakeReporter began receiving reports about a suspicious person who joined WhatsApp groups and, in direct conversation with group members, asked for photos from demonstrations in Israel. In exchanges with this individual, indicators emerged connecting him to Iranian entities: broken Hebrew; backward question marks (؟), which are typical of Persian; screenshots from a phone with an interface in Persian; and a 1.5-hour time difference, reflecting the time difference between Israel and Iran (see Figure 2). Moreover, attempts to receive donations from Israeli citizens were identified.

Figure 2. Messages Between an Online Agent who Contacted Activists in the Balfour Protests and an Activist Whose Time Zone Is Characteristic of Iran's



As part of this operation to impersonate BB (Black Banners) movements, in addition to infiltrating WhatsApp groups and making contact with Israeli citizens, a website was found that posed as part of the Black Flag movement. The pictures shared with the operators and updates on the demonstrations were posted on this website. As part of the operation, three domain names were acquired in November 2020, with names similar to the real "black flags il" movement. Moreover, about 10 accounts affiliated with this operation were set up on social media networks, including an account in Arabic. The accounts followed central activists in the protests. This influence operation was reported on the Kan 11

television channel,[7] and its operators responded in a video that they created, which was posted on the group's Telegram channel. Following the report on Israeli television, Facebook and Twitter closed the relevant accounts, although one of the websites and the Telegram channel related to this operation are still active.

ADUK ("Devout")—The Virtual Religious Association for the Religious Community (2020–2021)

The ADUK operation was active on several platforms, including Facebook, Twitter, and a Telegram channel, and posted content with a right-wing orientation related to the Haredi community. Meta confirmed to the BBC that Iranian operators were behind it. The Facebook and Twitter accounts that belonged to the network were closed by the platforms, but its Telegram channel continues to operate.

The name of the operation was ADUK, which was an acronym for "The Virtual Religious Association for the Religious Community." The operation aimed to promote a Haredi agenda with a right-wing orientation. According to the Telegram channel, the topics discussed included "the voice of the religious community, news in real time, Haredi news in real time, the struggle against violence (police and Arab), anti-secular, interesting questions in Jewish law (Halacha), stories of the righteous." In particular, the channel made statements against the police as well as claims of the IDF's incompetence. The channel also addressed issues such as COVID-19 (the operation took place during the peak period of the pandemic), the cost of living in Israel, and so forth. In addition, the operation posted halachic issues under the hashtag (interesting issues in halacha) as well as Shabbat times each week.

Most of the content posted on the Telegram channel was replicated from real posts made by ultra-Orthodox social media users. Operation ADUK's Facebook page and group used stolen pictures of a deceased Russian Jewish man. The operation's other characteristics included copying content from authentic accounts that served the operation's agenda; creating fake assets to develop authenticity (a logo, the invention of the name ADUK, the creation of a special page as part of creating the fake identity); adding logos to the pictures posted; engaging in incitement, racism, and hate speech; attempting to appeal to emotions; consistently using the same hashtags (#enough is enough, #hot news); and sharing content in groups and channels that appealed to a right-wing and Haredi

[7] Oren Aharoni, "Investigation: Who Is Trying to Impersonate Black Flag Activists?," KAN, March 3, 2021, https://www.kan.org.il/content/kan-news/politic/281335/

population. At its peak in March 2022, the operation published over 600 posts on Telegram (see Figure 3).

Figure 3. Number of messages published per month on the Telegram channel of ADUK (based on Telemetrio)

It seems that the goal of the ADUK operation was to deepen the divisions and rifts in Israel. ADUK's Telegram channel had reached 770 followers on March 20, 2022. Although the operators invested in this operation and posted content consistently and systematically, it did not gain widespread exposure and did not have significant influence over the Israeli public.

FakeReporter exposed the operation's activity on its Twitter account on February 3, 2021.[8] The network was subsequently covered by the BBC,[9] and in response to the reporter's request for a response from Meta, Meta confirmed that the operators of the accounts were Iranians.

Making Contact With Political Activists Associated With Netanyahu (July 2021–December 2021)

This group of accounts was discovered following a report received in November 2021, according to which a suspicious account had made contact with an Israeli citizen and tried to get her to say things about demonstrations in support of the political right. As a result of the report, approximately ten fake Facebook and Twitter accounts were identified, which had joined about 90 Facebook groups, more than half which were groups of Netanyahu supporters. These accounts posted content mainly against the government, which was then led by Naftali

[8] FakeReporter, "Under the guise of a Haredi network organization, an Iranian cell has been operating on social media for months.." [in Hebrew] X (formerly Twitter), February 3, 2022, https://twitter.com/fakereporter/status/1489164051011846144

[9] Tom Bateman, "Iran Accused of Sowing Israel Discontent with Fake Jewish Facebook Group," BBC, February 3, 2022, https://www.bbc.com/news/world-middle-east-60229146

Bennett and tried to inflame tensions in Israel by fueling demonstrations and protest activities.

The fake accounts posted replies to prominent political activists, and they succeeded in making direct contact with some of these activists and received their phone numbers. The fake accounts were connected as virtual friends, amplified messages, sometimes sharing identical content, and they were active at similar times. The fake accounts created original content that aimed, in part, to promote real demonstrations that were held in Israel.

In one case, the operators of these accounts created and shared an invitation to a demonstration in September 2021, in which photographs from the fake accounts were integrated with pictures of real political activists. Afterward, the invitation was shared by political activists in groups connected to the Likud. Various actions taken by these accounts indicate deep familiarity with Israeli political activists.

The accounts that were identified as part of this operation were first opened in July 2021, and in November 2021, initial reports of suspicious activity by these accounts were made. On December 29, 2021, Channel 12 News broadcast a report about the interference operation,[10] after which Facebook and Twitter removed the accounts belonging to this operation.

The Elections to the 25th Knesset in November 2022

During the period of this research, the elections to the 25th Knesset took place in November 2022. At that time, additional operations with similar characteristics were uncovered. They included:

An Operation to Cause a Split in the Knesset List of the Religious Zionism Party.

Prior to the elections, a number of Twitter accounts were created, of which 40 have been identified. All these accounts were opened on August 2, 2022, and used profile photos of men who were employed by the real estate company RE/MAX. The accounts posted copied content, including caricatures and jokes, and did not raise any suspicions until September 14, the day before the submission of the Knesset party lists, when they began posting caricatures of Itamar Ben-Gvir and called for a split in the Religious Zionism Party using the hashtag #run alone in the elections. On October 18, 2022, FakeReporter reported the operation to Twitter

[10] Dafna Liel, "Report: This Is How an Iranian Network Disseminates Content in Israel—In Order to Inflame the Political Debate," [in Hebrew] N12, December 29, 2021, https://www.mako.co.il/news-digital/2021_q4/Article-5496b9571470e71026.htm

and publicized it on its own channels and in *Haaretz*. On October 19, the accounts were removed.

Voter Suppression Operation on Election Day. Another operation was carried out to suppress voter turnout on election day, and it included two stages with indications that the same entity was behind both stages, based on activity patterns. In the first stage, hundreds of Twitter accounts were opened during a short window of time on October 17, but they did not post content until October 28—three days before the elections. Two days before the elections, these accounts began to coordinate thousands of tweets. The profiles posed as Israeli citizens, mainly opponents of Netanyahu, and called for boycotting the elections. The first group of accounts in the operation was removed before election day, while another group began its activity on election day. On October 31, the day before the elections, FakeReporter reported the operation to Twitter. The first set of profiles was removed on election day.

On election day, the second stage of the operation began. Several hundred Twitter accounts were created on October 22 and operated on election day. This operation also included posts in Arabic and promoted content aimed at suppressing voter turnout. On election day, FakeReporter reported the accounts to Twitter, and they were removed.

After the Elections: The Election Fraud Campaign. A group of accounts that operated on Facebook, Twitter, Instagram, and Telegram made claims about election fraud and nonacceptance of the election results and called for a protest in front of the Prime Minister's Office the day after the elections. About 15 accounts operated as part of this operation, and more than a thousand fictitious accounts followed them, apparently to increase the credibility of the main accounts in the operation. This collection of accounts that operated around the Israeli elections underlines the great interest that agents outside of Israel showed toward central events in the country and raises questions about their impact on the integrity of the elections.

Part 2. Shared Characteristics of the Interference Operations

In this section, we will present the modus operandi of the agents managing the interference operations. These pattern can be used to identify future interference operations, and they point to characteristics that require further examination. However, it is important to note that the operators of the interference operations continuously adapt and learn, and some of the characteristics are expected to

change. One of the main changes in the past year relates to the accessibility of generative AI technologies, which affects the way influence operations are now waged.

The following is a list of common characteristics in the interference operations under study:

Content Related

- The fictitious accounts that belong to interference operations generally used Hebrew names. These names were intended to cause the Israeli Hebrew-speaking population—the target audience of the operations—to believe that these were authentic accounts belonging to real people and not fictitious accounts with foreign interference agents behind them.

- The profile pictures that were used in the interference operations were mainly stolen images or photos of unknown origin. Additionally, in some cases, pictures from stock photo databases; selfies in which it is difficult to identify the people photographed because the faces were hidden by the telephone; and photos of porn actresses that had been distorted making it impossible to locate their source were all used as profile photos.

- The accounts belonging to the interference operations often responded to posts about current events in Israel. In this way, they increased their credibility as Israelis who were knowledgeable about events in their country, were involved in the issues at the center of the local discourse, and received greater attention.

- In many cases the content posted on the fictitious accounts was copied from real users; that is, real people (including journalists, prominent tweeters, viral content, posts by news outlets, and so forth).

- The content of the posts addressed controversial issues in Israeli society. The variety of issues discussed indicates that these operations did not have an interest in favoring or acting against certain figures in the political system or in Israeli society but rather sought to identify issues that could deepen rifts in Israeli society and that could arouse intense responses on social networks.

- Many posts were characterized by poor grammar and inarticulate language. Sometimes, original posts were written in broken Hebrew. This stems from the fact that the writers were not native speakers, learned the language from listening, or used an automatic translation engine (such as Google Translate), causing the use of imprecise and incorrect language. In addition, when writing

original content in Hebrew, they sometimes used incorrect or inappropriate words.

Relating to the Pattern of Activity of the Accounts in the Operations

- The fictitious accounts belonging to the operations functioned simultaneously on a variety of platforms. For example, accounts with the same name or using the same profile pictures were opened at the same time on Twitter, Facebook, Instagram, and so forth. This increased the credibility of the fake accounts in the eyes of those interested in checking their authenticity—the greater their internet presence was, and the more investment made in it, the more these accounts gave the impression that real people were behind them.

- The interference operations used frameworks that include groups, communities, and pages created by their operators. The pages and groups were given names of initiatives that represent the operation. Moreover, they created fictitious figures that promoted the content on the groups and pages of the initiatives or operated them.

- It is evident that most operations continued over an extended period. During the period of activity, the accounts that belonged to the operation systematically posted a variety of types of content, gradually building their credibility.

- The fictitious accounts operated in a coordinated manner. For example, they posted things at regular times (during hours of activity that seemed like work shifts).

- The fictitious users in the interference operations were members of popular Facebook groups with diverse political affiliations (for example, "Benjamin Netanyahu the Official Group") and posted content in them. In this way they succeeded in gaining publicity and exposing an authentic audience to their content.

Part 3. Indicators of Suspicious and Inauthentic Behavior on Social Networks

The following list of characteristics can indicate coordinated, inauthentic activity on the internet. A single characteristic, however, is insufficient for determining with a high level of certainty that an account is not authentic:

- The use of stolen, fake, or AI-based profile pictures, or the inability to identify the figures appearing in them, and so forth
- Publishing content copied from real users (influencers, media outlets, and so forth)
- Repetition and duplication of identical responses to other users (fictitious or real) several times
- Follower-to-following ratios between suspicious accounts—this sometimes makes it possible to identify additional fictitious accounts
- Unusual usernames—for example, ones that only have a first name, or a group of accounts with usernames that have a fixed pattern
- Membership in numerous Facebook groups, most of them on political issues or related to the content areas of the operation
- Creating groups on Facebook and WhatsApp as well as Telegram channels with the name of the activity and aiming to promote the content of the operation
- Posting content at consistent times.

The list of characteristics below differentiate between locally coordinated inauthentic activity and foreign interference. Many of the signs included in this list relate to the use of language and understanding of the cultural-social context, which makes it possible to distinguish between an inauthentic Israeli account and a foreign agent. It is important to note that as artificial intelligence technologies improve, some of these suspicious indicators could disappear. Among them, we can note the following characteristics:

- Errors in Hebrew when writing original content or in correspondence with Israelis
- Backward question marks that can indicate the use of a keyboard in Arabic or Persian
- Repetitive content and sharing controversial and sometimes inflammatory issues.
- Complex systems that operate across multiple platforms over time, backed by significant organization with resources and infrastructure for conducting an influence operation

- Platform confirmations (Facebook, Twitter) that these accounts are operating from outside of Israel. Usually, the platforms will not state the precise source of the activity

- Time difference from Israel (in screenshots for example)

- The use of non-Israeli phone numbers from outside of Israel (for example, from the Palestinian Jawwal network or other area codes that are not +972) for WhatsApp users.

In some cases, evidence makes it possible to determine with a high degree of certainty that an operation is conducted by an Iranian body:

- Screenshots and reports from internal sources (such as Facebook) indicating that the device is set to Iran's time zone, the interface language is Persian, or confirming the identification of inauthentic networks as part of influence operations active in Israel.

- Linguistic errors in original Hebrew texts characteristic of Persian speakers, as verified by linguistic analysis.

Based on the outlined above, it can be inferred that Iran is behind most of the operations analyzed in this research. The content and nature of the interference operations' activity suggest that the operators' primary objective is to intensify internal polarization in Israel by discussing controversial issues and by magnifying and exaggerating messages (for example, by focusing on controversial issues and **amplifying extreme messages**, such as comparing Israeli leaders to Hitler and **embedding** antisemitic content).

The focus on content relating to internal Israeli issues, such as elections or political protests, suggests a possible intent by the operators of these influence operations to interfere with Israel's internal discourse and disrupt or influence democratic processes.

In addition to goals related to cognitive efforts and influencing mindsets, some of the operations also involve clear attempts to directly contact Israelis. In the operations studied, these individuals were political activists. Direct contact with Israeli citizens creates a different form of foreign interference, as it involves a hostile foreign agent using Israeli citizens without their knowledge.

Part 4. Lessons from Foreign Interference in Social Networks in Israel

In addition to the value of being the first in-depth study examining foreign interference operations in Israel, we also see its methodological value for conducting similar studies in the future, as well as the tools and technologies necessary for this purpose.

Insights on Foreign Interference Operations in Social Networks

A focus on controversial issues. The operations studied encompass a wide range of issues that are central to the Israeli discourse. It seems that those behind the interference operations have a deep understanding of current events in Israel and adapt their content to address controversial issues. These issues include support for the opposition to current prime ministers, Israeli elections, among others. The content shared also demonstrates familiarity with current events in Israel, such as the cost of living, COVID-19, and so forth.

The investment of resources in the development of influence operations as a sign of state interference. It is clear that significant efforts are made to create accounts that appear authentic by posting substantial content over time. In doing so, these fictitious accounts build credibility. In this way, the fictitious accounts gain credibility, and the communities and channels that they manage attract new followers organically, as people add their friends. This level of investment suggests the involvement of a state entity or entities behind these operations, with significant resources invested in interfering with what is happening in Israel.

Routine activity along with special events. The foreign interference operations on social networks are ongoing, but they also strategically time their actions around key events. As revealed in the interference operations we have studied, the operators identify opportune moments within Israeli public discourse and specific content areas upon which to focus. For example, there are operations that specifically target current events, such as the Knesset elections.

Few responses alongside studying the Israeli public. Despite the significant efforts invested in most of these interference operations, the majority have failed to generate significant publicity or provoke responses from Israeli users. However, it is important to consider two kinds of responses and their implications. First, Israelis have become aware of the presence of hostile influence agents on social media, and they warn about this and respond to them accordingly. Indeed, awareness of the phenomenon has increased over the years, partly due to reports in leading media outlets both in Israel and abroad. The realization that foreign agents are involved in internal discourses could create a sense of insecurity,

mistrust, and vulnerability. However, it is possible that this awareness has not gained much attention among the Israeli public because these operations are woven into a domestic discourse of hatred, making it difficult to distinguish the foreign interference (which is disguised as being Israeli) from the authentic internal discourse.

In addition, more sophisticated operations, such as infiltrating WhatsApp groups and creating personal connections through them, have led to situations where Israeli citizens have unknowingly shared information with hostile agents. This poses a risk to Israel's national security and exploits innocent citizens who are unable to distinguish fake users from real ones and view fake accounts, groups, and channels as credible. The public's ability to cope with this challenge depends, in part, on the public's level of digital literacy, and some populations are more vulnerable than others in this sense.

Challenges Inherent in Researching Interference Operations in Social Media

The "glass ceiling" of civil society. It is difficult to prove links with foreign agents without the support of a third party. This study illustrates that without support from third parties—such as assistance from the technological platforms themselves or members of the security establishment—confirming with certainty that accounts are fictitious and that interference operations are conducted by foreign agents is difficult. In most of the cases examined, except for those in which there was direct communication with the operators of the operation, it was not possible to state with absolute certainty that the accounts were part of a foreign influence operation.

"An analogue study in a digital world." One of the main difficulties of this study was that it relied primarily on analyzing static screenshots of accounts and content. When the study was conducted, much of the content had already been removed from the internet. This limited the ability to add analytical and statistical dimensions to the analysis, perform semantic analyses, and identify patterns in the different operations, in addition to constraining the insights that we could derive from the existing content.

Difficulty Estimating the Impact of the Interference Operations and the Risk Posed to Israel's Security

A major challenge in studying foreign interference operations on social networks is the difficulty of estimating their impact on Israel's security, democracy, and national resilience.

This difficulty is similar to measuring marketing efforts aimed at influencing public opinion, as their impact is not necessarily measurable. While operations on many networks have been conducted over a long period without significant achievements, such as accumulating a large following, it is still difficult to accurately estimate their influence on Israel's national security, even when potential damage exists. For example, during the Balfour protests in 2020, a high-ranking police officer read a call for violence against the police from a social network account during a television broadcast, relying on a fake account posing as one of the protest organizations.[11] Such incidents can deepen rifts and tensions in Israeli society and influence the Israeli discourse. Due to the difficulty of estimating the impact of foreign interference operations on social networks and the intentions behind them, it is also challenging to assess the potential dangers they pose.

Part 5. Addressing Foreign Interference Operations in Social Networks in Israel

Addressing the threat of foreign interference in social networks requires a methodical and systemic approach in cooperation with the variety of entities involved—the security establishment and the tech companies that operate the platforms where the operations are conducted—as well as adapting regulations in Israel to address the problem and involving the public via the media and civil society organizations in the initial identification of suspicious accounts.

Lack of Systemic Treatment of the Threat of Foreign Interference Operations in Social Networks in Israel

The main conclusion drawn from this research is that there is currently a lack of a systematic approach for addressing foreign intervention in social networks in Israel in an organized and methodical manner, from the moment the threat appears until its removal by social media companies. This indicates a need for ongoing, systematic, and continuous research into the phenomenon. Additionally, in our view, a comprehensive perspective is missing—from identifying the operations and assessing the threat they pose, to exposing the networks to the public through the media, and ultimately, removing them from the internet.

Difficulty for Security Agencies in Operating within the Public Civilian Sphere on Social Networks

[11] Lior Kenan and Amit Maniv, "The Police: The Claim that Demonstrators Called for Violence Was Based on Fake News," [in Hebrew] Channel 13, https://13tv.co.il/item/news/politics/security/fake-news-police-crime-minister-1139597/

Foreign interference operations usually take place within the public civilian sphere of social networks, which allows Israelis and foreign entities to interact, posing a significant challenge for the Israeli security forces. The challenge is not only technical, but it also involves concerns about infringing upon the freedom of expression of Israeli citizens, and the fact that sometimes it is not possible to determine with certainty that these are foreign entities. That is, it is possible that those attempting to influence the Israeli discourse by means of coordinated, inauthentic behavior are local. The involvement of civil society bodies could reduce the harm to democratic foundations since civilians report the suspicious profiles and activity, not security agencies. Moreover, intelligence agencies naturally prefer to operate in covert environments, further explaining their limited presence in the public areas of the internet.

The Role of Social Networks in Addressing Foreign Interference

The companies that operate the social networks—primarily Twitter and Meta, which owns Facebook, WhatsApp, and Instagram—play a decisive role in addressing foreign interference operations. First, the companies have access to information that allows them to identify and monitor foreign interference attempts over time. Moreover, they can remove accounts that are part of these operations. Currently, their technological capabilities in the Hebrew language result in insufficient filtering and identification of content that violates Meta's community standards.

Existing legislation in Israel is not suitable for addressing foreign interference operations on social networks because it does not provide a means for citizens to directly contact the platforms. There is no clear government point of contact for citizens to report incidents on the networks, no prohibition on the trade of fake user profiles, no legislation mandating the monitoring and removal of fake accounts by the platforms, and insufficient international cooperation with other countries dealing with similar threats on social networks in the legislative, investigative, diplomatic, and intelligence contexts. Another issue is the lack of a direct channel of communication that allows Israeli citizens to contact the tech companies that operate the social networks.[12]

The Dilemma of Media Exposure: Increasing Public Awareness or Strengthening Hostile Agents?

[12] Digital Sovereignty: How the New Government Should Address the Dissemination of Fake News and Influence Operations [in Hebrew], INSS, https://www.inss.org.il/he/publication/truth1/

One of the main approaches globally in dealing with disinformation and post-truth is educating the public on digital literacy.[13] From this perspective, exposing foreign interference operations on social networks in Israel helps raise the public's awareness and increase skepticism toward fake accounts or those suspected of being fake. In other words, media exposure has value in improving the general public's digital literacy, and the public can be enlisted in actively taking part in identifying suspicious accounts.

However, it is also important to understand the cost of exposure and its long-term consequences. First, exposing the networks can embolden their operators, incentivizing them to continue their interference operations by demonstrating their impact on the Israeli public, gaining publicity, and influencing the national agenda. In addition, once the operations are exposed, they can be used as a tool for political mudslinging, thus serving the goals of the operators and deepening the divisions and rifts within Israeli society.

Part 6. Recommendations for Action, Policy, and Legislation

Systemic Recommendations:

One of the main conclusions is that currently no single body in Israel conducts systematic and consistent research regarding the threat of foreign interference on social networks in Israel. As a result, the issue falls between the cracks and relies on the efforts of the security establishment and civil society, which address it in an uncoordinated manner. Although the issue falls under the responsibility of the Israel Security Services (Shin Bet), there are reasons why it does not receive optimal attention. Our recommendation is to establish a dedicated body for in-depth and ongoing research on interference operations. This body should focus not only on real-time removal but also on identifying patterns of activity, characteristics, and so forth. This body will require intelligence, technological, and analytical capabilities. Working in synchronization and coordination with all relevant actors, this body should consider all the implications, including the decision of when to expose foreign influence networks to the public. Establishing this body will help regulate the relationship between intelligence agencies and civil society organizations.

A systematic and continuous study of the issue will provide deeper insights into the adversary's patterns of action. It will also allow for better and faster identification of interference operations on social networks and prompt response

[13] For an example of addressing misinformation in Finland via educating the public on digital literacy, see Jenny Gross, "How Finland Is Teaching a Generation to Spot Misinformation," *New York Times*, January 10, 2023, https://www.nytimes.com/2023/01/10/world/europe/finland-misinformation-classes.html

to intervention operations in emergencies and routine situations. Ongoing study of the issue will help monitor the learning and development of interference operations and equip the public with tools to deal with them. We recommend strengthening the research on foreign influence and intervention in social networks within the security system as well as among civilian entities such as research institutes and NGOs.

Meanwhile, the intelligence community, led by the Shin Bet, should expand its involvement in addressing the threat of foreign interference in social networks in Israel. This expansion should involve continuous activity, beyond just elections, and additional bodies besides the Shin Bet should be included.

While this study focused on interference operations on social networks where content was posted only in Hebrew, it is imperative to continue researching operations that target Israeli citizens who speak other languages, such as Arabic, Russian, Amharic, and so forth.

Furthermore, it is important to expand research to additional platforms where interference operations are used, such as TikTok and LinkedIn, which were not examined in this study. Over time, monitoring should be expanded to any new social networks that develop. Additionally, it is essential to monitor new technologies employed by interference operators**,** such as generative AI technologies.

Recommendations Relating to Government Ministries

With respect to government bodies, there should be increased awareness of the threat of foreign interference and influence in democratic processes in general, and in social networks in particular, as a significant new threat to national security and resilience. To this end, **awareness should be raised among individuals in relevant government ministries** (the Ministry of Justice), law enforcement (the Israel Police), and the relevant authorities (the Central Elections Committee, National Cyber Directorate, NSC, National Digital Agency), which should be designated as responsible for addressing the problem. Moreover, the public should have an accessible means to report possible foreign interference on social networks. Increasing the awareness of government bodies can lead to the advancement of necessary regulation on social networks.

Recommendations Relating to Regulation in Israel

There is a need for legislation that would require the major social networks to create a direct communication channel for Israeli residents to report complaints

and receive clarifications related to content. In addition, legislation should prohibit the trade in fake users and empower state authorities to take action against the operators of fake accounts. It should also obligate the platforms to monitor and remove these accounts and to cooperate with other countries in addressing the risks of foreign interference in social networks within the legislative, investigative, diplomatic, and intelligence contexts. In this framework, it is necessary to supervise and restrict the architecture of the platforms, including their algorithmic engine and business models, while maintaining the end users' freedom of expression. Finally, there is a need to update privacy legislation in Israel.

First, tech companies should invest in allocating resources and technologies that are adapted to the languages spoken in Israel, primarily Hebrew and Arabic. Relevant recommendations can also be found in **Facebook's report following Operation Guardian of the Walls.** Social networks should **allocate local monitoring teams** and deploy **fact-checkers familiar with Israel's languages and cultures.** It is important to ensure that the service is **responsive to Israeli queries, aligned with local time zones,** and that inquiries by civilian and state bodies are answered in a sufficient time period before events on the social networks get out of control.

The Committee to Adapt the Law to the Challenges of Innovation and the Acceleration of Technology (the Davidi Committee), which operated on behalf of the Ministry of Justice in the 36th government, called for the establishment of a regulatory body for digital activity.[14] Currently, the state's contact with the platforms is managed by the Ministry of Justice's Cyber Unit. In 2020, over 4,000 requests to remove information from social networks were submitted to the Cyber Unit by security agencies, constituting 94% of all the requests made. In the case of Adalah v. the State Attorney—Cyber Unit, the High Court of Justice (HCJ) determined that "the activity of the Cyber Unit in its current format is essential to the immediate preservation of national security and social order, but it is not free of difficulties, which relate mainly to the problem of authorization in primary private legislation for the unit's activities." The Ministry of Justice is not authorized in legislation to take action against the social networks; thus, the HCJ recommended arranging such authorization in legislation.

[14] Ministry of Justice, "Summary of the Committee's Work on Adapting the Law to the Challenges of Innovation and Accelerating Technology, Regarding Illegal Content in the Digital Space," [in Hebrew] October 2022, https://www.gov.il/BlobFolder/guide/davidi-committee-main/he/committee-summary.pdf

At the same time, in the 36th government, a committee in the Ministry of Communications examined regulating digital content platforms.[15] One of the committee's proposals, which was adopted in December 2022 by the former minister of communications,[16] was the establishment of a public council with the purpose of increasing the supervision of social networks. According to the proposal, the council would be chosen by government and civil society leaders and would serve as a contact point for public complaints about foreign interference as well as to help formulate policy.[17]

In general, we recommend removing any coordinated inauthentic activity suspected to be foreign, regardless of its impact, the messages published, or actions taken following its activity. It is essential to reach an understanding with tech companies to share information about foreign interference operations they identify on social networks targeting Israel and to deepen research and understanding of adversary activities with maximum transparency.

Recommendations Relating to Civil Society

This research highlights the critical role of research institutes and civil society organizations in addressing the phenomenon of foreign interference in social networks in Israel. These entities are able to identify and monitor potential cases of foreign interference, raise public awareness about this phenomenon, and advance targeted research on this issue. However, this study also illustrates the limitations of civil society in dealing with the issue and the need to cooperate with state bodies and tech companies that operate the platforms to effectively address and mitigate the issue.

Recommendations Relating to the Israeli Public

Enhancing the public's digital literacy is crucial so that Israeli citizens can learn to identify fake accounts that operate in their digital environment and attempt to mislead them as part of interference operations. Responsibility should be given to a body that addresses this issue regularly, and not just around events such as Knesset elections or wars. One possibility is to incorporate the subject into the

[15] The Advisory Committee to the Minister of Communications on Examining the Regulation of Digital Content Platforms, "Recommendations of the Committee," [in Hebrew] December 2022, https://www.gov.il/BlobFolder/reports/14122022/he/Report-digital-platforms.pdf

[16] Ministry of Communications, "Report of the Advisory Committee to the Minister of Communications on Examining the Regulation of Digital Content Platforms," [in Hebrew] December 14, 2022, https://www.gov.il/he/pages/14122022

[17] Tamir Hayman, David Siman-Tov, and Amos Hervitz, "Regulation of Social Media in Israel," INSS Insight No. 1679, January 8, 2023, https://www.inss.org.il/publication/social-media/

curriculum of the Ministry of Education and to appoint the National Digital Unit to be responsible for promoting digital literacy among the adult population.

Additionally, partnerships should be initiated with relevant bodies around current events that could serve as fertile ground for foreign interference operations, such as the Home Front Command during military operations, the Central Elections Committee during election campaigns, and so forth. The main issue is to appoint a dedicated body responsible for this issue in routine times, which will receive budgets for public awareness and education efforts. The public council mentioned above, which includes public representatives, could be the basis for such a body. Other relevant entities include the National Cyber Directorate, the Ministry of Intelligence, civil society organizations, and research institutes that can characterize the phenomenon and develop ways to address it. When a communication channel is established between the public and the tech companies that operate the social networks, and a clear national point of contact is created to which the public can report security incidents on social networks, it will be important to inform the public of their existence and encourage their use. This way, the public can also complain about interactions with foreign agents.

Recommendations Relating to the Traditional Media

The traditional mass media—television channels, news sites, radio, and newspapers—play a role in increasing the public's awareness of foreign interference operations in social networks. Thus, it is important for the media to expose some of the operations to improve the public's digital literacy. However, there is a risk that media exposure may encourage the agents behind such interference operations to continue their activities within the social networks in Israel. After considering the various perspectives, we have concluded that, as a rule, it is worthwhile to publicize these interference attempts. The consideration of raising public awareness (as part of a means of protection and creating resilience) outweighs the concern of giving resonance to foreign subversive activities. However, in cases where national security is at risk, or there is a potential to enhance the research and achieve significant insights by monitoring the operation, delaying public disclosure should be considered. To facilitate this, the establishment of a military-civilian advisory forum is recommended. Furthermore, it is also important to raise awareness among journalists who specialize in covering state and security issues across different media platforms regarding the existence of interference operations on social networks, including the spread of disinformation. This would enable them to deepen their understanding of the impact of these operations on Israeli democracy, given how the incidents can spill over from the internet to traditional media.

Recommendations for Future Studies

To understand the current state of foreign interference operations and the latest approaches used, **ongoing, systematic research is needed**. This research should focus on identifying patterns of the adversary to see how operations change and develop over time. It is important to investigate the causes of these changes, whether they result from measures taken by Israel or steps taken by the social networks themselves, and so forth. Technological developments, for example, such as the accessibility of generative artificial intelligence technologies can affect these operations in ways that challenge some of the insights presented in this study (for example, identifying foreign interference operations based on elements related to language, reducing the need to steal photos because it is possible to create photos for fictitious accounts that look credible, and more). In 2022, over two-thirds of the coordinated, inauthentic operations on Meta used accounts with photos generated by GAN technology. The operators may think that by using these pictures, their accounts appear more authentic and genuine and can deceive bodies that investigate interference operations and rely on overt information. This presents a significant challenge in identifying and investigating interference operations. Changes in interference operations can also be influenced by the emergence of new social platforms, such as Telegram or TikTok, and increased usage of them. The way that fake accounts operate in interference operations has also changed, and a transition to smaller, more focused operations is evident, where fewer accounts are involved compared to larger and more disruptive operations seen in the past. This type of systematic and consistent research of interference operations should rely on a range of information sources, including a mechanized framework for information gathering and analysis, as well as information collected and published by research bodies and civil society organizations both in Israel and abroad. Effective identification, warning, and research efforts require a combination of skilled analysts, technological tools capable of handling and preserving large amounts of information, as well as issuing urgent warnings about significant incidents on the internet.

Among the challenges in the field, attributing the accounts to the organizations and individuals behind them, as well as providing concrete proof of their involvement and incriminating them are particularly difficult. This difficulty is rooted in user privacy protection provided by the social networks, which includes masking identification data and other user details. Consequently, it is impossible to discover IP addresses, email addresses, geographical locations, and phone numbers of accounts in general, and especially those involved in inauthentic activity. In contrast, automated tools for alerting, connecting, and monitoring interference operations could be highly effective.

We recommend emphasizing the technological context in the following fields:

1. Invest in a reliable database that is updated over time—a fundamental component of any "defensive enterprise" needs to have the ability to "harvest" and "store" information from the relevant networks over time. To effectively combat interference threats over a wide variety of platforms (TikTok, WhatsApp, Telegram, Facebook, Twitter, Instagram, Reddit, and more), it is necessary to implement various methods of retrieving the information and gathering it over time for the purpose of applying statistical analysis and performing retroactive identification of malicious accounts.

2. Invest in metadata tools for identifying suspicious, coordinated online activity.

3. Invest in semantic processing and content-based processing tools to automatically detect "inflammatory" messages, to identify posts that have common language errors indicating they were written by non-Hebrew speakers (requires research), and to detect content created by deepfake algorithms as part of addressing the growing challenge in the field of generative AI.

Iranian Foreign Information Manipulation and Interference During the Swords of Iron War

Nitsan Yasur and Danny Citrinowicz[1]

In recent years, Iranian actors have carried out a range of hostile influence operations as part of the Israeli public discourse, aiming to expand social and political rifts, create political tension and chaos, and encourage demonstrations and distrust of the government and its democratic institutions. Since the outbreak of the war in Gaza, the Iranian influence operations have focused on issues related to the war and the attempt to sow distrust and demoralization, incite violence against Arab citizens, and deeply penetrate the discourse surrounding the issue of the return of the hostages. These operations have been conducted on a variety of social media platforms, have used artificial intelligence tools, and have simultaneously attempted to influence both the general public and individuals to advance the operations' objectives.

The Iranian influence operations blur the boundaries between the digital realm and the physical world, as well as between influence, recruitment, activation, and intelligence-gathering practices—a combination that produces new threats in the digital realm. The State of Israel should respond to the threat of Iranian influence efforts in the digital realm. It should work toward an integrated solution that includes diverse spheres of action—legislation, developing technological solutions, advancing research and public literacy—while involving all the players in the field, such as the security forces, research bodies and academia, the media, civil society organizations, legislators, social media platforms, and tech companies.

The use of the digital dimension in war aims to undermine citizens' ability to clarify reality and blur the lines between truth and lies, victims and perpetrators, and winners and losers. The enemy not only uses fake accounts and floods the internet with manipulative content and narratives, but it also receives assistance from local forces within Israel. The enemy promotes or supports local content while exploiting local people who echo and disseminate its content and narratives. This

[1] Nitsan Yasur is a researcher on disinformation and social networks. Danny Citrinowicz is a research fellow in the Iran Program at INSS.

phenomenon represents an increased blurring of the country's sovereign borders, the boundaries between the physical world and the digital realm, as well as those between influence operations, intelligence gathering, and recruitment. [2]

The social media platforms have, in a sense, become "mediators" in the information war, enabling hostile agents to widely disseminate harmful content and false information on their platforms. These platforms, which were once seen as promoting open communication, have now become the main arena where the digital dimension of war takes place, with the enemy exploiting them to disseminate disturbing content, incitement to violence, and false claims.[3]

This article examines the Iranian influence operations that have been carried out in Israel during the Swords of Iron war from October 2023 to May 2024. It relies on a broad analysis of social media accounts that were part of influence operations active in the Israeli discourse from 2020 to 2022, which were published in the Israeli and international media and described in depth in the article "Foreign Interference and Iranian Influence in Social Networks in Israel."[4]

We begin the article by describing the target audiences of the main influence operations during the first few months of the war. We then present an analysis of the phenomenon, identifying main patterns and describing significant case studies of the operations. Finally, we provide a look into the future, including an assessment and recommendations for state authorities, the companies that operate the platforms, media organizations, civil society, and the public.

Iran in the War in Gaza

To better understand Iran's cyber operations during the war in Gaza, it is essential to first examine Tehran's interests in the military campaign. Iran's involvement is driven by specific strategic objectives of the Iranian regime and does not occur in isolation.

---

[2] This article is part of a memorandum that will be published soon on foreign influence and interference as a strategic challenge. The memorandum includes articles that examine the challenge from the perspective of adversaries (such as Russia and Iran), and discusses aspects of influence methods. It will also include an examination of the challenge during normal times and during the disruption of democratic processes, the deepening of social rifts, election campaigns, and wars. The articles reflect a connection between systemic understandings and the policy needed to address it in Israel and in Western countries. The memorandum concludes a joint project of the Institute for National Security Studies and the Israel Intelligence Heritage and Commemoration Center (IICC).

[3] Tehilla Shwartz Altshuler, "The Fourth Dimension of the War is Undermining Israelis' Ability to Clarify Reality," [in Hebrew] Israel Democracy Institute, November 7, 2023, https://www.idi.org.il/articles/51289

[4] Inbal Orpaz and David Siman-Tov, "Foreign Interference and Iranian Influence in Social Networks in Israel," [in Hebrew] Special Publication, Institute for National Security Studies, June 10, 2024, https://www.inss.org.il/he/publication/iranian-influence/

After Hamas's invasion of southern Israel on October 7, the Iranian leadership was caught off guard by the timing of the attack.[5] In response, the Iranians made a strategic decision to push for a quick ceasefire, aiming to maintain Hamas as a significant military and political force in the Gaza Strip.[6] To this end, Iran activated its proxies—Hezbollah, the Houthis, and the Shiite militias in Iraq—to target both the Israeli army and the American presence in the region. The objective was to exert pressure on Washington to cease its support for Israel or to force Jerusalem to end the conflict. At the same time, Tehran sought to avoid a direct military confrontation with Israel, fearing it could escalate into a broader conflict with US forces in the Gulf, especially given Washington's unprecedented show of support for Israel, including deploying aircraft carriers to the region and issuing a clear warning to Iran not to intervene in the war ("Don't!").

Given this policy, Iran viewed the cyber domain as the only way to directly increase friction with Israel during the war without risking a direct Israeli response. Tehran believed that through cyber, it could exact a price on Israel while avoiding attribution, given the difficulty of proving Iran's involvement.[7] In this way, Tehran aimed to fulfill its strategic objectives without incurring significant repercussions. Moreover, the fact that Iran had been conducting large-scale influence operations against Israel for some time without escalating tensions likely bolstered its confidence in continuing and intensifying these operations. Iran believed that it could accomplish its goals using the same infrastructure, modus operandi, and especially the same tools. It appears that Iran believes that weakening Israel's internal cohesion during the war could expedite or at least promote the understanding within Israel of the need to end the war in Gaza, aligning with Iran's objective of avoiding a large-scale escalation.[8]

It is important to note that the cyberattacks carried out by Iran since October 7 have aimed to support these objectives. Iran has targeted "support" infrastructure critical to Israel's military operations, such as civilian hospitals that have weak defenses. These attacks have served the cognitive aspect of Iran's strategy and allegedly have damaged critical infrastructure, hampering Israel's war efforts. Iran has even glorified these operations, effectively hitting two birds with one stone, as it increases the pressure on the Israeli government to stop the war. It seems that Iran believes that a combination of actions by its proxies and its own direct cyber

[5] "Swords of Iron: The Iranian Leadership Was Surprised by the Attack on the Gaza Envelope," [in Hebrew] *Maariv,* October 11, 2023, https://www.maariv.co.il/news/world/Article-1044274
[6] Ece Goksedef, "Iran Warns Israel to Stop War in Gaza or Region Will 'Go Out of Control,'" BBC News, October 22, 2023 https://www.bbc.com/news/world-middle-east-67188346
[7] Chuck Freilich, "The Iranian Cyber Threat," Memorandum No. 230, INSS, February 2024, https://www.inss.org.il/publication/iranian-cyber/
[8] "Kamal Kharazi, "Khamenei's Advisor: Iran is Not Interested in Regional War," [in Hebrew] *Maariv*, July 2, 2024, https://www.maariv.co.il/news/military/Article-1111765

actions “below the threshold of escalation” allows it to achieve its strategic objective of preserving Hamas in Gaza, without paying a heavy price in a direct conflict with US forces in the region.

The Findings

The Iranian influence operations focus on exploiting existing disagreements and rifts. It is not surprising that the Iranians took advantage of the war in Gaza to interfere and attempt to exert influence. They have used this opportunity to advance their strategic objectives by capitalizing on internal tensions in Israel, such as the hostage issue, the number of casualties, the lack of trust in the government and government institutions, and lack of confidence in the security forces, as well as the escalating divisions within Israeli society.

Iran’s influence operations are evident in various issues, particularly those that are controversial and receive significant public attention. The operations and the profiles they use have addressed a wide range of topics. These operations have not been limited to advancing a specific political agenda or candidate but rather have focused on whoever they believe would serve their interests most effectively. The operations described in this study were carried out using fake social media accounts, which can be attributed with a high degree of certainty to foreign state entities, specifically Iranians. The identification of these operations is based on statements by the General Security Service (Shin Bet) and their publication in the media. This study specifically examines seven foreign influence groups that were active during the first six months of the war in Gaza, from October 2023 to May 2024.

The Foreign Influence Operations in This Study

Aryeh Yehuda News Flashes

The goal of this operation was to spread propaganda and false information while posing as a local news updates channel. The operators opened groups on various platforms, including WhatsApp, Telegram, and Facebook, presenting themselves as an extreme right-wing Israeli group. Through these accounts, they disseminated incitement against Arab Israeli citizens, imitating a local extremist right-wing channel. They also targeted the security forces and various public figures, seeking to sow chaos and division in Israeli society. In addition, they attempted to encourage violent gatherings outside hospitals, spreading disinformation about “terrorists” being hospitalized throughout Israel, as discussed below.

Egrof (Fist)

This operation presented itself as an extremely right-wing Kahanist group, using TikTok, Instagram, Twitter, Facebook, and WhatsApp. This group disseminated extreme content, with the aim of sowing divisions and tensions in Israeli society and increasing friction between Jews and Arabs, as well as incitement against the Israel Security Forces. Those behind this operation also attempted to contact real Israeli activists and promote a demonstration in Jerusalem, causing significant security tensions.

Dema'ot HaMilḥama (Tears of War)

This operation maintained a database of individuals who had been murdered, killed, or taken hostage. It posted stylized content with photographs and promoted content to inflame tensions and encourage radicalization. This group also engaged in deceptive recruitment tactics, specifically targeting Israelis and enlisting their help in performing tasks related to the hostage issue, such as putting up signs in public and assisting with local procurement. It even went as far as to publicize "job offers" on various job search websites and groups.

BringHomeNow

This operation utilized Telegram and embedded itself into legitimate, authentic online activity, using names and hashtags that were similar to those used by the Hostages Families Forum.[9] Its main goal was to establish a local presence and collect personal information from Israelis by directing individuals to a "volunteer" form where they were asked to fill out their personal info. As part of their efforts, signs bearing this operation's name were put up on bus stops in Tel Aviv, and it even ordered a wreath for the family of one of the hostages.

Ḥasrot onim (Helpless)

This operation sought to embed itself in the local discourse while disseminating messages that aimed to demoralize Israeli women, including female soldiers, women who had been injured or killed, and female hostages, by portraying them as "helpless."

Kan+

Digital assets were used to promote a fake platform for conducting research and surveys, leveraging visual elements associated with the Kan 11 TV channel. The

[9] The mistake in the name is intentional. The idea was to be similar to the original BringThem HomeNow but not be identical.

apparent objective of this operation was to gather information about Israelis who contacted them and responded to their surveys.

Second Israel

For more than two years, this operation focused on various issues in the Israeli public discourse.[10] In 2021, it simultaneously operated multiple social media accounts that opposed religious influence, supported the separation of religion and state, and championed the rights of the LGBTQ+ community. However, this operation also maintained accounts that impersonated well-known rabbis and incited against secular people, women, and the LGBTQ+ community. During the elections for the 25th Knesset in 2022, this group worked to influence left-wing supporters, disseminating messages against Itamar Ben-Gvir by portraying him as "dangerous for Israel," while at the same time promoting a campaign about "election fraud" led by supporters of the Likud Party and the right wing. Following the outbreak of the war in Gaza on October 7, this operation shifted its focus and began responding to the ongoing events. It promoted a "treason from within" conspiracy theory and incited against the protestors who opposed the "regime coup." At the same time, it also blamed Netanyahu for the October 7 events while disseminating videos of Netanyahu created using deepfake technologies.[11] The same operation promoted a deepfake video depicting several well-known rabbis blaming Netanyahu for the debacle that led to the October 7 events.

The Diverse Target Audiences of Iran's Influence Operations—Playing On Every Team

The attempt to simultaneously target all sides using influence operations has already been described in a previous study.[12] An example of this can be demonstrated in two graphic images that were published by the same operation, targeting both supporters and opponents of Netanyahu and Bennett (see Figure 1). Another example can be found in the "Second Israel" operation, which lasted for two years and was exposed in *Haaretz* newspaper about two months after the war began. [13] Even before the outbreak of the war, this operation had been discussing various current events in the Israeli discourse, and in 2021, and again

[10] Omer Benjakob, "Fake Rabbis and AI-Bibi: For Two Years, A Foreign Network Sowed Chaos in Israel," *Haaretz*, December 20, 2023, https://www.haaretz.com/israel-news/2023-12-20/ty-article-magazine/.premium/fake-rabbis-and-ai-bibi-for-two-years-a-foreign-network-sowed-chaos-in-israel/0000018c-8710-de71-a3ee-e75ba3900000

[11] Refaella Goichman, "The Presenter Is Not the Prime Minister: Foreign Network Poses as Netanyahu, Using Deepfake Technologies," [in Hebrew] *TheMarker,* December 13, 2023, https://www.themarker.com/captain-internet/2023-12-13/ty-article/.premium/0000018c-62ca-dbd5-a39c-fffbbda70000

[12] Orpaz and Siman-Tov, "Foreign Interference and Iranian Influence in Social Networks in Israel."

[13] Benjakob, "Fake Rabbis and AI-Bibi."

following October 7, it began to operate different accounts sharing opposing messages, as discussed above.

The Iranian influence operations target different audiences simultaneously in the digital realm. In the current context, there are several main themes directed at the different target audiences on both ends of the political discourse:

- Expanding military force, continuing the war, and even resettling the Gaza Strip;
- Returning the hostages as part of a deal and ending the war;
- Protesting against the judicial coup and appealing to opponents of Netanyahu
- Supporters of Netanyahu and the government.

Figure 1. Simultaneous Campaign Directed at Different Target Audiences by an Iranian Influence Operation

Note: On the left, "Netanyahu... is the real COVID in Israel." On the right, "Bennett . . . is the real COVID in Israel." *From* Orpaz and Siman-Tov, "Foreign Interference and Iranian Influence in Social Networks in Israel."

Several groups, such as "Fist" and "Aryeh Yehuda News Flashes," promoted and echoed calls to continue the war and intensify the use of force, with some advocating for the conquest of the Gaza Strip and the establishment of settlements in Gush Katif. In contrast, a few groups such as "BringHomeNow," "Tears of War," "Helpless," and the "Second Israel," called for prioritizing the return of the hostages through negotiation and a ceasefire.

These groups targeted distinct audiences even before the war broke out, aiming to exacerbate and widen social divisions. Some groups promoted statements against the government, calling for Benjamin Netanyahu's removal, while others disseminated inflammatory messages, blaming the opponents of the "judicial

reform" and the "Kaplan protestors" for the October 7 events. In addition, these groups sought to incite real-world violence against Israel's Arab citizens.

A Shared Modus Operandi of the Operations

The influence operations followed a similar modus operandi to those described in previous studies.[14]

Digital Assets Across Multiple Platforms

The Iranian influence operations extensively utilized major social media platforms, including X (formerly Twitter), Facebook, Instagram, YouTube, WhatsApp, and Telegram. An analysis of these operations within the context of this study reveals a focus on the "quality" of the digital assets (accounts, channels, and so forth) rather than their "quantity." Although the number of operations spanned different social media platforms, the number of active profiles was relatively limited but of high quality. That is, the Iranian operations chose to invest resources in managing a smaller number of high-quality digital assets rather than a large volume of lower-quality ones.

Branding and Organizing Around a Central Fictitious Body or Organization

The Iranian influence operations were clearly organized around a central "brand" while building and investing in digital assets across various social media platforms. The choice of operation names and images, logo design, and consistent design themes for graphic publications demonstrated a deep understanding of the local Israeli discourse and nuances. The advanced preparation of these digital assets gave them a professional image and enhanced their credibility. By investing in the development of a comprehensive and consistent "brand," the influence operations were able to establish clear identities that could be adapted to the different target audiences.

A Support Network of Fake Profiles

To support the branded digital assets of the various operations and enhance their credibility, a limited number of high-quality fake accounts, posing as belonging to Israelis, were used. These accounts specifically served as "contact people" for communication about the campaigns and messages promoted by the operation. In addition, a large number of lower-quality fake accounts (bots) were sometimes used with less effort. These accounts played a role in increasing visibility by reposting materials, hashtags, and messages across the various social media

[14] Orpaz and Siman-Tov, "Foreign Interference and Iranian Influence in Social Networks in Israel."

platforms. These accounts also artificially promoted the main digital assets through likes, shares, comments, and direct referrals.

Expanding the Activity to Additional Internet Services Compared to Previous Operations

In addition to utilizing social media platforms, there has also been a growing trend of using other free and open internet services for information gathering, such as Google Forms, petition websites like Drove, landing pages that consolidate the various digital assets, and PayPal accounts for fundraising.

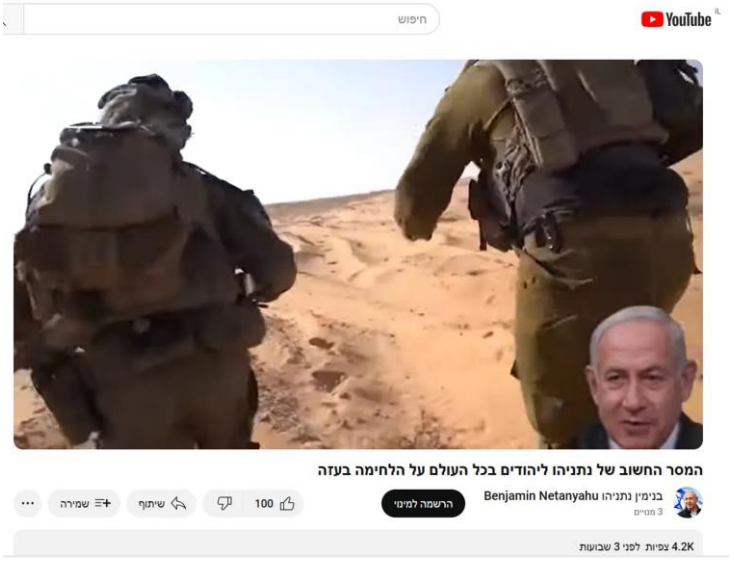
Use of AI Tools

One notable application of AI tools during the war in Gaza has been to design and disseminate placards and deepfake videos. While these AI products are not yet at a perfect level of production, their quality is relatively high, and they can easily deceive citizens, the media, and elected officials. Moreover, the quality of these AI products, as well as the extent of their distribution, is rapidly increasing. As a result, they present a significant challenge in identifying, monitoring, verifying, and countering false information.

"The Second Israel" disseminated two deepfake videos as part of its operation. In the first video, Prime Minister Netanyahu supposedly speaks to world Jewry and explains in English why he is not responsible for the October 7 massacre (See Figure 2). He names who is really to blame in his opinion, including the IDF, the security forces, the police, the opposition, and the demonstrators against the government, and calls on viewers to invest in Israel in order to prevent economic damage to the country.[15] In the second video, five senior Israeli rabbis supposedly accuse Netanyahu of strengthening Hamas, dividing the nation, and for causing the debacle that led to the October 7 events (see Figure 3). They call to stop the war and return the hostages.[16]

[15] Goichman, "The Presenter Is Not the Prime Minister."
[16] Benjakob, "Fake Rabbis and AI-Bibi."

Figure 2. Deepfake Video of Prime Minister Netanyahu from a YouTube Account Posing as Netanyahu's Account



Note: The caption reads "Netanyahu's important message to Jews worldwide about the fighting in Gaza."

Figure 3. Deepfake Video of Rabbis against Netanyahu

Note: Across the top, it reads "Rabbis rebel against Netanyahu," and in red, "Warning: Fake." The red does not appear in the original video and was added when publishing the film in *Haaretz*.

Blurring the Boundaries between the Digital and Physical Worlds

Using the Physical World to Increase Credibility in the Digital World; Using the Digital World to Create Real Events

Influence operations aim to shape the local discourse in order to achieve their strategic objectives. As mentioned in the introduction, Iran, despite being physically distant, has both the capability and motivation to operate in the digital realm with the intention of manipulatively influencing the general public, opinion leaders, journalists, and decision-makers. Iranian influence operations go beyond the boundaries of the digital world and attempt to create sensational fabricated events or dramas that capture local attention and shape the discourse. In addition to these efforts, these operations are increasingly extending their influence from the digital realm to the physical world.

Familiarity With Local Discourse, Radicalization Attempts, and Creating Violence—"Aryeh Yehuda News Flashes" as a Case Study

These influence operations are not detached from the local Israeli discourse. Instead, they exploit existing divisions or key issues in the local discourse. For example, the extreme right-wing Hebrew-language Telegram channel "Nazi Hunters" shared photographs of well-known Palestinians with crosshairs over their faces and details about them, intended to incite viewers. Shortly thereafter, the "Aryeh Yehuda News Flashes" Telegram channel posted similar photographs and details of Arab Israeli citizens with crosshairs on their faces. This demonstrates a keen awareness of and familiarity with the local discourse, as well as an intent to radicalize the local discourse and incite violence in the real world.

In a calculated effort to provoke physical violence in the days following October 7, the "Aryeh Yehuda News Flashes" Telegram channel posted false information, claiming that "Palestinian terrorists" were hospitalized at various hospitals across Israel, with the intent of causing citizens to protest and engage in violence at multiple hospitals in Israel. On October 11, 2023, members of La Familia, a far-right extremist group of fans of the Jerusalem Beitar soccer team, went to Sheba Hospital after hearing reports that a "Palestinian terrorist" was being treated there. They attempted to break into one of the wards and caused a disturbance at the entrance to the emergency department, resulting in the arrest of three of them.[17]

[17] Liran Levi, "Clashes at Sheba: Members of La Familia Tried to Break into the Ward Where They Thought a Terrorist Was Hospitalized, 3 Arrested, Documentation," [in Hebrew] *Ynet*, October 11, 2023 https://www.ynet.co.il/news/article/byjrk8vwt

Creating Media Storms and Taking Control of the Local Discourse

The act of sending a funeral wreath to the home of the parents of Israeli hostage Liri Elbag on April 7, 2024, was an unusual incident that revealed the unique use of digital assets by Iranian operators to create a media storm. Accompanying the wreath was a card that read "May her memory be blessed. We all know that the country is the most important." The wreath and message immediately raised suspicions since Liri Elbag was still alive and had not been declared dead.

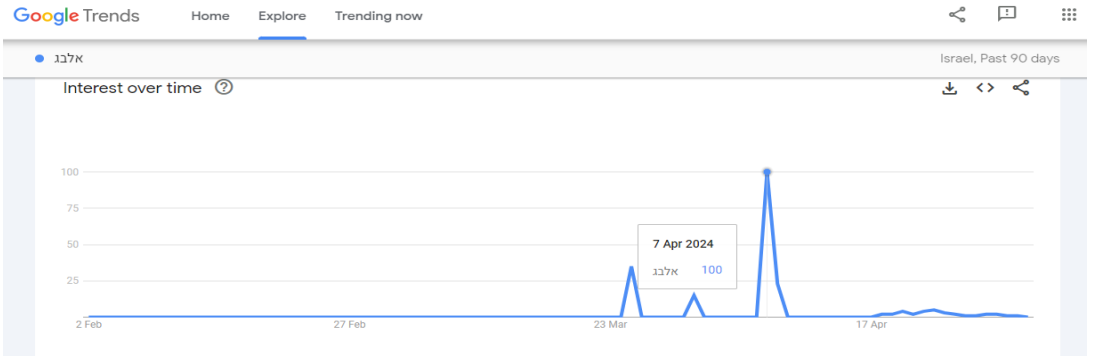
Nonetheless, this action demonstrated the operators' close familiarity with the hostage situation and the families involved. It is likely that the intent behind sending the wreath and the card was not only to cause sorrow for Elbag's parents but also to generate media attention and publicize the painful incident. Indeed, it did not take long for the public and media uproar to ensue. Liri Elbag's mother was interviewed on Keren Neubach's radio program "Daily Agenda" and asked, while crying, "Who does something like that? Is it my fault that my daughter is a hostage? Do I need to apologize for fighting to bring her back?"[18] Before it was apparent that Iranian operators had purchased and delivered this wreath,[19] different groups in Israeli society accused the other sides of sending the wreath.

The incident also demonstrated the ability of the influence operations to create spins, take over the public and media agenda, and fuel hate, anger, and distrust between different segments of Israeli society and between the Israeli public and the state's institutions. The effect of this incident can be observed on Google Trends, which shows a surge in interest in the name "Elbag" on the day this incident was made public (see Figure 4).

[18] Karen Neubach (@kereneubach), "Shira Elbag, mother of Liri, on the memorial wreath that arrived," [in Hebrew] X, April 7, 2024, https://x.com/kereneubach/status/1776895073944256769

[19] Yoav Zitun, Itamar Eichner, Yael Ciechanover, "Shin Bet: Iran Likely Behind Delivery of Funeral Wreath to Hamas Hostage's Family," *Ynet*, July 4, 2024, https://www.ynetnews.com/article/hkfkhzglc

Figure 4. The interest in "Elbag" following the sending of the wreath



Source: Google Trends

Furthermore, this incident can be viewed as a demonstration of the operators' deep understanding that a simple message like this would create a media storm when received by the hostage's family. It took place against the backdrop of the debate in Israel about the return of hostages, which created a divide between those advocating for achieving a "total victory," seen as "for the good of the country," and those favoring the return of the hostages, seen as "harming the war effort." The seemingly innocent wording of the note perfectly aligned with the deep and painful rift in Israeli society and cynically exploited the anguish and worry of the hostage's parents.

The deep familiarity and understanding of the domestic arena in Israel, as well as the audacity of the operators, are further demonstrated by the way in which the wreath was ordered. It was discovered that Iranians, using an Israeli mobile phone number and whose WhatsApp account was connected to the fictitious BringHomeNow operation, had contacted a local Israeli flower store and ordered the wreath. The email address provided was under the name of a policeman who had been murdered on October 7 and whose body was being held in Gaza. The order was placed under the name Berezovsky, which is the surname of the Shin Bet director.[20] Moreover, it was revealed that the name of the person who had paid for the wreath had also purchased advertisements[21] on the popular Telegram channel of Israeli blogger Daniel Amram, who had promoted and recommended

[20] Yael Freidson, Yaniv Kubovich, Bar Peleg, and Omer Benjacob, "A Funeral Wreath Was Sent to the Home of the Hostage Liri Elbag; The Shin Bet assess: Iran is responsible," [in Hebrew] *Haaretz*, April 7, 2024, https://www.haaretz.co.il/news/politics/2024-04-07/ty-article/0000018e-b853-d906-a5cf-bad7f72f0000
[21] FakeReporter (@FakeReporter), "Daniel Amram published this evening the receipts . . . " [in Hebrew] X, May 16, 2024, https://x.com/FakeReporter/status/1791194864899485978

the Telegram channel "Tears of War," a digital asset that was used in an Iranian influence operation.[22]

The details of this incident also highlight the importance of constant tracking, archiving, and organization of existing information in helping to identify other events, accounts, or content as part of foreign influence operations. The Shin Bet's statement and report disclosing a forensic connection to an Iranian influence operation were quickly published in the media, thus preventing further dissemination and development of the discourse surrounding the incident.

Creating a False Impression of Credibility, Authenticity, and Localness—Putting Up Signs in the Public Sphere as a Case Study

A prominent trend in several Iranian foreign influence operations, both before and after the war's outbreak, involves placing physical content related to the influence operation in public spaces. This includes signs on balconies, placards on the street, and posters at bus stops. In Israel, these signs, placards, and posters are reportedly photographed by those who put them up and then sent to the agents of the influence operation. The images are then disseminated through the operation's accounts on social media platforms. Evidence suggests that locals are deceived into collaborating with foreign agents via personal messages on social media platforms and instant messaging apps, being asked to place the signs, photograph them, and send the images to the operators.

This tactic—of placing signs in the public sphere, photographing them, and then posting them online—creates a false impression of credibility, authenticity, and local presence. When social media users encounter a new organization or a suspicious account, the visibility of signs in the public sphere makes them less likely to suspect that the account is foreign, malicious, or inauthentic.

The Digital Realm as an Overlapping Arena: Influence, Intelligence Gathering, and Recruitment

A distinguishing feature of Iranian foreign information manipulation and interference compared to disinformation and influence operations from other sources, is the blurring of familiar boundaries of an "influence operation" in social media platforms. For foreign state agents, the digital realm becomes an expansive arena for executing strategic objectives across various domains.

[22] Refaella Goichman, "For 800 Shekels: The Iranians Disseminated a Campaign Against Israel on the Telegram Channel of Blogger Daniel Amram," [in Hebrew] *The Marker*, May 16, 2024, https://www.themarker.com/advertising/2024-05-16/ty-article/.premium/0000018f-80c5-dd4f-ab8f-95edef020000

Iranian influence operations build digital assets and entities with accounts and profiles across multiple platforms, posting content aimed at shaping Israeli society and discourse. By spreading messages, graphic materials, and other content, they create a false impression of widespread political support or opposition. However, their activities extend far beyond mere influence. These digital assets are also used to contact Israeli citizens directly through private messaging apps (such as WhatsApp, Telegram, and social media platforms messengers). This private communication further blurs the lines between influence, operations, recruitment, cyber activities, and intelligence gathering—all occurring within the same digital ecosystem, often using the same assets.

By crafting the appearance of significant and credible digital assets and spreading messages designed for influence, these operations cultivate a sense of authenticity and local following. When these assets are used to privately contact citizens, they present an even more credible image, increasing the likelihood of successful engagement.

An analysis of these influence networks during the war, as highlighted by the Shin Bet's statement in January 2024, reveals that Iranian operations attempt to deceptively recruit Israelis for tasks through methods like fictitious job offers and distributing surveys. Private communications include requests to place signs (designed by the Iranians) in public places, photograph demonstrators or the homes of security personnel, fill out surveys, and even carry out physical actions, such as transporting packages, ordering wreaths of flowers to be delivered to the home of a hostage's parents,[23] or paying for advertisements on popular Israeli Telegram channels.[24]

The "Tears of War" influence operation, which began after the war's outbreak, demonstrates the multifaceted and overlapping uses of the digital realm. Iranian operations leverage the same digital assets to simultaneously pursue objectives related to influence, intelligence gathering, operations, and recruitment.

[23] Omer Benjakob, "Shin Bet: Iran Used Israelis to Photograph Homes of Security Personnel and Encourage Discussion of the Hostages," [in Hebrew] *Haaretz*, January 15, 2024, https://www.haaretz.co.il/news/politics/2024-01-15/ty-article/0000018d-0e82-de9c-a3df-6ffbbed60000; Freidson, Kubovich, Peleg, and Benjakob, "A Funeral Wreath Was Sent to the Home of the Hostage Liri Elbag."
[24] FakeReporter (@FakeReporter), X (Formerly Twitter). https://x.com/FakeReporter/status/1791194864899485978; Refaella Goichman, "For 800 Shekels: The Iranians Disseminated a Campaign Against Israel on the Telegram Channel of Blogger Daniel Amram," [in Hebrew] *The Marker*, May 16, 2024, https://www.themarker.com/advertising/2024-05-16/ty-article/.premium/0000018f-80c5-dd4f-ab8f-95edef020000

Influence Is an Opportunity During War—The War Is an Opportunity for Influence

The various Iranian influence operations in Israel during the war can be divided into three groups: (1) Operations launched after the war broke out, (2) Operations active before the war that shifted focus to events related to the war, and (3) Dormant operations, previously exposed and abandoned, that were reactivated during the war.

1. *Operations Launched After the War Began*

Many of these operations started shortly after significant events. The following operations focused exclusively on the war:

- *"Tears of War"*—addressing the war, the pain of bereavement, and the grief it causes.
- *"BringHomeNow"*—posing as the Hostage Families Forum, attempting to gain local connections and influence the discourse around the return of hostages.
- *"Helpless"*—addressing Israeli women, female hostages, and murdered women portrayed as "helpless" due to the war.

2. *Operations Active Before the War and Shifted Focus to War-Related Messages and Content*

- *"The Second Israel"*—which dealt with social divisions, such as tensions between secular and religious communities, rabbis and LGBTQ+ groups, and the political right and left. It also promoted election fraud conspiracy theories and engaged in private communications with Israeli citizens.
- *"Two Hearts"*— posed as a local dating group, using romantic deception as a means to contact Israeli citizens.
- *"Aryeh Yehuda"*—a right-wing news flash network that primarily focused on disseminating news and current events from a right-wing perspective.

With the outbreak of the war, the focus of these operations shifted to dealing with the war, the hostage issue, and increasing tensions around questions like the hostage deal, IDF operations in Gaza, the entry of humanitarian aid, and the resettlement in Gush Katif. They promoted incitement against Arab Israeli citizens and encouraged violent activities by right-wing activists.

The "Fist" operation, which showed an affinity for extreme right-wing content (the fist corresponds with the profile picture and the design theme of the "Kahane Lives" symbol), promoted incitement against supporters of the left and left-wing organizations and incited violence against Palestinians. Some digital assets of this operation were active before October 7, but activity in these accounts increased after the war began.

Reactivated Operations

Most of these operations' digital assets were closed by the social media platforms after media exposure. However, accounts that "survived" the closures, particularly on Telegram, resumed activity during the war after a prolonged period of inactivity. Two examples are BBMOVEMENTS and ADUK, which were active in 2020 and 2021 and were initially exposed by FakeReporter and covered in the international media.[25] This shows how significant events, such as the war in Gaza, can trigger new influence operations, modify existing ones, and revive old assets that had survived previous shutdowns and exposure by security authorities, the media, and civil society. From this, we can learn that crises present opportunities to expand influence operations, and existing ones can be leveraged to shape and influence current events in line with the strategic goals of those behind the influence operations.

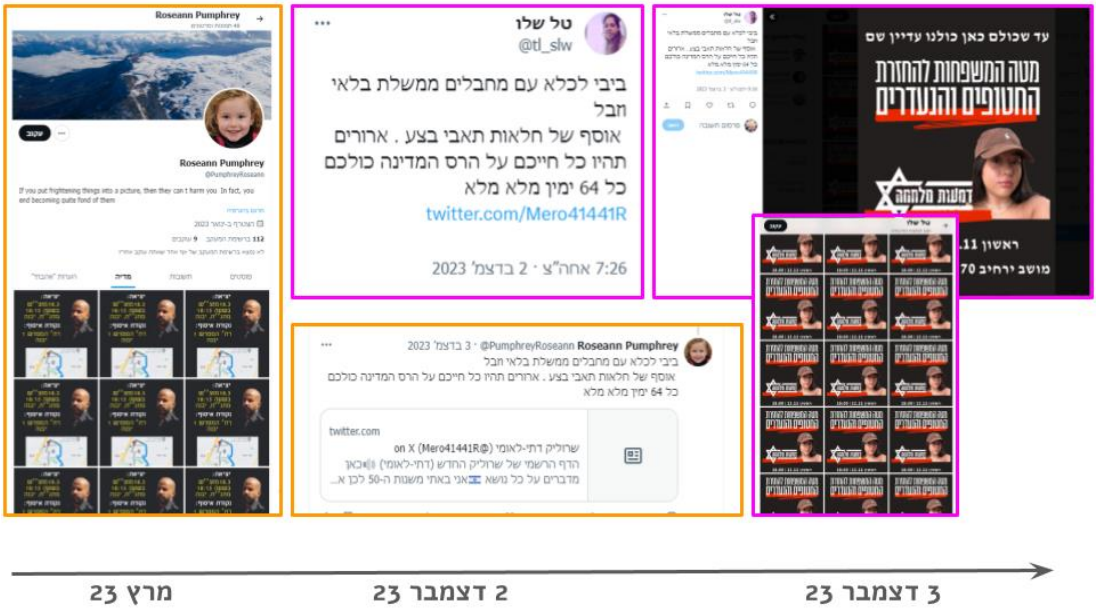
The reuse of accounts is found in both high-investment assets and simpler accounts, such as those used by bots. For example, an account that previously shared on X a post with police officers' details during an influence operation in March 2023 later resurfaced in December 2023. This account shared a post on X (formerly Twitter) that was retweeted hundreds of times by dozens of other accounts: "Bibi to jail with terrorists, defective garbage government. Collection of greedy scum. May you be cursed for your entire lives for the destruction of the country, all of you, all 64 fully right-wing" (see Figure 5). Some of the fake accounts that spread this post in early December 2023 were also used to promote a fake event supporting the family of one of the female soldiers held hostage.

This example demonstrates how an account used on X in an influence operation in March 2023, which was not closed by the platform, resurfaced in December as part of a pool of accounts involved in a separate operation called "Tears of War" (see Figure 5). The exposure of these digital assets can create a chilling effect and,

[25] Tom Bateman, "Iran Accused of Sowing Israeli Discontent with Fake Jewish Facebook Group," BBC, February 3, 2022; See also Orpaz and Siman-Tov, "Foreign Interference and Iranian Influence in Social Networks in Israel."

over time, can push the accounts “underground.” Often, the accounts post media articles or statements from the Shin Bet that link them to the foreign influence operations, but they typically deny the allegations, casting doubt on the credibility of these reports. The activity typically continues as long as the accounts remain active and are not shut down by the platforms.

Figure 5. Reuse of Accounts From Previous Operations



Note. From left to right, the same accounts used in March 2023, and again in December 2, 2023, and in December 3, 2023.

Conclusions

The Iranian influence efforts on social media platforms continue to use the same tactics seen in previous studies and operations before the war, while the use of diverse platforms is expected to expand further. This includes creating fake organizations and brands that exploit protest movements and civil organizations within Israel. These operations invest in high-quality uniform graphic materials and use a small number of fake profiles to directly contact citizens and local figures.

Although the overall operational methods have not changed, the operations seem to have become more precise, likely due to the experience and ongoing contact with the Israeli public, internet users, and the media. Prolonged engagement with Israeli society allows the agents of these operations to learn from public discourse, the successes and failures of previous operations, and direct interaction with citizens via private messages, further enhancing Iran's understanding of its target audience in Israel.

Iranian influence operations and their assets are constantly evolving. The fast pace of current events in Israel provide fertile ground for new influence operations. This has been seen by the emergence of assets branded as "groups or organizations of protestors" during the demonstrations against Prime Minister Netanyahu, the protests of Likud supporters against the Bennett–Lapid government, and the protests against the judicial overhaul. These operations exploit the public's unrest and momentum by creating shared causes and fostering interaction, and it is likely that the Iranians again will create fake civil initiatives and organizations designed to influence Israelis in response to the current events.

Exposing these digital assets should not be seen as the only means of addressing this phenomenon. The influence operations often deny media reports or Shin Bet statements about their activities, and they will continue to operate as long as the accounts remain open. In the context of Tehran's long-term strategic objectives, exposing these operations and their digital assets serves Iran's goals of fostering distrust in information and thereby undermining the public's ability to make informed decisions. Additionally, this exposure strengthens the reputation of Iran's cyber and digital capabilities and its ability to operate against Israeli society. The use of both old and new assets, which is characteristic of Iran's influence operations, also presents an opportunity for Israel to develop defensive strategies, while learning from past operations can help identify and counter future influence operations.

An analysis of these findings shows a deep understanding of the "soft underbelly" of the Israeli public, its discourse, and the media dynamics. The influence operations are sophisticated but simple to implement, creating the "perfect storm" to advance Iran's strategic objectives. These operations have evolved beyond merely causing a stir online—they now can create real world consequences, with local citizens unknowingly and indirectly driving the spin.

The use of AI-generated content is becoming more prevalent in these operations. Although not yet perfect, their quality is high enough to deceive citizens, members of the media, and public officials. The growing sophistication, volume, and distribution of AI-generated content create significant challenges in identifying, monitoring, verifying, and debunking it.

Looking Toward the Future

- Iran is expected to deepen its influence operations in Israel, where it has opportunities to advance its strategic objectives at a minimal operational costs and low risk of an Israeli or American response.

- The use of AI-generated content is likely to expand, improving the quality and credibility of fake content, increasing its volume and pace of distribution, and allowing more targeted messaging based on analyses of the local discourse.

- Influence operations are expected to spread to new social media platforms and internet services. The agents of the operations will exploit any platform that can effectively be used to influence the Israeli public, including those that allow direct messaging, information gathering, and the establishment of credibility, authenticity, and a local presence.

- After this study was completed, the Israeli media reported that a young Haredi man had been manipulated by an account on Telegram, supposedly belonging to a woman. According to the reports based on a Shin Bet statement, the man was asked to perform various tasks, including putting up signs, hiding packages and money, and delivering threatening messages. The man refused to carry out more serious actions, such as setting fire to a forest and harming citizens.[26] Although it is unclear whether this incident is connected to the influence operations described here, it warrants further examination, especially the targeting of the Haredi community.

[26] Shlomi Heller, "Slaughtering a Sheep, Setting Fire to Vehicles, and Breaking Windows: Iranian Agents' Demands of a Beit Shemesh Resident," [in Hebrew] *Walla*, July 16, 2024, https://news.walla.co.il/item/3678174

Recommendations

For Policy Makers

- Israel should take Iranian influence operations seriously, both during routine times and in war. These operations pose a growing threat; by exploiting vulnerabilities within Israeli society, Iran successfully influences public discourse, generates media storms, and even affects decision-makers. Foreign influence operations should be recognized as a key threat, and appropriate resources should be allocated to address them.

- Clear distinctions should be made between the digital and physical worlds and between various operational areas within the digital realm, such as influence operations, recruitment, intelligence gathering, and cyber activities. The State of Israel needs to define which bodies are responsible for addressing these threats, while balancing the need to monitor foreign and malicious influence without infringing on legitimate internal discourse and freedom of expression.

- Plans should be developed to respond to cyber and digital attacks and hold perpetrators accountable. These activities threaten national security and erode the foundations of democratic society, and malicious actors should face consequences for their actions.

- Social media platforms should be required to address foreign influence operations transparently, providing data on their scope, target audiences, and the agents behind them.

- AI technologies enhance the scale, quality, and speed of disinformation in the influence operations. Israel should adopt technological solutions to monitor and analyze large data sets, detect behavioral anomalies, and identify fabricated content.

- Operations with a small number of high-quality assets often evade detection due to their limited scale. These operations, conducted via private messaging, present a significant challenge for monitoring and cyber defense. Israel should reassess its technological approach to identifying and countering this type of threat.

- It is important to remember that there is no “silver bullet.” A combination of technological tools and human involvement should be used to identify influence operations and neutralize them early, thereby reducing their impact.

For Research Organizations and Civil Society Organizations

- Foreign influence operations directly target civil society. Therefore, it is necessary to strengthen the capacity of civil society organizations, fact-checkers, academic researchers, and media organizations so that they can play a central role in researching, monitoring, exposing, and countering these operations.

- Efforts should be made to enhance the Israel public's ability to critically consume information, operate safely online, and report suspicious online activities. Public campaigns and both formal and informal education are key to this effort.

- The Iranian influence operations consistently create new digital assets and reuse old ones. Israel can turn this into a defense opportunity by building a repository of knowledge to help identify and expose influence operations based on insights from past operations.

"Pray for Na'ama" – Russian Information War Against Israel[1]

Vera Michlin-Shapir and Daniel Rakov *

Introduction

On January 30, 2020, Na'ama Issaschar, a 26-year old Israeli-American backpacker, landed in Israel. She was accompanied by Israeli Prime Minister Benjamin Netanyahu, who traveled to Moscow especially to bring her home. The only words she uttered were: "Thank you… I am still shocked."[2] Her shock was understandable. She was arrested in April 2019 at a Moscow airport for allegedly possessing a minuscule quantity of drugs, for which she was sentenced to 7.5 years in jail. She was released after lengthy high-level negotiations between Prime Minister Netanyahu and Russian President Vladimir Putin.

The enigmatic nature of this affair and its rapid transformation from a seemingly mundane case of injustice to a high-level political affair raises multiple questions. Was this an ordinary case where a relatable human story attracts attention from the media? Or was this a case of a Russian information war where various Russian actors worked in cooperation and coordination across domains to influence Israeli media and public discourses and to affect political decision-making?

By analyzing primary materials, mainly from leading Israeli Hebrew-language media outlets (Ynet and Mako websites), which aim to appeal to the general Israeli public, and the website of the Russian state-backed news outlet Russia Today (RT), this paper sheds new light on the story of Issaschar and the related story Aleksei Burkov—a Russian hacker arrested in Israel whom Moscow demanded to be traded for Issaschar.[3] It reveals the case as a Russian informational-psychological

***** Dr. Vera Michlin-Shapir is the Academic Director of the Sympodium Institute for Strategic Communications. Previously, she was a researcher and lecturer at the Institute for Strategic Communications at King's College London. From 2016 to 2020, she was a Research Fellow at INSS. Lt. Col. (res.) Daniel Rakov specializes in Russian policy in the Middle East and competition between the great powers in the region. From 2019 to 2021, he served as a Research Fellow in the Russia Program at the INSS

[1] The authors would like to thank Dmitry Adamsky, Itai Brun, Yaakov Falkov, Ofer Fridman, Dudi Siman-Tov, Yelena B., and especially Vera Tolz, for their thoughtful comments and wise suggestions. We are grateful to a member of Issaschar's family and the journalists who covered the story in Israel who kindly helped us to reconstruct the timeline of the affair and to retrieve important details. We also thank Daniela Tsirulnik for research assistance.

[2] Itamar Eichner and Itai Blumenthal, "Na'ama Issaschar in Ben-Gurion Airport: 'Thanks to Everyone, Still Shocked from This Situation,'" [in Hebrew] *Ynet*, January 30, 2020, https://www.ynet.co.il/articles/0,7340,L-5669377,00.html.

[3] Additionally, we researched the general coverage of the Issaschar and Burkov in Russian, Hebrew, and English media and social networks, starting from Burkov's arrest in Israel in December 2015 until Issaschar's release in January 2020. We also conducted interviews with Issaschar's family, journalists

influence operation in Israel, in which RT played a key role. RT is a Russian news channel aimed at foreign audiences, owned, and financed by the Russian government. It is widely considered an important component of the Russian state toolbox of information war, while its practices are inconsistent with journalistic ethics.[4]

This operation took place long before the Israeli authorities recognized the threat of Russian malign influence operations in Israeli politics.[5] The article demonstrates that RT acted in coordination with other Russian government bodies, and its coverage of the case helped the Russian state exert pressure and extract diplomatic gains from Israel. Consequently, it shows the holistic approach of Russian state actors to information and media space, where media coverage (including the use of manipulative narratives) works to advance the Kremlin's interests in the international arena.

This is the first attempt to examine the Issaschar affair as an informational-psychological influence campaign within the Russian framework of information war. Prior to this research, Issaschar's case was never investigated in Israel or elsewhere as an information campaign and was reported in Israel as a case of political extortion where Issaschar was described as "a tool in a game" or a "bargaining chip."[6]

The limited scope of this article meant that we could not encompass the complex and, at times, contradictory roles of the various actors involved in this affair. Most of the Russian and Israeli activities on this matter are not available in the public domain, difficult to investigate, and draw robust conclusions. In this article, we

---

who covered the story in Israel, and former Israeli public officials. Studying the impact of the Issaschar affair on social media discourse is beyond the scope of this research.

[4] For further reading on RT, see Mona Elswah and Philip N. Howard, "'Anything that Causes Chaos': The Organizational Behaviour of Russia Today (RT)," *Journal of Communication* 70, no. 5 (October 2020): 623–645, https://doi.org/10.1093/joc/jqaa027; Vera Michlin-Shafir, Dudi Siman-Tov, and Nofar Sha'ashu'a, "Russia as an Information Power," [in Hebrew] *Modi'in Halakha uMa'ase* 4 (April 2019); Vera Tolz, Stephen Hutchings, Precious N. Chatterje-Doody, and Rhys Crilley, "Mediatization and Journalistic Agency: Russian Television Coverage of the Skripal Poisonings," *Journalism* 22, no.12 (July 2020), https://doi.org/10.1177/1464884920941967.

[5] Nadav Eyal, "Intelligence Officials in Israel Demanded From the Russians: Stop the Online Influence Operations," [in Hebrew] *Ynet*, July 21, 2023, https://www.ynet.co.il/news/article/hks3ymd9h.

[6] Asaf Liberman, "Bargaining Chip – the Full Story Behind the Imprisonment of Na'ama Issaschar," [in Hebrew] *Kan 11*, October 18, 2022, https://www.youtube.com/watch?v=wQ554jKQYeA&t; Carmel Libman, "Issaschar family on Hacker Extradition: 'Justice Minister's Decision Is Inhuman,'" [in Hebrew] *Mako*, October 30, 2019, https://www.mako.co.il/news-world/2019_q4/Article-53dfae6923e1e61027.htm; Michal Peylan, "Na'ama on Her Way to Freedom," [in Hebrew] *Mako*, January 29, 2020, https://www.mako.co.il/news-world/2020_q1/Article-340db61f633ff61026.htm.

refrained from discussing RT's probable coordination with the various Russian security agencies, the legal system, the courts, and the political leadership implied by the timeline and the dynamics of this affair. We also decided not to discuss the involvement of religious organizations such as Jewish Chabad and the Russian Orthodox Church, which played a role. Nevertheless, focusing on RT's role suffices to demonstrate that the Issaschar affair is an example of Russia's information war in Israel.

The article is divided into four parts. First, we present a review of the theoretical framework of the "information war" and the methodology employed in this article. Second, an overview of the timeline of the detentions of Issaschar and Burkov, which is the result of an open-source investigation by the authors, is laid out. This recount of events provides background to the third part, where we offer empirical evidence that Russian state actors, including RT, participated in a coordinated information operation. Last, the article discusses the impact of the operation on Israeli narratives.

Theoretical Frameworks and Methodology

The academic debate on Russia's information and influence efforts has received considerable attention.[7] These studies point to a growing metamorphosis between information, international relations, and conflicts in Russian strategic thinking.[8] They focus on explaining Russian information operations' strategies, doctrines, techniques, and cultural traits. Such Russian activities have been

[7] See Dmitry (Dima) Adamsky, *Cross-Domain Coercion: The Current Russian Art of Strategy* (Paris: IFRI Security Studies Center, 2015); Yaacov Falkov, "Russian Information Warfare in the Ukraine War," [in Hebrew] Israel Intelligence Heritage & Commemoration Center (IICC), March 14, 2023, https://www.intelligence-research.org.il/post/influence-russia-ukraine; Ofer Fridman, "Conceptualization of Foreign Influence and Foreign Interference," [in Hebrew] Israel Intelligence Heritage & Commemoration Center (IICC), January 4, 2024, https://www.intelligence-research.org.il/post/fridman-january-2023; Ofer Fridman, "'Information War' as the Russian Conceptualisation of Strategic Communications," *The RUSI Journal* 165, no. 1 (2020): 44–53, https://doi.org/10.1080/03071847.2020.1740494; Tolz, Hutchings, Chatterje-Doody, and Crilley, "Mediatization and Journalistic Agency"; Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020).

[8] Dmitry (Dima) Adamsky, "From Moscow With Coercion: Russian Deterrence Theory and Strategic Culture," *Journal of Strategic Studies* 41, no. 1–2 (2018): 33–60, https://www.tandfonline.com/doi/full/10.1080/01402390.2017.1347872.

termed in various ways, including "hybrid war,"[9] "active measures,"[10] "cross-domain coercion,"[11] and "information war."[12]

This article will take a slightly different approach, relying on authentic Russian terms to provide a theoretical framework that explains the country's activities in the information space and the role played by RT.[13] In Russia, the debate on influence activities in the information space is permeated with war-like metaphors. The most popular term to describe such activities is *informatsionnaya voyna* or "information war," within which operations of *informatsionno-psikhologicheskoye vozdeystviye* or "informational-psychological influence" occur. In the Russian context, these terms describe a combination of military and non-military methods aimed at influencing the information-psychological landscape of a targeted audience.[14] The current article will consider Issaschar's case within this authentic Russian terminological conceptualization.

To the best of our knowledge, there is no official public Russian doctrine on "information war." Yet, we found that various Russian institutions and agencies conceptualized the securitization of the information domain. Russian writing on the subject in the past 15 years has described the information war as a cross-domain confrontation where political, economic, diplomatic, and media spheres

[9] Mason Clark, *Russian Hybrid Warfare* (Washington DC: Institute for the Study of War, 2020), https://www.jstor.org/stable/resrep26547.1.

[10] Rid, *Active Measures*.

[11] Dmitry (Dima) Adamsky, "Deterrence à la Ruse: Its Uniqueness, Sources and Implications," *NL ARMS Netherlands Annual Review of Military Studies* (2020), https://doi.org/10.1007/978-94-6265-419-8_9.

[12] Nina Jankowicz, *How to Lose the Information War: Russia, Fake News, and the Future of Conflict* (London and New York: I. B. Tauris, 2020).

[13] RT's activities have received the most attention from media studies scholars, who argued that Russian media campaigns should be considered within the framework of global media studies. See Tolz, Hutchings, Chatterje-Doody, and Crilley, "Mediatization and Journalistic Agency." They have pointed out that within the Western discourse, the term "information war" lacks sufficient theorization and remains limited in explaining Russia's activities. See also Vitaly Kazakov and Stephen Hutchings, "Challenging the 'Information War' Paradigm: Russophones and Russophobes in Online Eurovision Communities," in *Freedom of Expression in Russia's New Mediasphere,* ed. Mariëlle Wijermars and Katja Lehtisaari (London: Routledge, 2019), 137–158. Furthermore, numerous studies about RT's activities raised doubts about its ability to reach and influence audiences in Western countries, with its viewership remaining largely marginal. See Joshua Benton, "How Many People Really Watch or Read RT, Anyway? It's Hard to Tell, but Some of Their Social Numbers Are Eye-Popping," *Niemanlab*, March 2, 2022, https://www.niemanlab.org/2022/03/how-many-people-really-watch-or-read-rt-anyway-its-hard-to-tell-but-some-of-their-social-numbers-are-eye-popping/; Tolz, Hutchings, Chatterje-Doody, and Crilley, "Mediatization and Journalistic Agency."

[14] Fridman, "'Information War."

are deeply intertwined, and civilian and security state actors are expected to work together.

The Unusual Story of Na'ama Issaschar

On April 9, 2019, Issaschar was on her way back from India to Israel via Moscow when she was arrested at the airport.[15] She was told that nine grams of Indian Hashish were found in her checked-in luggage, and she was being charged with drug possession, which was later aggravated to drug smuggling.[16] At this point, from diplomatic and legal perspectives, there was nothing extraordinary about Issaschar's case, as there have been hundreds of Israelis imprisoned abroad for drugs and other offenses, justified or not, while the Russian judicial system has been known for being particularly punitive and Kafkaesque.[17]

In August 2019, Issaschar's family appealed for help from the Israeli government through the media. The Israeli media portrayed the case as the maltreatment of a young girl by the Russian authorities, but the story failed to attract much attention.[18] Yet, behind the scenes, the idea of trading Issaschar for a Russian citizen jailed in Israel was being proposed. On at least two occasions in August and September 2019, a person who called himself Konstantin Bekenshtein left public comments on *Mako* (see Figure 1). He claimed that "The Russians are ready to give back Issaschar for Aleksei Burkov!!!" and that "[The] girl will return home only in exchange for the release of a Russian citizen named Aleksei Burkov." Bekenshtein obsessively contacted Issaschar's family with similar suggestions. Israeli journalists found later that Bekenshtein was a Russian-speaking Israeli of dubious background who, in the past, had served a jail sentence for fraud at the same

---

[15] Issaschar returned to Israel from a long trip as part of a large group of backpackers. The only odd thing, she recalled, was that while boarding the plane in India, she was moved from her prebooked flight to a later transit flight from Moscow to Tel Aviv, which effectively separated her from the group. From a personal conversation with a member of Issaschar's family.

[16] A month later, the Moscow prosecutor's office aggravated the charges from illegal possession of drugs (punishable by up to three years in prison) to drug smuggling (punishable by up to 10 years). See Nikita Sologub and Elizaveta Pestova, "She Did not Understand, What Does it Mean - Being Arrested in Russia. The History of Na'ama Issaschar, Who Wanted to Get Back to Israel by Transit Flight through Moscow, but Got Detained due to Claims of Drug Smuggling," [in Russian] *Mediazona*, October 10, 2019, https://zona.media/article/2019/10/10/naama.

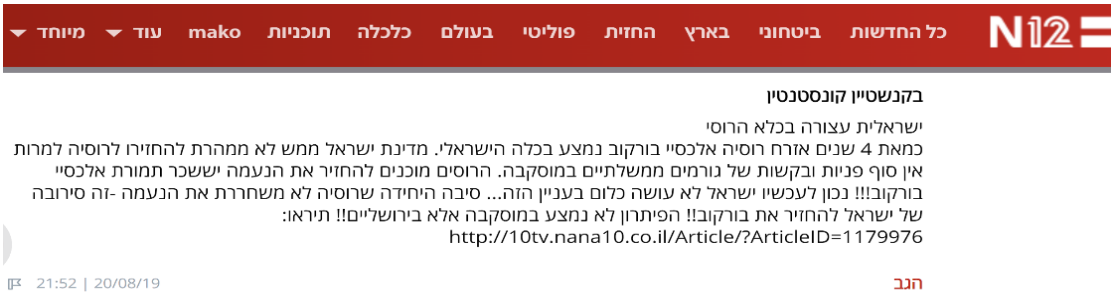
[17] Nina Fox, "Hundreds of Israelis Are Still Imprisoned Abroad," [in Hebrew] *Mako*, January 30, 2020, https://www.ynet.co.il/articles/0,7340,L-5669482,00.html.

[18] Tom Cohen and Amit Waldman, "Mother of the Jailed Israeli in Russia: 'I Hope the Government Will Get Her Out, I Was not Allowed to Get Close to Her," [in Hebrew] *Mako,* August 15, 2019, https://www.mako.co.il/news-world/2019_Q3/Article-418b7bbe9959c61026.htm.

prison where Burkov was awaiting extradition, making it possible that they had met in prison.[19]

Aleksei Burkov is a Russian national who was arrested in Israel in December 2015 for cybercrimes committed in the United States and was awaiting extradition. In hindsight, Bekenshtein's online comments should have raised concerns in Israel about possible political motives behind Issaschar's imprisonment in the weeks before Netanyahu asked Putin to release her and received an official demand to exchange her for Burkov.[20] But the comments were odd and likely were not identified by the Israeli government, and were ignored by the media and Issaschar's family. As such, Issaschar 4r53\]444eremained largely anonymous.

Figure 1. Comments Left by Bekenshtein About Issaschar in N12 (August 20, 2019)



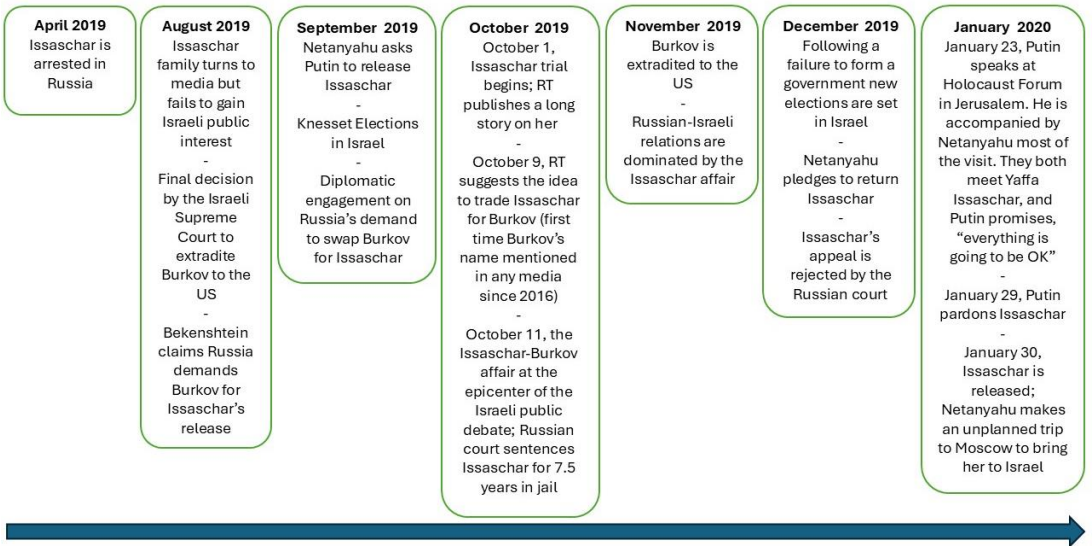
Russian citizen Alexei Burkov is detained in an Israeli prison for almost four years. The State of Israel is in no hurry to return him to Russia despite endless requests from government officials in Moscow. The Russians are ready to return Naama Issachar in exchange for Alexei Burkov!!! Currently, Israel is not doing anything about this... The only reason Russia is not releasing Naama is Israel's refusal to return Borkov!! The solution is not found in Moscow but in Jerusalem!!

[19] "An Israeli Is Imprisoned in Russia," [in Hebrew] *Mako,* August 20, 2019, https://www.mako.co.il/news-israel/2019_q3/Article-2fd3d9aa90eac61027.htm; Liza Rozovsky, Bar Peleg, and Noa Landau, "The Friend of the Russian Hacker: I Turned to the Issaschar Family After He Was Told About the Connection Between the Two," [in Hebrew] *Haaretz*, October 11, 2019, https://www.haaretz.co.il/news/law/.premium-1.7968356.

[20] It is not clear whether Netanyahu and his aides knew in advance, before asking Putin to release Issaschar, that his price tag would be Burkov. Israeli officials present contradictory versions two years after the events. In 2022, Netanyahu's national security advisor, Meir Ben-Shabbat, claimed that a demand to extradite Burkov to Russia in connection with the fate of Issaschar was mentioned by his Russian counterparts only after Netanyahu raised Issaschar's name before Putin. A similar sequence of events was described by a senior official from the Israeli Ministry of Justice who dealt with Burkov's extradition to the United States: He had not heard the name Na'ama Issaschar before Netanyahu had asked Putin to release her. The authors assume that if the Israeli officials had understood in advance that the Russians would demand to trade Burkov for Issaschar, Netanyahu would not necessarily have asked Putin for this humanitarian gesture, and it might have been addressed at a bureaucratic level. See Liberman, "Bargaining Chip," 21:10–21:33, 23:20–25:36.

Issaschar's case gained Israeli public attention in October 2019 (see Figure 2). On October 1, Issaschar's trial commenced in Russia. Although it was hardly reported by the Israeli media, Daniil Lomakin, the senior editor of RT in Russian, devoted a magazine article to Issaschar on RT's website.[21] A week later, on October 9, Lomakin, wrote another magazine story that became crucial for Issaschar's fate. In his second story, Lomakin focused on the jailed Russian hacker Aleksei Burkov. Lomakin interviewed Konstantin Bekenshtein (who left the comments a few months earlier), introducing him as a friend of Burkov and the instigator of a possible prisoner exchange.[22]

Figure 2. The Timeline of the Na'ama Issaschar Affair



On October 11, 2019, the day of Issaschar's sentencing, the Israeli press began intensely reporting about a possible swap between Issaschar and Burkov, quoting Lomakin's article on RT. In the mid-day, the Prime Minister's Office confirmed Netanyahu's involvement in behind-the-scenes efforts to help Issaschar and implied Israel's refusal to swap her for Burkov.[23] In the afternoon, Issaschar was

[21] Daniil Lomakin, "She Didn't Even Go Through Customs: Foreigner Is Suspected of Drug Smuggling During the Transit Flight," [in Russian], *RT na Russkom,* October 1, 2019, https://ru.rt.com/efhw.

[22] Daniil Lomakin, "Arrested in a Standard USA Scheme: Russian Citizen Detained due to an American Request Is Sitting Four Years in an Israeli Jail," [in Russian] *RT na Russkom,* October 9 2019, https://russian.rt.com/russia/article/675668-ssha-izrail-rossiyanin-ekstradiciya.

[23] The press release confirmed that Netanyahu raised Issaschar's case with Putin at least twice—in a meeting between the two in Sochi, Russia, on September 15, and in a phone conversation between the two on October 4. Apparently from their quick response, the Israeli side was aware of the Russian swap request before the RT publication and tried to deal with the issue through diplomatic channels, treating it as highly confidential and not even informing Issaschar's family. See "An Announcement by the Prime Minister's Office Considering Na'ama Issaschar," Israeli Prime Minister's Office

sentenced to 7.5 years in prison. Israel declined to swap Issaschar for Burkov, and he was extradited to the United States in November 2019. Interestingly, the negotiation for Issaschar's release continued for more than two months afterward.

Russia's suggestion for a prisoner swap and Issaschar's disproportionate punishment had an extraordinary effect on the Israeli media. It ignited unprecedented interest and an outpouring of sympathy for Issaschar. From October 11, 2019, until her release from prison in January 2020, Issaschar's case became one of the most reported items in the Israeli media. Netanyahu and his rival Benny Gantz, who were embroiled in a domestic political deadlock and recurring elections, became publicly committed to efforts to release her, which dominated Israeli–Russian relations for months. Amid the barrage of news reports, magazine articles, and public initiatives, one senior Israeli official even asked the public to "pray for Na'ama."[24]

While much of the intense reporting by the Israeli media on the Issaschar affair was organic, RT continued to influence the Israeli media's agenda. For example, Lomakin, RT's correspondent, visited Issaschar in prison and concealed his RT affiliation from her, presenting himself as a human rights activist and thus deviating from ethical journalistic standards.[25] Thereafter, Lomakin released photos and described how Issaschar was "practicing yoga and learning Russian."[26] Significant interest in Issaschar prompted Israeli Channel 13 to interview Lomakin, where he once more was introduced as a "human rights activist" who wanted to share "optimistic messages."[27] Our research discovered that Lomakin had become a member of Russia's state-sanctioned Public Supervisory Commission only a day

Spokesman, October 11, 2019, https://www.gov.il/he/Departments/news/spoke_naama111019; Conversation with a relative of Na'ama Issaschar, 2020.

[24] Yaron Avraham and Carmel Libman, "'Special Force to Bring Na'ama Home': After the Recording – Parties' Leaders Under Pressure," [in Hebrew] *Mako*, October 13, 2019, https://www.mako.co.il/news-world/2019_q4/Article-cf9f1d57b81cd61027.htm.

[25] Anna Rayva-Barsky, "Journalists Pretending to Be Human Rights Activists Interviewed Na'ama Issaschar: I Don't Believe That I'm That Famous," [in Hebrew] *Maariv*, October 23, 2019, https://www.maariv.co.il/news/world/Article-725316.

[26] Daniil Lomakin, "I Hope That Publication Will Help: Human Rights Activists Had Visited the Incarcerated Israeli Na'ama Issaschar Convicted of Drug Smuggling," [in Russian] *RT na Russkom,* October 22, 2019, https://ru.rt.com/ek97.

[27] Hen Zender and Roni Shchuchensky, "The Activist Who Met Na'ama Issaschar: She's in Good Shape and Practices Yoga," [in Hebrew] *Channel 13 TV*, October 23, 2019, https://13news.co.il/item/news/politics/state-policy/naama-activist-interview-916940/.

before he published his piece on a possible Issaschar-Burkov swap,[28] which allowed him to visit Issaschar in prison. He was appointed to that post as part of a government purge that replaced genuine human rights activists with regime loyalists.[29] Lomakin was evidently trying to dismiss reports in the Israeli media where Issaschar was portrayed as "exhausted" and not able to hold on any longer,[30] as well as suffering from intimidation and isolation.[31]

The Israeli media attention surrounding the Issaschar affair culminated in January 2020 during President Putin's visit to Jerusalem for the World Holocaust Forum, which commemorated the 75th anniversary of the liberation of the Auschwitz death camp. Prior to Putin's visit, it was announced that he would meet with Issaschar's mother,[32] causing the Israeli media to focus disproportionately on the fate of Issaschar rather than on any other aspect of the visit. It is likely that Putin had already decided to pardon Issaschar before his visit to Israel, but chose to postpone this procedure until after the Forum.[33] During the Forum, Putin was able to present Russian politicized narratives of the Second World War,[34] which created controversies with Eastern European leaders (the Polish president refused to attend, and Ukraine's president decided in the last moment not to enter the hall during Putin's speech).

A week later, Putin pardoned Issaschar, and Netanyahu flew to Moscow to escort her home. Although Russian and Israeli government officials claimed that

---

[28] RT, "RT Journalist Becomes a Member of the Public Observatory Commission,"[in Hebrew], *RT na Russkom,* October 8, 2019, https://ru.rt.com/eh1q.

[29] Editorial, "New Membership of Moscow, Moscow Region and Saint-Petersburg Public Observatory Commissions Excludes Several Human Rights Activists, Who Visited Detained Political Prisoners," [in Russian], *Novaya Gazeta,* October 8, 2019, https://novayagazeta.ru/news/2019/10/08/155967-v-novyy-sostav-onk-moskvy-podmoskovya-i-peterburga-ne-voshli-neskolko-pravozaschitnikov-naveschavshih-v-sizo-politzaklyuchennyh.

[30] Noa Lavie, "Na'ama Issaschar During Her Mother's Visit in Jail: Thankful for all the Support," [in Hebrew] *Ynet*, October 14, 2019, https://www.ynet.co.il/articles/0,7340,L-5607096,00.html.

[31] Niv Raskin, "Who's Threatening Yaffa Issaschar? I Turned Down a Proposal and Then Got a Message That Shook Me. I'm Frightened," [in Hebrew] *Mako,* November 17, 2019, https://www.mako.co.il/tv-morning-news/articles/Article-ad943f99f187e61027.htm.

[32] "Putin Will Meet in Israel With the Mother of Issaschar, Who Was Convicted in Russia," [in Russian] *RT na Russkom,* January 22, 2020, https://ru.rt.com/f8d1.

[33] During his meeting with Yaffa Issaschar, together with Netanyahu and the Greek Orthodox Patriarch of Jerusalem, Putin reassured her of a positive solution for her daughter's release, saying "everything is going to be OK." See Yaron Avraham and Yair Sherki, "On the Way to Na'ama's Release. Putin Said to the Press: 'Everything is Going to Be OK,'" [in Hebrew] *Mako*, January 23, 2020, https://www.mako.co.il/news-israel/2020_q1/Article-472c58db5b1df61026.htm.

[34] TOI Staff, " Yad Vashem Apologizes for Distortions Favoring Russia at Holocaust Forum," *Times of Israel,* February 3, 2020, https://www.timesofisrael.com/yad-vashem-apologizes-for-distortions-favoring-russia-at-holocaust-forum/.

Issaschar was pardoned on humanitarian grounds, reports indicated that a deal had been made between the two countries. Allegedly, Israel agreed to help with the Russian Orthodox Church's claim over ownership of the St. Alexander Nevsky Church in Jerusalem, a Russian Orthodox Christian site near the Church of the Holy Sepulchre, that was under the control of a Christian German NGO, much to Moscow's displeasure.[35] Other concessions reportedly included Israel's implicit support for the Russian narrative of the Second World War, which was evident from the World Holocaust Forum, and providing positive media coverage of Putin's visit to Israel. Thus, Issaschar's case became an effective tool for advancing political goals important to Russia.

Russia's Information War in Israel

We have identified four ways in which the Russian actors' involvement in the Issaschar case constitute a manipulative and deceitful intervention in the Israeli information space, resembling an "information war."

1. **Hijacking the Israeli Public Agenda**

One of the most significant findings of our media survey was that RT's report linking Issaschar to Burkov resulted in a notable increase in her coverage in Israel. Prior to RT's report, the Israeli media had shown little interest in Issaschar. From her arrest on April 9, 2019, until the news about the potential swap offer broke in Israel on October 11, 2019, she had been barely mentioned in Israel's leading media outlets.

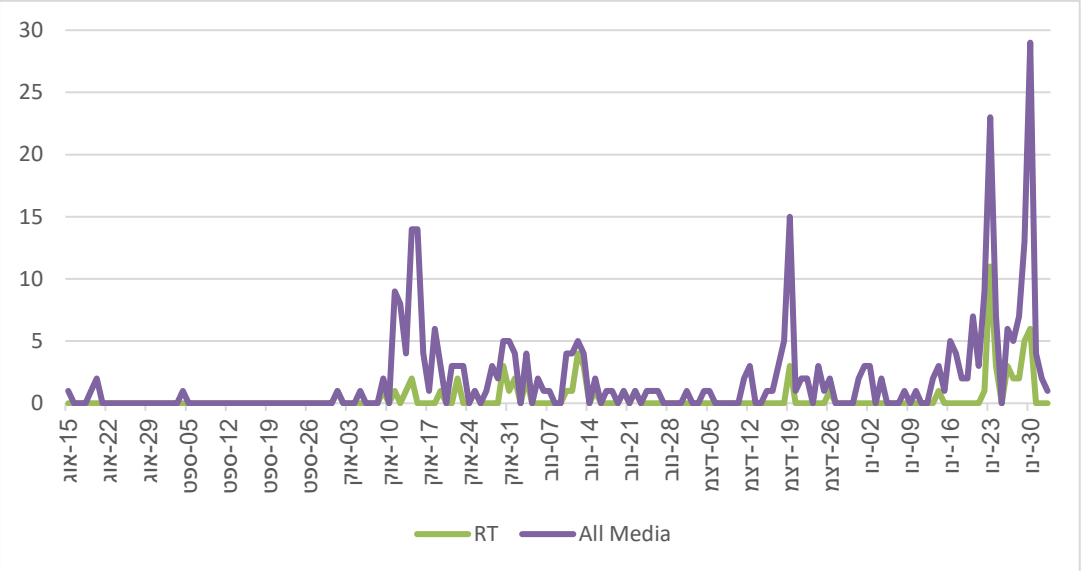
The RT story that linked Issaschar and Burkov clearly affected the Israeli media space. As the original story about the swap on RT was published in Russian on October 9, it took about 48 hours for the news to reach the largely Hebrew-dominated Israeli media.[36] From the morning of October 11 until her release, the Israeli media reported on Issaschar almost daily. The week following the news of a possible swap, Mako published 33 reports about Issaschar, and Ynet published

[35] Itamar Eichner, "The Moment of Truth for Na'ama Issaschar: What Do the Russians Want?" [in Hebrew] *Ynet*, January 22, 2020, https://www.ynet.co.il/articles/0,7340,L-5664164,00.html; Itamar Eichner, "Na'ama on the Prime Ministers Plane: This is the Quid-Pro-Quo Given to the Russians," [in Hebrew], *Ynet*, January 30, 2020, https://www.ynet.co.il/articles/0,7340,L-5669208,00.html; Liberman, "Bargaining Chip."

[36] Although Israel has a large Russian-speaking community, Hebrew dominates the domestic media, and there are only a handful of Russian-speaking prominent journalists. On October 10, 2019, RT posted a shorter version of the story about the swap on its English language website, and on October 11, the morning after, the story broke out in the Israeli media. See RT, "'I'm an Average Man': Russian Man Faces Extradition from Israel to the US on Hacking Charges," October 10, 2019, https://on.rt.com/a34m.

25 (see Figure 3). Symbolically, only when Ynet wrote on Issaschar's alleged connection to Burkov did the website generate a news tag with her name—signaling that only at that point did she become a news item worthy of tagging.

Figure 3. Media Coverage of Issaschar's Case (August 2019–January 2020)



The chart shows that Issaschar's case gained attention from the Israeli media only in response to RT coverage. This evident increase in media reporting on Issaschar could have been circumstantial (due to an Israeli interpretation of RT's reports as an official Russian request for a swap). Yet, RT did not deal with this story beforehand, and its in-depth coverage is hard to interpret as reporting of a newsworthy item. It looks more likely as an attempt to direct public attention to a hitherto marginal event. A closer look uncovered a long list of additional manipulative activities by RT, substantiating the claim that its role in the affair was to assist in an information operation.

2. The Backpacker and the Hacker—Comparable Victim Images

RT's manipulation of the media's agenda was in positioning Burkov and Issaschar in very similar terms—both as victims of unjust legal treatment. A detailed account of Burkov's grievances presented the artificial, almost random link between the two cases. RT and the Russian Embassy in Tel Aviv claimed that Burkov was an

"ordinary person" whose only chance for justice was "hope for an exchange" with Issaschar because he had fallen victim to unjust treatment just like her.[37]

This was manipulative, as it equated two very different legal realities. Issaschar was charged with a crime she had no way of committing (she could not have smuggled drugs into Russia because she never intended to enter the country but was only in transit). Burkov was subject to a year's-long FBI investigation for multiple online frauds and thefts, which amounted to $20 million dollars. The evidence against Burkov was reviewed by several Israeli courts and found to be of a sound legal standard.[38] These details, omitted from RT's reports, created a misleading portrayal, in which he and Issaschar were comparable victims. By doing so, RT helped the Russian government legitimize Issaschar's arbitrary detention.

3. Plausible Deniability of the Russian Government's Involvement

RT also presented the origins and nature of the proposal to exchange Issaschar and Burkov in a manipulative way, claiming that the instigators and lobbyists of the swap were Burkov's family and friends. For example, RT interviewed Burkov's sister, Natalya, and his alleged friend—the enigmatic Konstantin Bekenshtein, who had left public comments in August and September. RT suggests that these two independently and voluntarily initiated and lobbied for the swap.[39] This falsely framed the proposal as a humanitarian exchange when RT must have known that the swap was initiated by the Russian government and was much closer to a hostage-taking event, where a civilian was held in custody and promised to be released only after their country satisfied their demands. In doing so, they obscured the Russian government's role in initiating the request and allowed the Kremlin plausible deniability.

RT knew the true source of the deal since Russian officials most likely briefed its staff about it. We deduce it from the fact that in October 2019, Israeli and Russian officials were the only reliable sources who knew about the swap idea. Israeli officials were unlikely to share this with RT since they had kept it secret even from Issaschar's family. Russian officials, by contrast, had the knowledge, motivation, and access to RT to make the story public at that time (48 hours before Issaschar's

---

[37] Daniil Lomakin, "Arrested in a Standard USA Scheme: Russian Citizen Detained due to an American Request Is Sitting Four Years in an Israeli Jail," [in Russian] *RT na Russkom,* October 9, 2019, https://russian.rt.com/russia/article/675668-ssha-izrail-rossiyanin-ekstradiciya.

[38] Israeli Supreme Court of Justice, "Alexei Burkov Against the Minister of Justice and Attorney General," [in Hebrew] November, 2019, Case 7272/19, https://supremedecisions.court.gov.il/Home/Download?path=HebrewVerdicts%5C19%5C720%5C072%5Cv05&fileName=19072720.V05&type=4.

[39] Lomakin, "Arrested in a Standard USA Scheme."

sentencing) to pressure Israel. There is nothing wrong with RT publishing such an intriguing story without disclosing their sources or with Russian officials leaking the story at a time convenient for them to pressure Israel. However, RT's decision to publish a false claim about the provenance of the information was more problematic.

Contrary to RT's narrative, Bekenshtein was in no position to promote a deal between Israel and Russia. RT's narrative was also inconsistent with Bekenshtein's early comments on Mako and to Issaschar's family, where he claimed that "the Russians" were seeking the exchange and that Issaschar was held captive in Russia.[40] RT did not only conceal their sources, which is a common journalistic practice, but it also promoted a false version of reality that obscured the state-backed nature of the event where Russia attempted to leverage Issaschar's imprisonment against Israel, as confirmed by senior Israeli officials.[41]

4. Daniil, the Activist, and Lomakin, the Journalist

An incident involving RT's Lomakin raises further suspicion that he was working to influence the Israeli media discourse and exert pressure on the Israeli government. Lomakin's behavior points to possible state-backed actions aimed at influencing the Israeli information space. He was allowed by the Russian goernment to visit Issaschar in prison and reported a version of events that was not truthful but convenient for the Russian state. Moreover, as he was not investigating Issaschar undercover, he had no reason to hide his affiliation with RT from her. Hence, this was closer to a pattern of an influence campaign, where he deceived Issaschar and Israeli journalists to spread false information that was flattering to the Russian penitentiary system.

Reputational Damage to Russia—How an "Information War" Can Backfire

The limits of this information campaign should also be considered. After RT helped the Russian government establish plausible deniability, it also positioned Putin's subsequent pardon of Issaschar as a benevolent and humanitarian act. After Burkov was extradited, RT's reporting on the case noticeably diminished. RT resumed reporting on Issaschar around Putin's visit to Israel in January 2020. In its

[40] Noa Landau, Bar Peleg, and Josh Breiner, "'Disproportionate' Sentence for Israeli-American After Russian Request to Release Hacker Denied," *Haaretz*, October 11, 2019, https://www.haaretz.com/israel-news/.premium-israeli-source-moscow-pressed-to-release-hacker-in-exchange-for-detained-israeli-1.7967753; Niv Raskin, "Sister of Na'ama Issaschar, Jailed in Russia: The Girl Is Devastated. She Has Lost the Hope. It Is a Nightmare," [in Hebrew] *Mako,* September 4, 2019, https://www.mako.co.il/tv-morning-news/articles/Article-a53834871bafc61027.htm.

[41] Liberman, "Bargaining Chip," 26:50–29:50.

reports about the clemency, RT underlined that the expected pardon was a benevolent act by Putin, which corrected the excesses of the Russian judicial system.[42] Putin reflected on both points in his explanations for the pardon, which RT described as "guided by the principles of humanity."[43] Putin described Issaschar as "lucky," again highlighting his merciful disposition toward the case.[44]

When considering the impact of RT's influence campaign on the Israeli media space, its successes were mixed. Although it helped maximize pressure on Israel during a politically sensitive time and achieved some important returns for the Kremlin, Russia also suffered reputational damage in Israel. The Israeli media discourse around Issaschar developed along the lines of the most powerful political discourse in Israeli society—the captives/hostages discourse, in the IDF camaraderie spirit of "no one gets left behind." Following RT's linkage between Issaschar and Burkov, she was branded as a "captive," which drew an emotional outpouring of support for her and her family. For instance, Ynet's celebrity section reported that Israeli celebrities supported her under the title "We must not abandon her."[45] Netanyahu also echoed this discourse in a public letter to Issaschar: "We do not abandon any person to their fate."[46] But as part of the same discourse, Putin was depicted as a "hostage-taker" and villain, with such associations causing reputational damage for Russia in Israel.

Furthermore, RT's framing of a possible humanitarian exchange failed to gain support for a Burkov–Issaschar deal. While public sympathy was largely with Issaschar and her family, a course of action that would have angered Israel's closest ally, the United States, unsurprisingly failed to gain support. Israel's strategic partnership with the US was evidently a strong and underlying political discourse in Israel.

Conclusion

[42] Roman Shimayev, "Guided by the Principles of Humanity: Putin Has Pardoned the Israeli Na'ama Issaschar," [in Russian] *RT na Russkom,* January 29, 2020, https://ru.rt.com/fac7.

[43] Marina Yudenich, "About Mercy," [in Russian] *RT na Russkom,* January 23, 2020, https://ru.rt.com/f8oc.

[44] Itamar Eichner and Eti Abramov, "A Kiss from Netanyahu: Na'ama Issaschar is on the Plane on its Way to Israel," [in Hebrew] *Ynet*, January 30, 2020, https://www.ynet.co.il/articles/0,7340,L-5669172,00.html.

[45] Yoni Froim, "Celebrities Support Na'ama Issaschar: We Should not Abandon Her," [in Hebrew] *Pnai Plus (Ynet Group)*, October 15, 2019, https://pplus.ynet.co.il/rechilut/article/5607531.

[46] Itamar Eichner, "Netanyahu in a Letter to Na'ama Issaschar: We do not Abandon Anyone," [in Hebrew] *Ynet*, January 13, 2020, https://www.ynet.co.il/articles/0,7340,L-5659066,00.html.

The Issaschar affair is a relatively early but important example of the intensifying modus operandi of the Putin regime, which involves hostage-taking of foreign civilians on Russian soil to leverage them for high-level political quid-pro-quo. Other high-profile arbitrary detentions of foreign citizens, all Americans, by the Russian authorities include businessman Paul Whelan, basketball player Brittney Griner (who was released in exchange for Russian arms dealers Viktor Bout), and journalist for the *Wall Street Journal* Evan Gershkovich.[47] The information domain plays a prominent role in this modus operandi, as domestic public pressure is essential for ordinary civilians who have been imprisoned by the Russian authorities to be considered eligible for a high-level political intervention and exchange.

While this case was not initially considered an information operation, the Russian holistic definition of information war suggests otherwise. The Russian understanding of the media space as a deeply securitized arena allowed the Kremlin to use various actors, with RT among them, to influence Israeli public discourse to pressure the Israeli government to negotiate with Russia.

This article explores the contours of an informational-psychological Russian campaign in Israel, where Issaschar's imprisonment and release were used by RT (a government-owned and operated entity) to advance Russian state goals. Using the conceptual framework of information war, we traced how a civilian Russian state-backed news agency triggered an affair that had outsized significance for Russian–Israeli relations and Israeli internal politics for five months. This approach gave the Kremlin flexibility and maneuverability as it exerted pressure on the Israeli government and society. As a result, even in the face of Israeli defiance to release Burkov in exchange for Issaschar, Russian pressure on Israel continued and eventually led to Israeli compromises vis-à-vis the Kremlin.

This research contributes to the current debate on Russian influence operations in several ways. First, it highlights this interesting example of an ongoing broad and varied Russian psychological-informational effort that has not received enough attention in the context of Russian–Israeli relations. Second, the Issaschar affair should have served as an early warning sign to the Israeli government and authorities that relations with Russia were about to deteriorate. This became more evident in 2022 after Russia invaded Ukraine, and even more so since October 2023, after the Kremlin embraced Hamas' narrative in the Gaza war. Further

[47] Natasha Bertrand, Katie Bo Lillis, and Jennifer Hansler, "US Proposal to Russia to Free Whelan and Gershkovich Included Swapping a Number of Suspected Russian Spies, Sources Say," CNN, December 5, 2023, https://edition.cnn.com/2023/12/05/politics/state-department-whelan-gershkovich-proposal/index.html.

deterioration in the relationship can be expected and Israel should take appropriate measures to address this threat.

This brings us to the final contribution of this article, namely, calling attention to Israeli lack of preparedness for Russian influence activities. Israel has been slow to address the comprehensive nature of the Russian information war.[48] In contrast to many Western countries that blocked RT's broadcasting following Russia's full-scale invasion of Ukraine, RT, along with other state-backed Russian news outlets, continue to operate freely in some parts of the world, including Israel. As a result, RT is able to participate in influence efforts under the guise of a media outlet, putting Israel at risk of malign Russian influence. Israel should develop an integrated government–civil society strategic approach to counter and combat malign influence operations by Russia and other actors. This process should begin as soon as possible and include learning, policy review, and the reallocation of resources and efforts.

[48] Yaacov Falkov, "Russian Information Warfare in the Ukraine War," [in Hebrew] Israel Intelligence Heritage & Commemoration Center (IICC), March 14, 2023, https://www.intelligence-research.org.il/post/influence-russia-ukraine.

Russian Influence in Israel During the War in Gaza

Ophir Barel, Vera Michlin-Shapir, Milàn Czerny[1]

Since the outbreak of the war in Gaza, Russian agents have been carrying out hostile influence activities against the Israeli public, aimed to undermine public confidence in the actions of the Israeli army and harm the strategic alliance between Israel and the United States. These activities are part of a long-term information warfare that Russia is waging around the world, with the intent of strengthening its standing in the international arena at the expense of the United States and its allies. Russian agents have conducted interference operations in the mainstream media and social networks, but it has not generated substantial change in the Israeli public discourse, although it has sometimes successfully penetrated the mainstream media discourse in Israel. This article examines the impact of the Russian influence operations, with the help of conventional models. It reflects an escalation in Russian hostility toward Israel, and its expansion could undermine the stability of Israeli society in wartime. Accordingly, it is recommended that Israel advance new conceptual and organizational measures to address the threat of foreign influence, in addition to increasing the Israeli public's awareness of the phenomenon.

Introduction

Since the outbreak of the war in Gaza, there has been a rise in the involvement of Russian agents—or those who align with the Russian government's messaging—in influencing the public discourse over social networks in Israel. While this activity promotes diverse messages related to the war and takes place on various platforms, it has one main underlying principle: the Russian information war against Israel is part of the broader cognitive campaign that Russia is waging against the West, with the goal of weakening the solidarity between Western countries and strengthening Russia's political and military importance in shaping the world order.

In this article, we first present the principles of the Russian information war as expressed over the past decade while examining its manifestations in Israel. We then discuss at length three efforts to promote pro-Russian messages during the war in Israel—the Doppelganger campaign, sponsored articles in the Israeli media, and the Telegram group "Ukronazim"—and their degree of impact on the public discourse in Israel during the war. To this end, we have focused on publications that appeared in Hebrew in mainstream news outlets in Israel, social networks, and online forums since the outbreak of the war. We then analyze the consequences of the Russian activity

---

[1] Ofir Barel is a researcher at the Yuval Ne'eman Workshop; Milan Czerny is an investigative journalist at Shomerim - the Center for Communication and Democracy; Dr. Vera Michlin-Shapir is the academic director at the Sympodium Institute for Strategic Communication. Before that, she was a researcher and lecturer at King's College London. The authors of the article would like to thank Dr. Michal Farah for her assistance in writing the article

while examining other possible action scenarios. We believe that the Russian activity described here is part of an escalation in Russia's hostile activity against Israel. Finally, we present policy recommendations for addressing this trend.

Background: Russian Information War Since the Annexation of Crimea

In the years after Russia's annexation of Crimea in 2014 and increasingly since Russia's intervention in the 2016 US presidential elections, research on Russian efforts to carry out information and influence operations has attracted considerable attention in the West. While Western researchers use a variety of terms to describe Russian influence activities, such as hybrid war, the Gerasimov doctrine, and others, the most common term in Russia to describe these activities is "information war." It is described as "a type of confrontation between parties, represented by the use of special (political, economic, diplomatic, military and other) methods [based on different] ways and means that influence the informational environment of the opposing party [while] protecting their own [environment], in order to achieve clearly defined goals."[1]

Russia's use of information warfare against the West is constant, based on a perspective that acknowledges the existence of a state of war between the sides, even without direct military confrontation.[2] This war is being waged to achieve Russia's strategic objectives of weakening and polarizing the West as well as bolstering the country's international standing as a great power that dictates the rules of the game in the international arena.[3] In order to accomplish this strategic goal, and due to an understanding of Russian military inferiority vis-à-vis Western countries,[4] Russia aims to weaken the democratic and economic institutions of the West in the internal arena and to undermine the West's legitimacy internationally.[5] Figure 1 provides details on the various measures that Russia uses to conduct its information warfare.

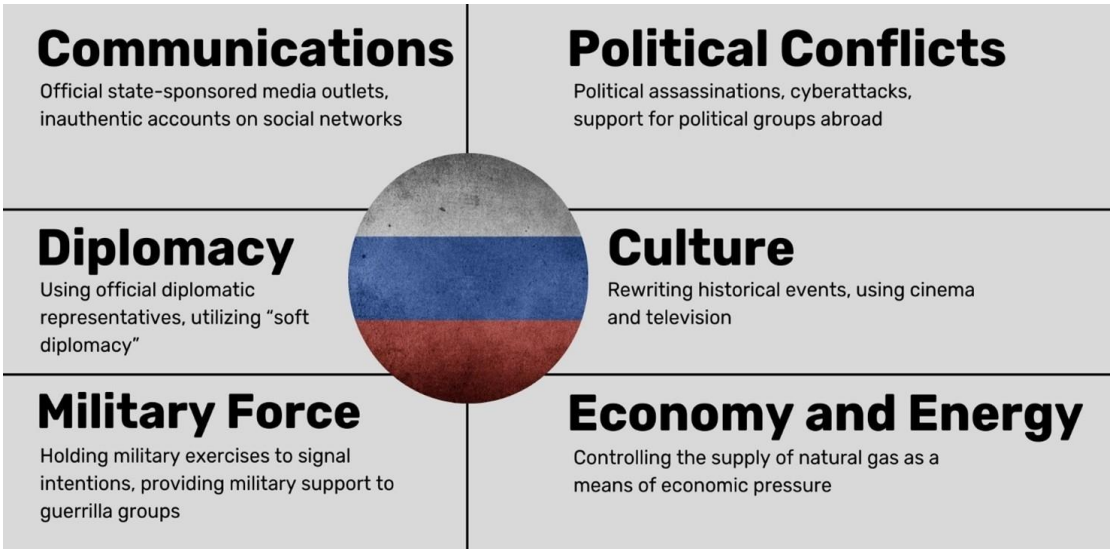


Figure 1. Mapping the Measures Russia Uses to Conduct Its Information Warfare. | *Note*: Seely, *A Definition of Contemporary Russian Conflict: How Does the Kremlin Wage War?*, 7.

First, since Russian influence activities are, by definition, multidimensional, the targets are not always able to recognize the concept of information war, understand that they are being targeted by Russian influence activities and assess the level of risk posed

by these activities. For example, in the past it was believed that the Russian government would refrain from engaging in malicious influence activities against Germany, due to Russia's significant economic interests in Germany.[6] However, even before Russia's full-scale invasion of Ukraine in 2022, researchers described how Russia worked to harm the official German establishment and weaken the country's democratic institutions by enlisting local political groups sympathetic to Russia, such as the Alternative for Germany (AfD) party, and wings within the Social Democratic Party (SPD).[7]

A second characteristic of Russia's information war is the simultaneous use of several channels to transmit messages. As a rule, Russian influence activities are diverse and seemingly not controlled by a single centralized body. This creates a sense of chaos in the Russian modus operandi, but in reality, it allows for the creation of a variety of content that can reach diverse audiences on multiple platforms. According to American researchers from the US State Department, there is no single communication platform through which Russian propaganda and disinformation are disseminated. Instead, it is done through a variety of platforms that sometimes share similar content and sometimes adapt the content for different target audiences.[8] In Israel, identical content was identified as being disseminated across multiple platforms, as described below.

A third characteristic is the use of the target audiences themselves to disseminate messages. Researchers from RAND found in 2018 that Russian activity aims to penetrate the American news cycle. When this objective is achieved, American networks organically disseminate the information for the Russians.[9] Figure 2 presents the methods of disseminating Russian propaganda to various audiences around the world, based on Russia's interference in the 2016 US presidential elections and Russian influence operations in other parts of the world.

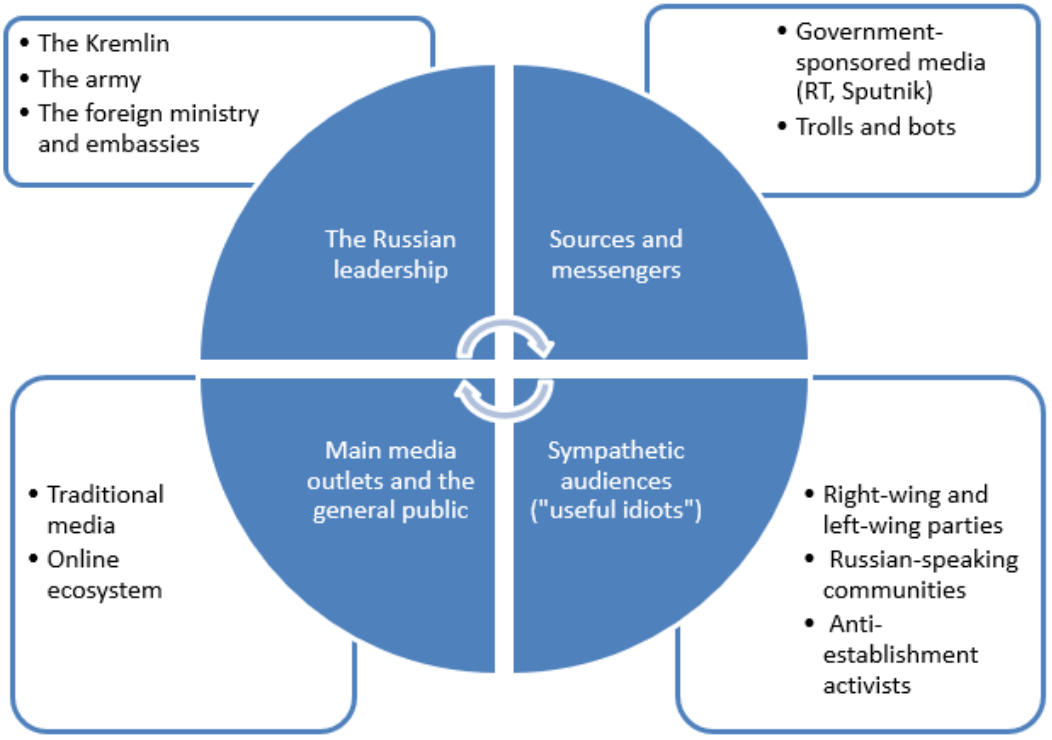


Figure 2. Methods of Disseminating Pro-Russian Messages in International Influence Operations | *Note:* Bodine-Baron et al., *Countering Russian Social Media Influence*, 7.

In recent years, the app Telegram has gained a central place in the media landscape. One main reason for this is its lenient policy on the dissemination of illegal content and the use of fake accounts, which sets it apart from other social networks. As a result, several authorities in Europe have imposed fines on Telegram.[10] Moreover, the European Union's Digital Services Act (DSA) grants the European Union powers to compel social networks with at least 45 million European users to take action against the spread of false information. According to Telegram, as of February 2024, it has only 41 million regular monthly users in Europe, which currently exempts it from complying with the provisions of the DSA.[11] However, official sources in Europe cast doubt on this number, and in May 2024, they began a probe of the company to conduct an up-to-date assessment of the number of users.[12]

Russian Influence Activity Among the Israeli Public in the War in Gaza

Since the outbreak of the war in Gaza, individuals associated with the Russian government or expressing support for its policies have carried out a series of influence operations targeting Israeli audiences on various platforms, promoting views of the war that align with the Russian government. One example of such a view is the assertion that US policy during the war actually harms Israel's security. It is important to note that this type of activity was already identified prior to the war, and even if the messages may have changed, the underlying objective remains the same.

For several years now, Russia has considered Israel an integral part of the Western alliance that it opposes. Previous studies have shown that Israel became a target of Russian information campaigns as early as 2019, following the arrest of Na'ama

Issachar in Moscow and the subsequent influence campaign that the Kremlin waged.[13]

The deterioration of Israel's relations with Russia following its full-scale invasion of Ukraine worsened during the war in Gaza, reaching a new low. This situation has had an impact on the information domain, with Israel becoming a target for various malicious influence activities conducted by Russian agents. The most prominent example is Israel's inclusion in the international influence campaign known as "Doppelganger," which Russia continuously wages against countries it perceives as enemies, such as Ukraine, as well as adversary states such as France and Germany. The Hebrew version of the campaign includes articles supposedly published on the *Walla!*, *Mako*, and *The Liberal* websites, claiming, for example, that Israel's political-strategic needs should prevent it from intervening in favor of Ukraine in the war.[14]

The outbreak of the war in Gaza led to a further escalation in Russia's information warfare against Israel. In addition to the anti-Ukrainian messages, new messages were introduced to weaken the confidence of Israeli citizens in the IDF and the government during the war and to strain strategic relations with the United States. As already mentioned, this study focuses on Russian influence activities conducted in Hebrew on social networks since the outbreak of the war.

This study most likely does not cover all Russian influence activities carried out due to technical difficulties in gathering data from the social networks themselves and locating Russian influence activity in real time (difficulties that we present later in greater detail in this section). Moreover, by focusing only on activities that involved posts in Hebrew, it is possible that we overlooked additional influence activities in other languages. However, the findings of this study clearly indicate the increasing interest of the Russian government and intelligence in what happens in Israel.

1. *Doppelganger*

Since the onset of Russia's war against Ukraine in February 2022, entities associated with the Russian government have been conducting an ongoing influence operation in the international arena. This operation aims to achieve two primary goals: (1) undermining Western support for Ukraine by spreading false information about alleged corruption and the supposed Nazi character of the country, and (2) sowing discord in public opinion within countries supporting Ukraine by promoting the claim that their support is causing economic and social damage.

As part of the operation, dozens of websites posing as well-known news websites from around the world, with fake news about Ukraine and the war, have been created. For this reason, the organization EU DisinfoLab, which tracks the spread of false information throughout Europe, calls the operation "Doppelganger" (a German term for two unrelated people with a similar appearance), but it is also known by the name RRN (Recent Reliable News—one of the websites used in the operation). The fake articles have been promoted throughout the internet by fictitious accounts on social networks and via sponsored posts made by inauthentic Facebook pages. The main countries targeted in the Doppelganger campaign have been France, the United Kingdom, Italy, and Germany.[15]

Different sources have attributed the campaign's operation to groups associated with the Russian military and regime. In July 2023, the European Council imposed sanctions on the Russian IT companies Social Design Agency and Structura National Technologies, which are associated with the Russian regime, for creating the fake websites.[16] In addition, in February 2024, the Israeli cybersecurity company ClearSky published a report stating that code strings found in the fake websites were identical to strings used in cyberattacks conducted by APT28, a group of hackers identified with Russian military intelligence (GRU), which was involved, among other things, in breaking into the email servers of the Democratic Party during the 2016 US presidential elections.[17]

After the outbreak of the war in Gaza, the Doppelganger's operators expanded their activity in Hebrew and directed the influence operation toward promoting false narratives about the war. As in previous cases, the Doppelganger campaign made use of inauthentic accounts on X and Facebook, which simultaneously published links to fake articles on sites posing as the Israeli websites *Walla* and *The Liberal* (see Figure 3).

Figure 3. A sponsored post on Facebook linking to a fake article on a website posing as *Walla* accusing US policy of causing Israel losses in the war | *Note:* On the left, the headline reads "Pressure and 'urgent demands' of the US place Israel on the brink of death." On the right: "All of this war, of all the victims, it's just for the good of the US. But the main victim that the Americans are requesting us to sacrifice—to give up on a secure future."

The articles published in Hebrew focused mainly on the following narratives:

- claim that US involvement in the war has caused losses to Israel and endangered it, as those influencing US policy are leftists;
- antisemitic and anti-Israel incidents from around the world;[18]
- claim that there was a transfer of weapons from Ukraine to Hamas, which were used to carry out the October 7 massacre (a narrative that will be further discussed below);
- the damage to Israel's economy caused by the war;[19]

- claims that Hamas terrorists succeeded in their operations against the IDF (see Figure 4);

- Russia can strengthen Israel's security vis-à-vis Iran.[20]

Figure 4. Facebook ad from a Doppelganger campaign that includes the narrative of the IDF's withdrawal | *Note:* The post reads: "The barbarians in flip flops forced the IDF to withdraw. Israel lost to Palestinian gangs."

It is important to note that in at least one case, Doppelganger activity promoted content that did not originate from fake websites: at the end of March 2024, after the terrorist attack at Crocus City Hall, a concert hall in Moscow in which at least 144 people were murdered, a group of fake accounts on X made many posts intended to arouse Israeli empathy for Russia given the attack (see Figure 5). Some posts included a link to an article about the attack that was published on a website called Omnam.life, which has since been taken down. The identity of the website's operators is unknown, but it posted news from Israel and abroad from a pro-Russian and anti-Western perspective. The specific article that was promoted by the accounts tried to arouse the sympathy of the Israeli public for Russia following the attack by presenting it as being similar to the October 7 massacre. In both cases, the article claims that prior intelligence information received by certain bodies was not transferred to the right places, thus resulting in the attack not being prevented.[21] It is important to note that the website posted additional articles about the war, but it is not clear whether they were promoted throughout the internet.[22]

[image url="https://www.inss.org.il/wp-content/uploads/2024/09/PICTURE-5.png" credit="" alt=""]

Figure 5. Fake accounts on X promoting publications intended to create empathy among the Israeli public for Russia following the terror attack in Moscow | *Note:* The photograph on the left reads: "Stop war, stop violence! It causes pain to see all these miserable [sic] children." On the right: "We will stand by your side, Russia, in this difficult time. That we wish you peace."

This activity is part of a broader pro-Russian influence operation that was carried out in the days after the terrorist attack. Thousands of fake accounts on X posted anti-Ukrainian and anti-Western claims about the incident. For example, they claimed that the United States did not prevent the attack even though it received prior information about it. Some accounts indirectly linked the attack to the war in Gaza. One account, for example, claimed that Ukraine and the United Kingdom collaborated to carry out the attack in an attempt to distract public opinion from "the loss of the Suez Canal" due to the Houthis' attacks.[23]

An analysis of the scope of the activity of the Doppelganger campaign shows that in the months from November 2023 to March 2024, those behind the campaign maintained a steady pace of activity (see Figure 6). During this entire period, about 80 articles were posted. Certain periods were documented when there was an increased dissemination of articles. For example, on the night between November 20 and 21, 2023, over 2,000 fake X accounts made 3,000 posts with links to fake news articles in Hebrew (see Figure 7).

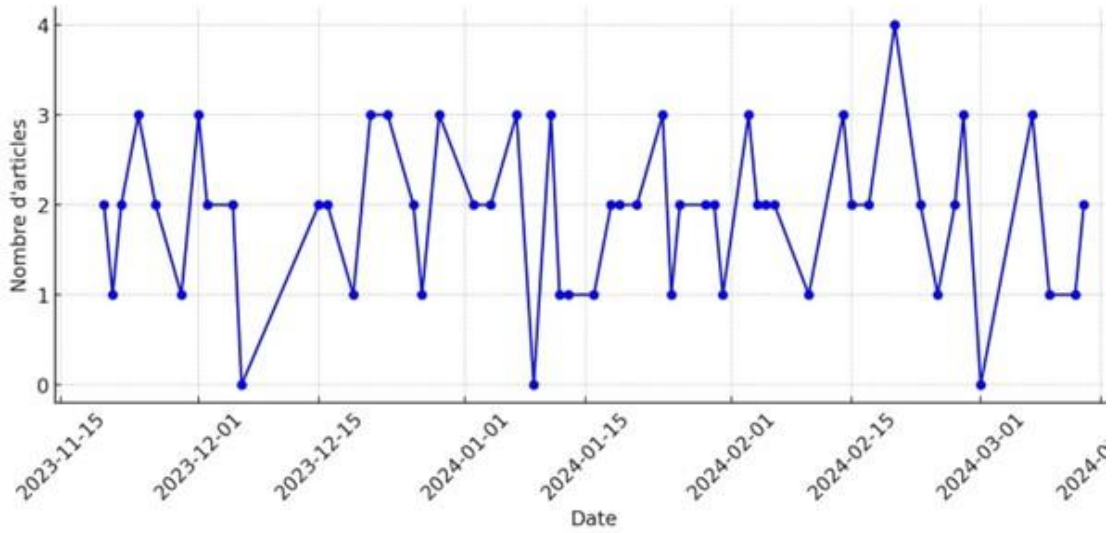


Figure 6. Number of articles in Hebrew disseminated as part of the Doppelganger campaign between November 15, 2023 to March 15, 2024.

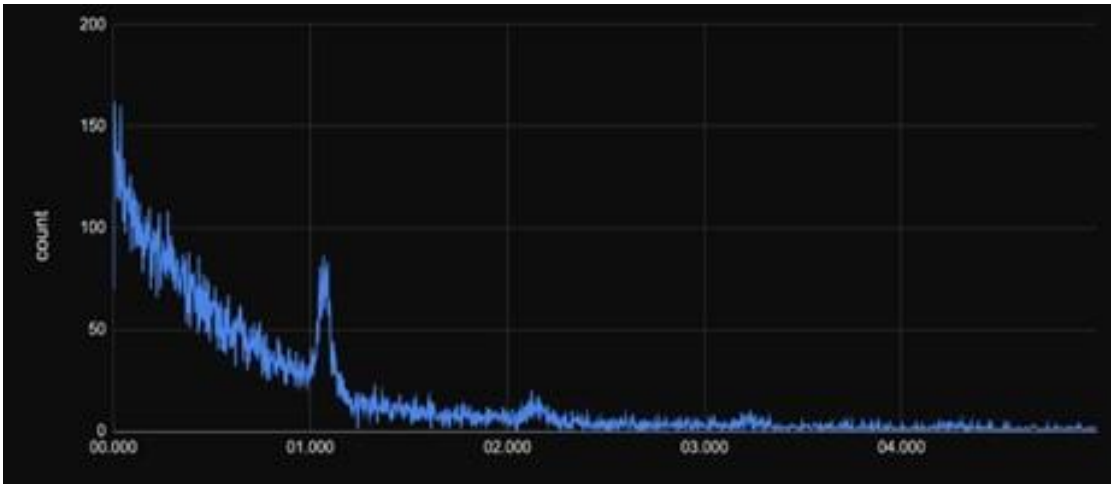


Figure 7. Number of Doppelganger campaign posts on X on the night between November 20–21, 2023.

The level of activity presented in the two graphs is consistent with the findings that attribute the Doppelganger campaign as a whole to tech companies associated with the Russian regime. This is due to the fact that the ability to consistently disseminate content in a foreign language, while adapting to the various developments in the war and conducting targeted promotions for short periods of time requires the use of considerable advanced technological and financial resources.

2. *Sponsored articles in the Israeli media favoring Russia*

In February and April 2024, the Seventh Eye, an Israeli website, published two investigations claiming that the news sites *Walla, Jerusalem Post,* and *Channel 13 News* had published articles with pro-Russian views on the Russia–Ukraine war and the war in Gaza. According to the Seventh Eye website, these articles were published no earlier than November 2023 and included interviews with researchers, military personnel, and politicians in Israel, which were conducted by an Israeli journalist named Nick Kolyohin who works for various international media outlets, including the Chinese news agency Xinhua. According to the Seventh Eye's investigations, these articles omitted certain statements by the interviewees that criticized Russia's policy.

The website also discovered that none of the media outlets mentioned that the articles were published with funding from an organization called the Russia–EU Communication Platform, which presents itself as aiming to promote cooperation and understanding between Russia and EU countries. However, the organization's description is quite vague, making it difficult to fully understand its essence and goals. In late March 2024, *Channel 13 News* posted two publications of this kind under the series "war and peace." The series aimed to describe the shared interests of Russia and Western countries and the importance of promoting understanding between them. The publications were removed after the Seventh Eye's query to Channel 13. According to Kolyohin, the articles published were important for understanding international geopolitics and his work aims to promote understanding and dialogue between Russia and the West. Kolyohin vehemently denies the claim that he is a Russian influence agent.[24]

At least one article funded by the Russia–EU Communication Platform was promoted using Doppelganger accounts, as shown in Figure 8. The use of these accounts could indicate, at least circumstantially, the existence of cooperation between the Russia-EU Communication Platform and the companies responsible for conducting the Doppelganger campaign.

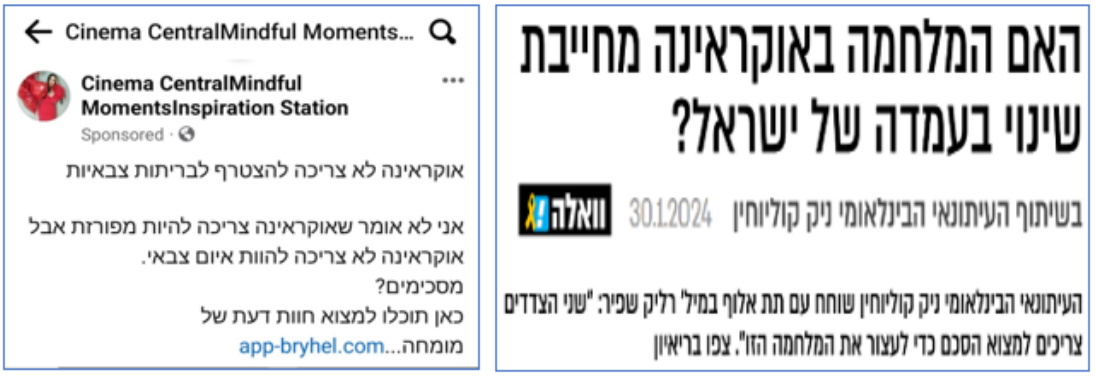


Figure 8. A sponsored post on Facebook (left) leading to the article published on the authentic *Walla* website (right) in cooperation with journalist Nick Kolyohin.

Note: The post on the left reads: "Ukraine doesn't need to join military alliances. I am not saying that Ukraine needs to be demilitarized but Ukraine doesn't need to be a military threat. Agree? Here you can find an expert opinion…" The article headline on the right reads: "Does the war in Ukraine obligate a change in Israel's position?"

3. *"Ukronazim"*

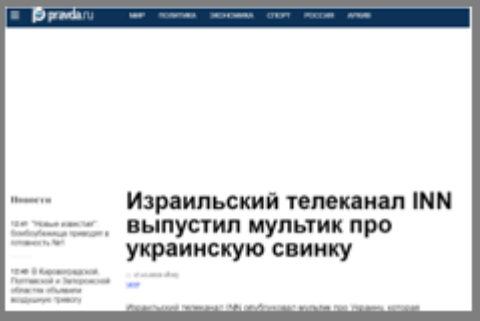
"Ukronazim: INN" (acronym for Israel Neged Nazism [Israel against Nazism]) is a Telegram group operating in Hebrew since March 2, 2022.[25] According to its description, the group aims to present its followers with

information that it believes "the Western-Israeli media and Facebook are hiding." The group covers the Russia–Ukraine war and other events in Israel and elsewhere from a pro-Russian or pro-Israeli perspective, while also taking an anti-Ukrainian and anti-Western perspective. A central theme of their reports is portraying the Ukrainian leadership, soldiers, and citizens as having nazi characteristics.[26] The Russian mainstream media has long described Ukraine as a nazi state, but this pattern

expanded significantly with the beginning of the war in February 2022.[27] In the context of events in Israel or those influencing Israel, Ukronazim represents a right-wing, and sometimes even far-right, viewpoint.[28]

Case study—Description of the Connection Between the Ukronazim Telegram Group and Russian Media

On October 11, 2022, the Russian Telegram channel CBO posted a three-and-a-half-minute animated video titled "Europe and Rabies." The video portrays Ukraine as a pig (a derogatory term for Ukrainians used by Russians who support the war) seeking to enter the territory of the European Union to escape the terror of Russia. After entering the European Union, Ukraine begins to exhibit highly inappropriate behaviors. As a result, at the end of the video, Europe decides to deport Ukraine. The following day, the Ukronazim group shared the video, and it was also posted on Russian-speaking and Georgian-speaking Facebook accounts and groups. In addition, the journalist Yevgeny Dodolyev, a host on the national Russian channel 1-Russia, shared the video on his YouTube channel (as shown in the photo, a post about the video on the Russian news site *Pravda*).



It is important to note that there are other Hebrew-language groups disseminating anti-Ukrainian content on Telegram. One example is a group called "Ukraine's crimes," with 240 followers. Its goal is "to provide the Hebrew-speaking population with the truth that is hidden by our media."[29] The number of followers of these other groups is significantly less compared to Ukronazim (Ukronazim has over 1,800 followers at the time of this writing, while these groups have fewer than 300 followers). This makes Ukronazim the most significant pro-Russian group operating on Israel's Telegram platform, increasing the interest in investigating its sources and modus operandi. While it is not possible to identify a specific entity behind the group, there has been at least one case where the Russian establishment media used a post from the Ukronazim

group to spread false information about Israel and Ukraine (a more detailed description is provided in the case study).[30]

As part of this study, we analyzed the characteristics and content of the Ukronazim's posts during the first four months of the war in Gaza (October 7, 2023 to February 7, 2024). A total of 791 posts were made in the group, of which 520 (about 66% of the total) discussed the war from various angles, mainly by describing the military actions between Israel and Hamas or presenting related events in the international arena.

As shown in Figure 9, the number of posts covering various events in the war and those discussing other issues (such as the war in Ukraine) and the ratio between the types of posts changed during those months. From the outbreak of the war until the middle of November 2023, the majority of the daily posts focused on the war. However, from that point forward, the proportion of posts related to the war decreased significantly, and most of the daily reports revolved around other issues, particularly developments in the war in Ukraine. This trend is noteworthy, especially given that prominent events in the war, such as the incident in which three hostages were mistakenly killed in Gaza by IDF fire, did not receive any response in the group. This suggests that the group's operators prefer to cover events that can be used to frame the war as part of the international struggle between Russia and the West. The killing of the hostages was a result of an operational error, and the group's operators were unable to connect it to their narrative.

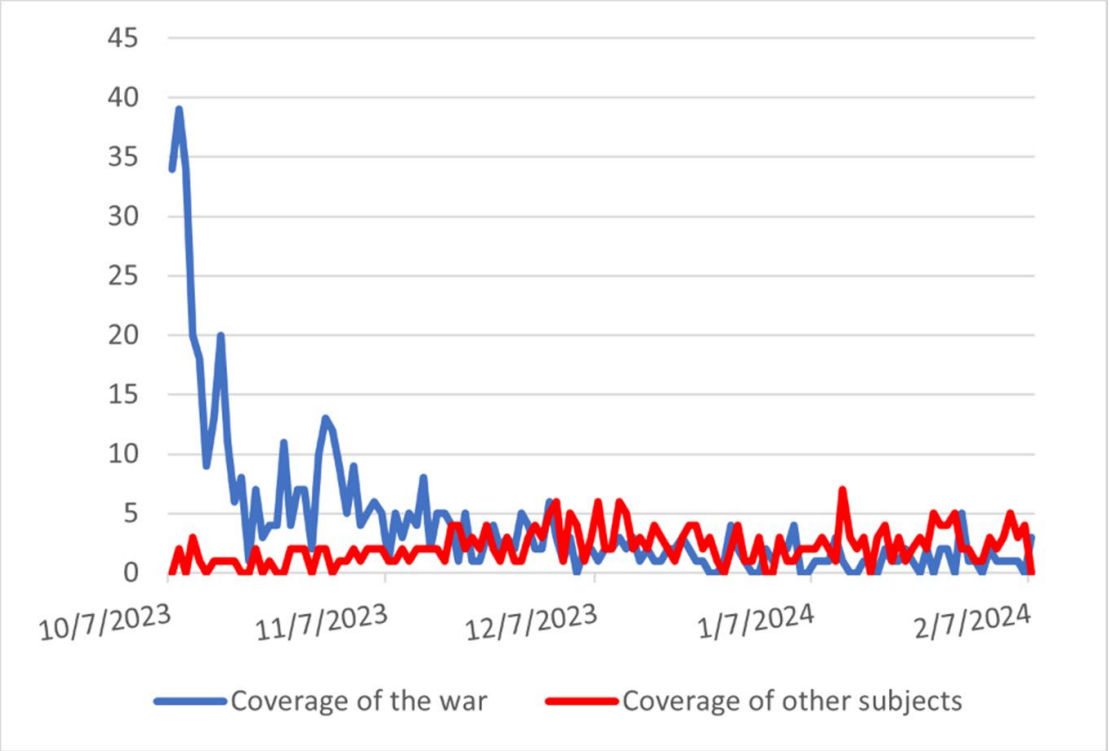


Figure 9. The number of posts relating to the war compared to other issues in the Ukronazim Telegram group from October 7, 2023 to February 7, 2024.

An examination of the posts related to the war reveals that the issue that received the most extensive attention was the international implications of the war. These included decisions made at the UN, demonstrations for and against Israel, and the responses

of official figures from various countries. There were 209 posts criticizing the policies of Western governments toward Israel, claiming that they are harmful to Israel.[31] In contrast, there were also posts highlighting the close relationship between Russia and Israel. This relationship was not just based on strategic cooperation against a shared enemy in Gaza and Ukraine but also on a connection between the nations. For example, one post showed the toys and flowers that Russian citizens had brought to Israel's embassy in Moscow after the October 7 massacre.[32] However, this report ignores the international support that Western governments expressed for Israel, mainly manifested in the significant military aid that the United States has granted to Israel, as well as the incisive criticism that the Russian government expressed toward Israel's actions in the war.

The second main issue that the group discussed was the war and its developments and their consequences for Israel and the Palestinians, including military measures, the November 2023 deal to release hostages, and political developments in Israel. A total of 196 posts were made on these issues.

On October 31, an article from the French television channel BFMTV was posted in the group. The article describes the spray-painting of Stars of David on buildings throughout Paris, apparently intended to threaten Jews.[33] This story was also promoted as part of the Doppelganger campaign, while on November 6, over 1,000 bots on X posted over 2,500 tweets about the story. France arrested four citizens on suspicion of the spray-painting and later claimed that the Fifth Service had carried out the graffiti on behalf of Russia's Federal Security Service (FSB), intending to cause instability in France given the rise in antisemitism there since the outbreak of the war in Gaza.[34] The Fifth Service has been described as the FSB's unit that is responsible for carrying out political influence activities and psychological warfare outside of Russia's borders, including for the purpose of maintaining Russia's influence in the former Soviet states.[35]

The fact that the number of posts that discussed the international aspects of the war was greater than those that discussed developments in the war itself could indicate Russia's tendency to seize and present events occurring in various places in the world as proof of prevailing international trends, such as the West's policy as a source of military instability and political and economic crisis, in contrast to Russia's responsible conduct.

Similar to the trend of posting reports connected to the war versus those not connected to it, there was also a trend reversal in the number of posts about military developments and international consequences, as shown in Figure 10. In the initial weeks of the war, the group mainly discussed direct developments in the war. However, starting from the end of October, the discussion of international aspects became comparable in scope to the description of developments in the war, and on certain days, the number of posts was even greater.

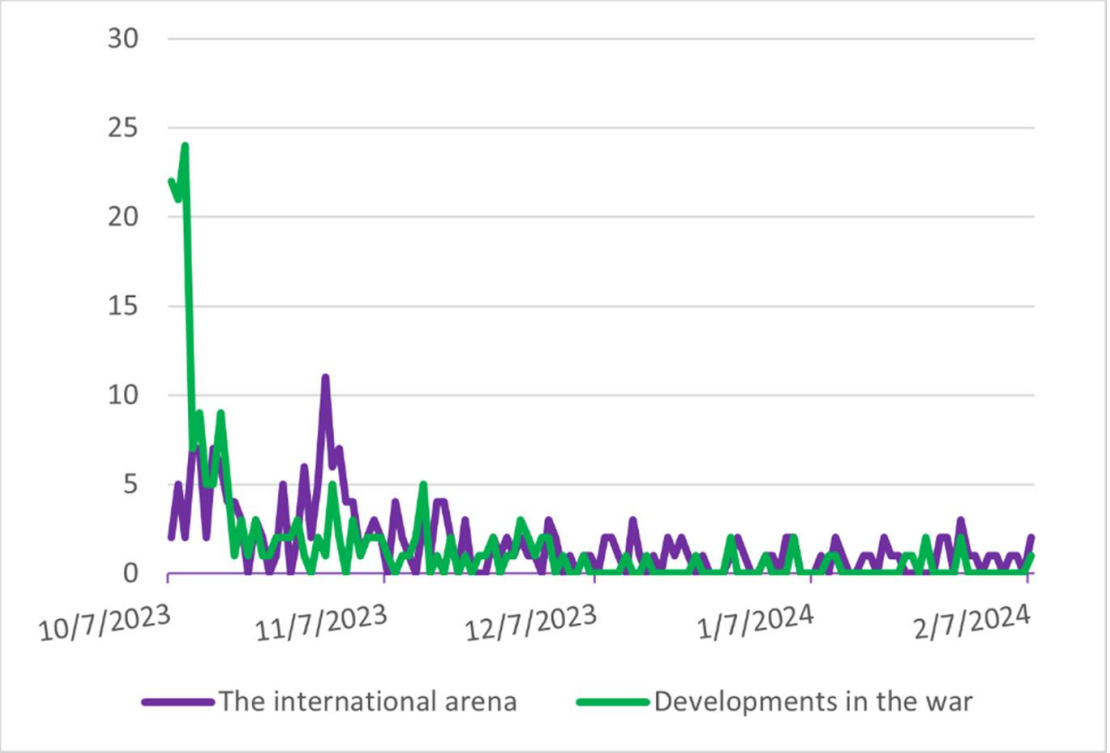


Figure 10. The number of posts presenting direct developments in the war, compared to the number of posts discussing its international aspects, from October 7, 2023, to February 7, 2024.

Other topics presented in the Ukronazim group included the transfer of weapons from Ukraine to Hamas (a false narrative that will be further discussed later),[36] describing the left in Israel as undermining the state's security, including blaming it for the outbreak of the war, and increasing the American military aid to Israel at the expense of Ukraine.[37]

Assessing the Impact of Russian Activity in Israel

The attempt to assess the full impact of Russian activity in Israel during the war in Gaza faces three main difficulties. First, there is no uniformity in the research literature regarding the best way to measure the impact of various content posted on the internet on users who are exposed to it. One approach focuses on measuring the active interactions of users with the content, such as responses and shares (referred to as "engagement").[38] Another approach considers the passive exposure to content (views) as the best metric for measuring impact.[39]

Second, the ability to gather and store findings about influence activity varies between social media networks. The Doppelganger activity on Facebook and X is not stored over time but is taken down by the initiators of the campaign after a predetermined period of time or removed by the social media networks themselves if they determine that the accounts involved violated their policy on inauthentic activity. In this situation, the only way to gather information from the two networks and assess their impact is by using screenshots taken during exposure to the activity, which cannot always be done. In contrast, activity on Telegram is stored over time and can be accessed and analyzed at any time. This discrepancy can lead to insufficient analysis of activity on Facebook

and X compared to Telegram, thus resulting in a partial picture of the state of influence activity.

Given these difficulties, we chose to measure Russian influence activity using two principles. First, we focused on researching public responses to the claim that Ukraine transferred weapons to Hamas, which were then used in the October 7 massacre.

On October 29, 2023, journalist and news presenter Ayala Hasson broadcasted a report on the Israeli Kan television channel supposedly showing the transfer of weapons from Ukraine to Hamas.[40] From our perspective, the penetration of this anti-Ukrainian claim from social networks to the mainstream media in Israel is a successful example of Russian influence activity. Therefore, we wanted to investigate the path of its penetration into the Israeli public discourse and its impact on it. This claim was previously published as part of the Doppelganger campaign and in the Ukronazim group.

Third, wherever possible, we measured the number and nature of active and passive interactions of users with social media content that included the narrative of Ukraine transferring weapons to Hamas. We performed a textual analysis of the written responses to posts those users shared, and we also analyzed the type of emojis that users posted in response to posts, using a guide that explained the meaning of over 200 emojis.[41] We used this analysis to categorize responses as supporting the narrative, opposing it, or not expressing an opinion on it. However, we used the "breakout scale" approach as the main method of tracking how the narrative spread on the internet and measuring its influence. The approach was developed by Ben Nimmo, the head of the threat intelligence team at Meta and an expert on influence and disinformation campaigns.[42] According to this approach, each influence operation can be rated on a six-step ladder, with each stage representing a different level of proliferation of influence operations. At the bottom and most basic level are influence operations that are carried out on a single social platform and whose messages do not spread to other places. At the top level are influence operations that lead to tangible impact on the world outside the virtual realm.[43]

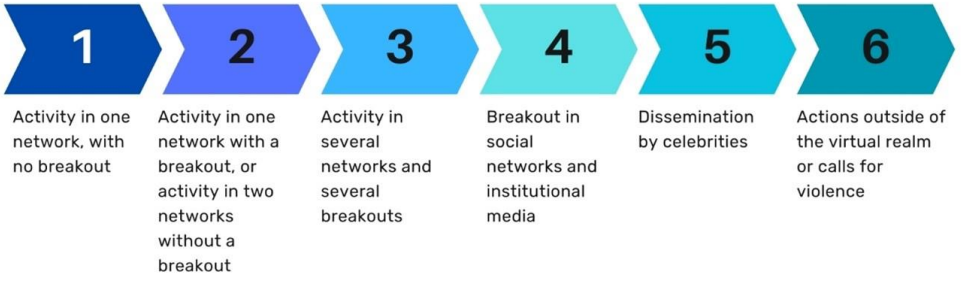


Figure 11. The breakout-scale model, which ranks the intensity of influence operations according to the pattern of their dissemination.

In tracking the discourse surrounding the claim that Ukraine transferred weapons to Hamas, we focused on posts that not only supported the claim but also opposed it, cast doubt on it, or presented alternative versions of this narrative. We recognize that

Russia's information campaigns aim not only to convince the target audience of the truth of a certain claim but sometimes intend to create public confusion and uncertainty regarding a certain issue, with the objective of weakening the public's opposition to Russia's actions. The existence of several versions of this claim—even if they are contradictory or posted by people unconnected to it—could serve this goal.[44]

As part of our research, we found that the claim that Ukraine had transferred weapons to Hamas had been widely shared throughout the internet in Israel. This claim was shared in three different arenas: (1) pro-Russian arenas (such as the Ukronazim group on Telegram and false articles circulated as part of the Doppelganger campaign), (2) the arena targeting people from former Soviet states in Hebrew (such as the Telegram group "Carmel News—news from the former Soviet Union and Israel"—with approximately 34,500 followers as of May 26, 2024), and (3) "open" arenas that do not have a specific target audience (such as X, Facebook, the television channel Kan, and online forums like Rotter). Our analysis of these arenas shows that the discourse surrounding the claim of weapons transfers from Ukraine to Hamas, the presentation of the claim, and responses from users took place on the internet over a two-month period from the onset of the war until December 6, 2023.

Figure 12 maps the discourse on the internet during this period, categorized by the arena of activity. From Figure 12, we can infer that the discourse in Israel took place mainly in October, whereas the highest number of posts was observed during the first week of the war and then again from October 28 to 30. During these times, most of the posts were documented in "open" arenas. The extensive discussion during the first week of the war can be attributed to the sense of surprise felt by the Israeli public following the outbreak of the war, which led them to seek explanations for how the debacle occurred. Toward the end of October, the discourse continued after Hasson's broadcast.

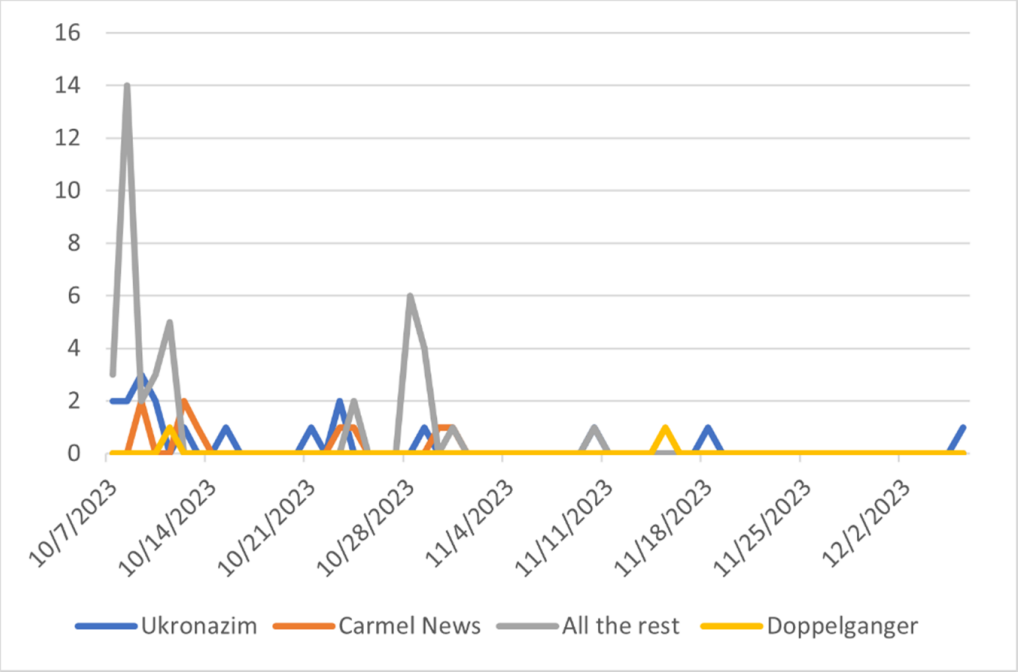


Figure 12. Documentation of the discourse in Israel about the claim of weapons transfers from Ukraine to Hamas, by place of publication, October 7 to December 6, 2023.

We used Nimmo's breakout scale model to measure the impact of promoting the message (or competing versions of it) among the public in Israel. Figure 13 charts the application of the model to the discourse in Israel.

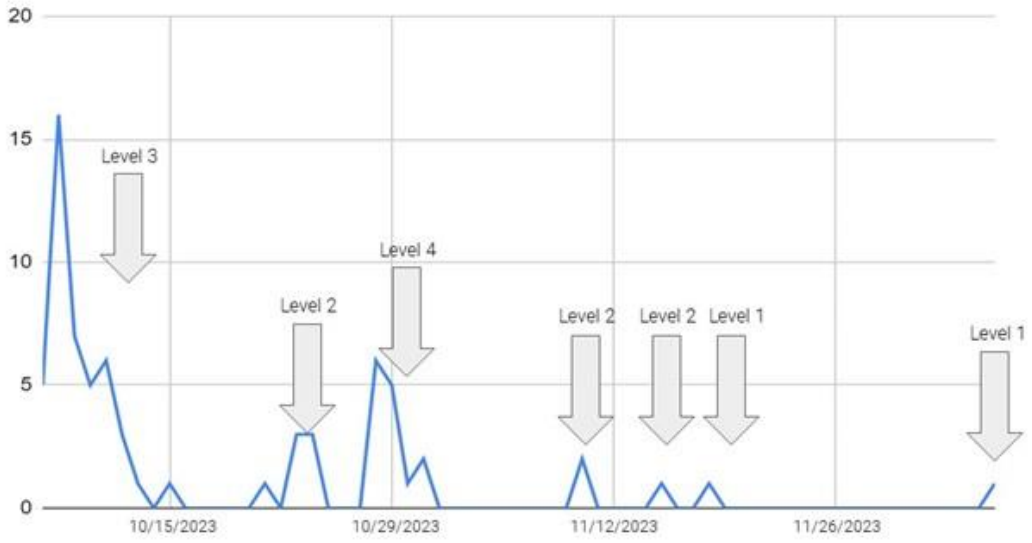


Figure 13. Characterization of the discussions on the narrative of weapons transfers from Ukraine to Hamas, using the breakout-scale model.

According to Figure 13, the model categorizes the promotion of the pro-Russian narrative about weapons transfers to Hamas, as well as the responses to it during the first week of the war as level 3 influence activity, representing influence operations that are publicized simultaneously across multiple platforms (but not in the mainstream

media). During this period, the discourse on the narrative took place in the Telegram groups Ukronazim and Carmel News, on X, on Facebook, and in at least one case, the sharing of content was documented in the Ukronazim group on Facebook. Subsequently, the discussion on the issue decreased, resulting in a decline in the level of influence to level 2, which represents influence activities that occur separately on different platforms or within a single platform but in multiple places (for example, such as posting the same content in different Facebook groups).

Following the broadcast on the Kan channel, the level of influence rose to level 4, the highest level documented during the war. Level 4 is characterized by influence activities that involve narratives that move from social networks into mainstream media. In this case, however, a reverse move occurred—from television to social networks. It is important to note that following the Kan broadcast, Ukraine's embassy in Israel posted a statement on its Facebook page completely denying the claim of weapons transfers to Hamas.[45] This denial indicates the extensive reach of the discourse that was documented in the Israeli media and social media networks after the broadcasting of the report on Kan.

In the subsequent weeks until December 6, the level of influence in promoting the narrative decreased to level 2 and then level 1, with level 1 representing influence operations that are only publicized on a single platform, without being disseminated to other groups, either within or outside of it.

Finally, we characterized the various user responses to the report of weapons transfers to Hamas and found two types of responses in each arena. In the Ukronazim group, which also published the narrative over the longest period of time (from October 7 to December 6), most of the user responses did not express an opinion related to this claim, but those that responded to the story supported it. In contrast, in the Carmel News group, the opposite was observed. In cases where the group posted declarations from official Russian sources supporting the story, most users expressed disagreement with them, mainly by using angry or ridiculing emojis (see Figure 14). Instead, posts in the group promoted an opposing view, that official Russian bodies transferred weapons from Ukraine to Hamas.[46]

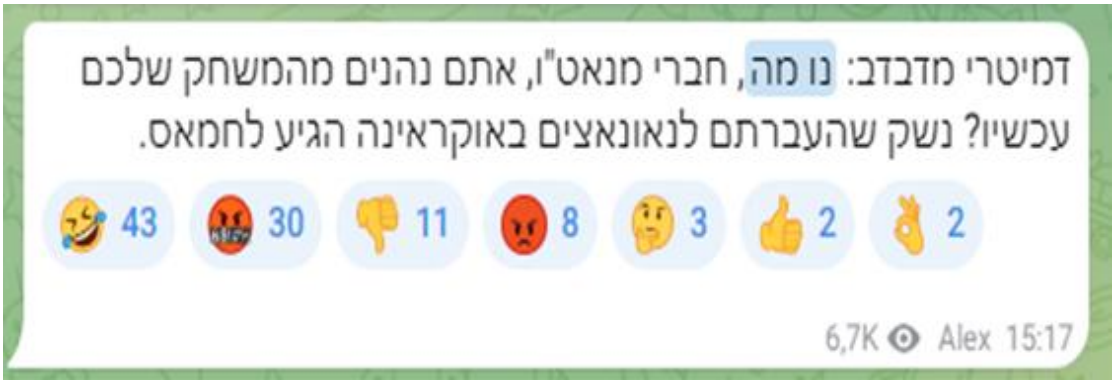


Figure 14. Post relating to the official Russian declaration of the story of the weapons transfers to Hamas in the Carmel News Telegram group, to which users responded with distrust | *Note*: "Dimitry Medvedev: Come on, NATO members, are you enjoying the game now? Weapons that you transferred to the neo-Nazis in Ukraine have reached Hamas." From Carmel News (@AlexmehaCarmel), Telegram, October 9, 2023, https://t.me/alexmehacarmel/10037.

In those arenas addressing the entire Israeli public, there was more extensive discussion of the story after the publication of the report on the Kan channel. This was reflected in the increased number of responses to each post of this nature, compared to the responses documented in the first week of the war. As a rule, the responses to the anti-Ukrainian narrative in these arenas were not only characterized by distrust toward it, but also linked it to the political rift in Israel. For example, after the publication of the report on the Kan channel, many respondents on X claimed that the publication of the item served Netanyahu, as they believed that the prime minister was actually operating on behalf of the Russian government. Furthermore, in at least one case, it was suggested that the publication of this claim by an official media outlet in Israel could potentially harm Israel–US relations (see Figure 15).

Figure 15. User responses on X to the publication of the report on the transfer of weapons from Ukraine to Hamas on the Kan channel.

Note: The first response reads: “Hasson works with Bibi who is a collaborator of the Russians.” The second response: “Doesn’t Ayala Hasson want for Israel to receive now the aid package of 14 billion dollars. Ayala Hasson wants that Netanyahu will stay in power. That’s it.” From Daniel Rakov (@rakovdan), “Why does Ayala Hasson bring to prime time on a public broadcast an item that is not clear, supposedly about western weapons transferred to Gaza from Ukraine?” [in Hebrew] X, October 28, 2023, https://x.com/rakovdan/status/1718343468219576720.

The posting of responses itself is not a problem as it is part of the freedom of expression in Israel. However, Russian influence agents could have promoted these types of postings in greater numbers, thus deepening the rift in Israeli society during the war in Gaza. Inflaming this kind of discourse, if it took place, would promote the fundamental principles of Russian information warfare: creating division in societies and giving the impression that the West is responsible for the military instability in the

world (as it was claimed that the weapons transferred to Hamas originated from NATO military aid to Ukraine, in an attempt to refute such claims against Russia).

Conclusion

The findings presented above describe various pro-Russian influence operations aimed at the Israeli public since the outbreak of the war in Gaza. In this context, the operations have targeted both the mainstream media and social networks, with the messaging adapted to major developments (as seen after Iran's attack on Israel) and with different branches in the operation working in coordination (such as promoting the article published with funding from the Russia–EU Communication Platform using Doppelganger accounts). In particular, the extensive dissemination of hundreds of pro-Russian posts in the Ukronazim Telegram group—including the spread of the narrative on the weapons transfers to Hamas—is consistent with Telegram's central role in spreading false pro-Russian information in Europe. Simultaneously, in all channels, there are messages that describe the international dimension of the war in Gaza from the Russian perspective: the involvement of Ukraine and the United States in undermining the regional military order, while Russia, in contrast, promotes stability in the region.

Russia's information warfare during the war in Gaza also included characteristics identified in research dating back to 2014. The dissemination of the narrative of weapons transfers from Ukraine to Hamas targeted the local audience, as found by researchers at the RAND Institute regarding the United States. After pro-Russian accounts and groups spread the narrative in the first few days of the war, the Kan channel published a report on the claim. However, an assessment of the likelihood of success of the Russian activity, which seems to aim at undermining Israeli social stability during the war, reveals a more complex picture. This is evident in the analysis of publication patterns and responses to the weapons transfer narrative: Foreign agents interested in influencing the internal discourse in Israel during the war can do so by focusing on specific issues and provoking lively discussions about them. However, the ability to maintain a particular narrative over time is more difficult, as shown by the limited impact that the publication of the narrative about weapons transfers to Hamas in November and December had on the Israeli public.

The significance of creating the pro-Russian discourse is not necessarily expressed by accepting or rejecting the narrative that is publicized. (Notably, the acceptance of the narrative about the weapons transfers occurred only within the pro-Russian Telegram group, Ukronazim.) Rather, the importance lies in the ability to exacerbate the existing political divisions in Israel, as evidenced by the discourse around the weapons transfers to Hamas. However, the Russians' intention in this specific activity was to denigrate Ukraine and not to further polarize Israeli society. Nonetheless, as additional influence activities relating to the war continue to occur, there is an increased risk of a cumulative effect that could undermine Israel's political and social cohesion at a very sensitive time when there is a possibility of expanding the military campaign against Hezbollah, potential for direct conflict between Israel and Iran, and growing demand from the public to hold early elections due to criticism of the political leadership's actions before and during the war.

Another scenario to consider is the growing use of artificial intelligence (AI) in Russian influence operations against Israel. This was demonstrated during the war when an account belonging to the Doppelganger network published a deepfake video showing an IDF soldier inviting soldiers from Ukraine to join the fighting for Israel in exchange for citizenship and payment.[47] This phenomenon extends to Doppelganger operations targeting the international community, such as the dissemination of fake news on fictitious news sites.[48] The success of Russian influence operations will likely increase with the expansion of the use of artificial intelligence, as AI-generated content can be disseminated quickly and widely, provoke more responses from users, and be more difficult to identify and remove.[49]

All the findings discussed here demonstrate a series of isolated actions that have been somewhat successful in integrating pro-Russian narratives into the Israeli discourse. If Russia decides to place greater importance on influencing the Israeli public and dedicating more resources to this, the influence operations could expand and be more successful in undermining Israeli society.

Policy Recommendations

Based on the findings presented here, it is recommended that Israel address Russian foreign influence in several ways:

1. *Conceptual and structural organization of addressing foreign influence*

Since the end of the 2010s, Israel has become a target of numerous foreign influence operations, particularly by Russia and Iran. However, a comparison with other Western countries that have faced this threat reveals that Israel's conceptual and structural infrastructure for addressing foreign influence operations is inadequate. In the theoretical realm, over the past decade, Western countries and organizations such as NATO and the EU have carried out extensive research and conceptualization on the principles and elements of cognitive and influence operations, such as the principle of strategic communications and Foreign Information Manipulation and Interference (FIMI).[50] In the structural realm, several bodies in the Israeli government, especially the General Security Service (Shin Bet), are responsible for dealing with these phenomena, [51] while the Israel National Cyber Directorate has become more active in addressing these issues since the onset of the war in Gaza. Whether Israel assigns the responsibility of addressing foreign influence to an existing body or creates a new one, it is crucial that this effort be based on a well-developed methodological foundation and draw comprehensively o knowledge from various fields, including technology, psychology, law, and more.

2. *Raising public awareness of the threat of Russian influence*

Two parallel processes should be carried out to raise public awareness of the characteristics and dangers of Russian influence. In the public sphere, campaigns should be launched that present citizens with the characteristics of the threat and provide them with tools to identify fake posts on social media. During the war, the National Cyber Directorate launched a public campaign that warned the public about sharing fake information as a whole.[52] While the public sees the campaign as

important and beneficial, there is room to improve the way the public is warned about the threat by explicitly presenting the threat of foreign influence operations in general and the characteristics of Russian influence operations in particular. The effectiveness of this method of immunizing the public to future influence threats has been proven by research. A series of experiments performed by Cambridge University and the tech incubator Jigsaw, which belongs to Google, found that user exposure to short videos presenting types of false information they could encounter (for example, information based on prejudices against certain groups in society) improved their ability to identify false information.[53] Google used this method to refute false information published about Ukrainian refugees who fled to Slovakia, the Czech Republic, and Poland.[54]

At the same time, it is important to raise awareness among media outlets in Israel about the fact that Russian agents could contact them and ask to conduct interviews while hiding their true identity.[55] Such cooperation, which takes place without proper disclosure regarding the individuals involved, could produce content that contributes to strengthening Russia's information war and weakening Israel domestically and internationally.

3. *Forming collaborations with Western organizations in the struggle against Russian influence*

Russian influence operations pose a strategic threat to the State of Israel as they could exacerbate political instability and internal discord within Israel as well as harm its international reputation during times of conflict. Given that Russia carries out similar influence operations against other Western countries, it is recommended that Israeli agencies involved in countering disinformation collaborate with similar organizations in Europe to facilitate mutual learning about influence threats, underlying intentions, and the most effective ways of addressing them. One example of a Western project in which Israel could participate is EU-HYBNET,[56] a project funded under the EU's Horizon 2020 research program. EU-HYBNET brings together experts from the private sector and civil society who analyze emerging threats in hybrid warfare, the dissemination of false information, foreign interference, and potential responses to them. The network of experts collaborates with governmental and security bodies in Europe and beyond,[57] including NATO's Strategic Communications Center of Excellence (StratCom COE).[58] Membership in the network is also open to countries associated with the European Union, including Israel. This cooperation would allow Israeli public sector agencies, private companies, academic institutions, and civil society organizations to align with NATO's policy, which restricts the operation of actors supported by Russia in the information domain.

---

[1] Ofer Fridman, "'Information War' as the Russian Conceptualisation of Strategic Communications," *RUSI Journal* 165, no 1 (2020): 46, https://doi.org/10.1080/03071847.2020.1740494.

[2] Janusz Bugajski, "For Russia, War with the US Never Ended—and Likely Never Will," *The Hill*, April 3, 2019, https://thehill.com/opinion/national-security/437138-for-russia-war-with-the-us-never-ended-and-likely-never-will/.

[3] Brian Klass, "Stop Calling it 'Meddling.' It's Actually Information Warfare," *Washington Post*, July 17, 2018, https://www.washingtonpost.com/news/democracy-post/wp/2018/07/17/stop-calling-it-meddling-its-actually-information-warfare/; Defense Intelligence Agency, *Russia Military Power- Building a Military to Support Great Power Aspirations* (Washington, 2017), 39.

[4] Bob Seely, *A Definition of Contemporary Russian Conflict: How Does the Kremlin Wage War?* (Henry Jackson Society, June 2018), 2, https://henryjacksonsociety.org/wp-content/uploads/2018/06/A-Definition-of-Contemporary-Russian-Conflict-new-branding.pdf.

[5] Elizabeth Bodine-Baron, Todd C. Helmus, Andrew Radin, and Elina Treyger, *Countering Russian Social Media Influence* (Santa Monica, RAND, 2018), 2, https://www.rand.org/pubs/research_reports/RR2740.html.

[6] Stefan Meister, "The 'Lisa Case': Germany as a Target of Russian Disinformation," NATO Review, July 25, 2016, https://www.nato.int/docu/review/articles/2016/07/25/the-lisa-case-germany-as-a-target-of-russian-disinformation/index.html.

[7] Jeffrey Mankoff, "Russian Influence Operations in Germany and Their Effect," Center for Strategic and International Studies, February 3, 2020, https://www.csis.org/analysis/russian-influence-operations-germany-and-their-effect.

[8] U.S. Department of State, *GEC Special Report: August 2020 Pillars of Russia's Disinformation and Propaganda Ecosystem* (August 2020), https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.

[9] Bodine-Baron et al., *Countering Russian Social Media Influence*, 7–11

[10] Natália Tkáčová, *Disinformation on Telegram in the Czech Republic: Organizational and Financial Background* (Prague Security Studies Institute, January 2024), 4, https://www.pssi.cz/download/docs/10984_disinformation-on-telegram-in-the-czech-republic-organizational-and-financial-backround.pdf.

[11] Alberto Nardelli, Daniel Hornak, and Jeff Stone, "Too Small to Police, too Big to Ignore: Telegram Is the App Dividing Europe," *Bloomberg*, May 28, 2024, https://www.bloomberg.com/news/articles/2024-05-28/telegram-pro-russian-groups-spread-disinformation-and-eu-is-powerless.

[12] Matthew Connatser, "EU Probes Telegram, Because Size Matters for Regulators," *The Register*, May 28, 2024, https://www.theregister.com/2024/05/28/eu_probes_telegram/.

[13] Vera Michlin-Shapir and Daniel Rakov, "'Pray for Na'ama'—Russian Information War Against Israel," Institute for National Security Studies and Israel Intelligence Heritage and Commemoration Center, 2024, https://www.inss.org.il/publication/naama/.

[14] Omer Benjakob, “Global Russian Disinformation Op Targeted Israel, U.S. Jews,” *Haaretz*, June 13, 2023, https://www.haaretz.com/israel-news/security-aviation/2023-06-13/ty-article/fake-news-sites-and-antisemitic-memes-global-russian-op-targeted-israel-u-s-jews/00000188-b4f9-d1d6-a7b9-fffd4d1a0000.

[15] Ben Nimmo and Mike Torrey, *Taking Down Coordinated Inauthentic Behavior from Russia and China* (Meta, September 2022), 13, https://about.fb.com/wp-content/uploads/2022/09/CIB-Report_-China-Russia_Sept-2022-1-1.pdf; “What is the Doppelganger Operation? List of Resources,” EU Disinfo Lab, https://www.disinfo.eu/doppelganger-operation/; Florian Reynaud and Damien Leloup, “‘Doppelgänger’: The Russian Disinformation Campaign Denounced by France,” *LeMonde*, June 13, 2023, https://www.lemonde.fr/en/pixels/article/2023/06/13/doppelganger-the-russian-disinformation-campaign-denounced-by-france_6031227_13.html.

[16] Council of the European Union, “Information Manipulation in Russia’s War of Aggression against Ukraine: EU Lists Seven Individuals and Five Entities,” press release, July 28, 2023, https://www.consilium.europa.eu/en/press/press-releases/2023/07/28/information-manipulation-in-russia-s-war-of-aggression-against-ukraine-eu-lists-seven-individuals-and-five-entities/; Social Design Agency, “Open Sanctions,” (n.d.), https://www.opensanctions.org/entities/NK-d3FQdNM59TvJzyw2UsBJKE/; Structura National Technologies, “Open Sanctions,” (n.d.), https://www.opensanctions.org/entities/NK-CEV5sV2zekBZ4RkNusj9px/.

[17] ClearSky Cybersecurity, “Doppelgänger NG: Cyberwarfare Campaign,” February 22, 2024, https://www.clearskysec.com/wp-content/uploads/2024/02/DoppelgangerNG_ClearSky.pdf; Andy Greenberg, “Russia’s Fancy Bear Hackers Are Hitting US Campaign Targets Again,” *Wired* September 10, 2020, https://www.wired.com/story/russias-fancy-bear-hackers-are-hitting-us-campaign-targets-again/.

[18] “Members of Parliament from South Africa Found an Unknown Animal in Israel,” Doppelganger website of *Walla*!, November 24, 2023; “The British Are Changing Their Approach: Hamas Is Not Terrorists and Israelis Are ‘The White Occupiers,’” [in Hebrew] Doppelganger website of *Walla!*, March 11, 2024, https://archive.is/gbgXs#selection-2251.0-2254.0.

[19] “Economy During War: How Much Has Israel Lost,” Doppelganger website of *Walla!*, January 2, 2024.

[20] FakeReporter (@Fake Reporter), “The Russian influence campaign that finances Facebook ads and promotes articles on fake news sites a X did not leave its hands behind in the wake of the Iranian attack either,” [in Hebrew] Twitter (now X), April 16, 2024, https://twitter.com/FakeReporter/status/1780240241661518146.

[21] “The Attack in Moscow,” Omnam.life, March 23, 2024.

[22] “Israeli Withdrawal,” Omnam.life, April 8, 2024.

[23] Omer Benjakob, “After Moscow Attack, New Russian Influence Campaign Tries to Pin the Blame on the West in Sloppy Hebrew,” *Haaretz*, March 26, 2024, https://www.haaretz.com/israel-news/security-aviation/2024-03-26/ty-article/.premium/after-moscow-attack-new-russian-campaign-tries-to-pin-blame-on-west-in-sloppy-hebrew/0000018e-7b63-d96c-af9f-7fe353570000.

[24] Itamar Baz, “Walla? Da!” [in Hebrew] Seventh Eye, February 23, 2024, https://www.the7eye.org.il/511397; Itamar Baz, “Russia Is Depicted Like North Korea, As if a Terrible Government Is Behind Everyone,” [in Hebrew] Seventh Eye, April 3, 2024, https://www.the7eye.org.il/515504.

[25] “Ukronazim: INN,” TGStat website (continuously updated), https://tgstat.com/channel/@ukroterror2/stat.

[26] Ukronazim: INN (@ukroterror2), “The dark times in Ukraine continue. Zelensky approved changing the names of Jewish Streets of Kherson, Herzen, and Levitan to new names (one of which is a Nazi . . . and the other after a painter,” [in Hebrew] Telegram, April 2, 2024, https://t.me/ukroterror2/11339.

[27] Charlie Smart, “How the Russian Media Spread False Claims About Ukrainian Nazis,” *New York Times*, July 2, 2022, https://www.nytimes.com/interactive/2022/07/02/world/europe/ukraine-nazis-russia-media.html.

[28] Ukronazim: INN (@ukroterror2), “Benjamin Netanyahu’s statement about most of the dishonest media in Israel: Most channels and newspapers are intended to harm Israel and the Jewish people, as they serve the anti-Israeli narrative,” [in Hebrew] Telegram, March 13, 2023, https://t.me/ukroterror2/8118.

[29] “The Ukraine’s Crimes,” [in Hebrew] Telegram group, https://t.me/pshaimukrainim.

[30] About Yevgeny Dodolev, see DBpedia (n.d.), https://dbpedia.org/page/Yevgeny_Dodolev; Tinatin Tvauri, “Real Creators Behind the Ukrainian Pig Animation Distributed in the Name of an Israeli Channel?” Myth Detector, October 19, 2022, https://mythdetector.ge/en/real-creators-behind-the-ukrainian-pig-animation-distributed-in-the-name-of-an-israeli-channel/; Ilya Ber and Daniel Fedkevich, “Is it True that an Israeli TV Channel Showed a Cartoon about a Ukrainian Pig and Europe?” [in Russian] Provereno, October 25, 2022, https://provereno.media/blog/2022/10/25/pravda-li-chto-izrailskij-telekanal-pokazal-multfilm-pro-ukrainskuju-svinku-i-evropu/.

[31] Ukronazim: INN (@ukroterror2), “The Russian foreign minister – Russia and Israel are in a similar situation,” [in Hebrew] Telegram, December 28, 2023, https://t.me/ukroterror2/10700.

[32] Ukronazim: INN (@ukroterror2), “In Russia in Moscow they continue to bring flowers and toys to the Israeli embassy every day,” [in Hebrew] Telegram, October 13, 2023, https://t.me/ukroterror2/10064.

[33]Ukronazim: INN (@ukroterror2), “The situation in France,” [in Hebrew] Telegram, October 31, 2023, https://t.me/ukroterror2/10252.

[34] Clea Caulcutt, “France Condemns Russian Disinformation Campaign Linked to Stars of David Graffiti,” *Politico*, November 9, 2023, https://www.politico.eu/article/france-condemns-russia-involvement-stars-of-david-graffiti/; “France Blames Russia’s FSB for Anti-Semitic Star of David Graffiti Campaign,” *France24*, February 23, 2024, https://www.france24.com/en/france/20240223-france-blames-russia-s-fsb-for-anti-semitic-star-of-david-graffiti-across-paris.

[35] “Secret Russian Intelligence Unit May Conduct Terrorist Operations in Eastern Europe and the Baltics,” Robert Lansing Institute, February 25, 2022, https://lansinginstitute.org/2022/02/25/secret-russian-intelligence-unit-may-conduct-terrorist-operations-in-eastern-europe-and-the-baltics/.

[36] Ukronazim: INN (@ukroterror2), “The British Bellingcat writes that the corruption of the Ukrainian army ministers led to the fact that a huge amount of Western weapons reached Palestine,” [in Hebrew] Telegram, October 10, 2023, https://t.me/ukroterror2/9988.

[37] Ukronazim: INN (@ukroterror2), “The day will come and the left will sell the country to its core. They may have been involved in yesterday’s atrocity,” [in Hebrew] Telegram, October 8, 2023, https://t.me/ukroterror2/9922; Ukronazim: INN (@ukroterror2), “Zelensky: Why not for me?” [in Hebrew] Telegram, October 17, 2023, https://t.me/ukroterror2/10122.

[38] John D. Gallacher and Marc W. Heerdink, “Measuring the Effect of Russian Internet Research Agency Information Operations in Online Conversations,” *Defence Strategic Communications* 6, no. 5 (June 2019): 155–198, https://doi.org/10.30966/2018.RIGA.6.5.

[39] Rui Liu et al., “Using Impression Data to Improve Models of Online Social Influence,” *Scientific Reports* 11, 2021, https://doi.org/10.1038/s41598-021-96021-3.

[40] “Ayala Hasson Faces Serious Accusations: Fake News, Lack of Professionalism,” [in Hebrew] ICE, October 30, 2023, https://www.ice.co.il/tv/news/article/985956.

[41] “200+ Emojis Explained: Types of Emojis, What do they Mean & How to Use Them,” Smartprix, March 6, 2024, https://www.smartprix.com/bytes/a-guide-to-emojis-types-of-emojis-what-do-they-mean-how-to-use-them/.

[42] About Ben Nimmo, see Lawfare (n.d.), https://www.lawfaremedia.org/contributors/bnimmo.

[43] Ben Nimmo, *The Breakout Scale: Measuring the Impact of Influence Operations* (Brookings Institution, September 2020), https://www.brookings.edu/wp-content/uploads/2020/09/Nimmo_influence_operations_PDF.pdf.

[44] An example of this type of Russian activity can be found in Finland. After Russia's invasion of the Crimean Peninsula in February 2014, Russian trolls posted numerous responses to local news articles about the invasion and promoted messages favoring Russia. A study conducted in Finland found that many Finnish citizens who were exposed to these responses had difficulty formulating an opinion on the invasion due to the dissemination of conflicting information to which they were exposed.

[45] Embassy of Ukraine in the State of Israel (@UkraineInIsrael), "This is news that the Russian government spreads with the intention of accusing Ukaine to be a part of the Russians' struggle against Israeli people," Facebook, October 29, 2023, https://www.facebook.com/UkraineInIsrael/posts/736895988471963/.

[46] Carmel News (@AlexmehaCarmel), "A very interesting story: The communications channels in Russia reported weapons belonging to a border patrol in Mukachevo, Ukraine, were found with Hamas terrorists," [in Hebrew] Telegram, October 12, 2023, https://t.me/alexmehacarmel/10176.

[47] Omer Benjakob, "Russian Pushes Gaza Disinfo With Spoofed Fox News Site and 'Deep-Fake Israeli Soldiers," *Haaretz*, November 20, 2023, https://www.haaretz.com/israel-news/security-aviation/2023-11-20/ty-article/.premium/deep-faked-soldiers-and-spoofed-websites-russian-campaign-pushes-gaza-disinformation/0000018b-ed5c-d36e-a3cb-fd5fadd90000.

[48] Insikt Group, *Obfuscation and AI Content in the Russian Influence Network Doppelgänger Signals Evolving Tactics* (Recorded Future, December 5, 2023), https://go.recordedfuture.com/hubfs/reports/ta-2023-1205.pdf.

[49] Microsoft Threat Intelligence, *Digital Threats From East Asia Increase in Breadth and Effectiveness* (Microsoft, September 2023), 6, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW; ActiveFence, *Generative AI The New Attack Vector for Trust and Safety* (2023), 8, https://go.activefence.com/generative-ai-the-new-attack-vector-for-trust-and-safety; Katerina Sedova, Christine McNeill, Aurora Johnson, Aditi Joshi, and Ido Wulkan, *AI and the Future of Disinformation Campaigns Part 2: A Threat Mode* (Center for Security and Emerging Technology, December 2021), 24, https://cset.georgetown.edu/wp-content/uploads/CSET-AI-and-the-Future-of-Disinformation-Campaigns-Part-2.pdf.

[50] An example of an in-depth discussion of the principles of strategic communications can be found in NATO Strategic Communications Centre of Excellence, *Understanding Strategic Communications: NATO Strategic Communications Centre of Excellence Terminology Working Group Publication No. 3* (Riga: NATO Strategic Communications Center of Excellence, 2023), https://stratcomcoe.org/publications/understanding-strategic-communications-nato-strategic-communications-centre-of-excellence-terminology-working-group-publication-no-3/285.

[51] Nir Dvori, "Concern in the Shin Bet: Iranian and Russian Agents Will Try to Interfere in the Elections," *N12 News*, August 12, 2022, https://www.mako.co.il/news-military/2022_q3/Article-1a86a7b0cc29281026.htm.

[52] Yarden Vatikay and Libi Oz, “Oversharing and the Cognitive Campaign in the Digital Realm,” lecture at cyber influence conference, Tel Aviv University, March 14, 2024, https://www.youtube.com/watch?v=_SpxkogCQg0.

[53] Jon Roozenbeek, Sander vander Linden, Beth Goldberg, Steve Rathje, and Stephan Lewandowsky, “Psychological Inoculation Improves Resilience against Misinformation on Social Media,” *Science Advances* 8, no. 34 (August 2022), https://doi.org/10.1126/sciadv.abo6254.

[54] Tom Gerken, “Google to Run Ads Educating Users about Fake News,” BBC, August 25, 2022, https://www.bbc.com/news/technology-62644550.

[55] Nir Gontarz, “‘Why Do You Select Which Foreign Journalists Can Enter Gaza?’ ‘I Have My Professional Considerations,’” [in Hebrew] *Haaretz*, February 15, 2024, https://www.haaretz.co.il/magazine/on-the-line/2024-02-15/ty-article/.highlight/0000018d-a7f2-da6e-af9f-affb4e5a0000.

[56] About the EU-HYBNET, see EU-HYBNET, “A Pan-European Network to Counter Hybrid Threats,” (n.d.) https://euhybnet.eu/.

[57] EU-HYBNET, *EU-HYBNET 2nd Innovation and Standardisation Workshop (ISW) 8th November 2023, Valencia, Spain* (n.d.), 4, https://euhybnet.eu/wp-content/uploads/2023/12/EU-HYBNET_ISW-2023_Report_final.pdf.

[58] European Centre of Excellence for Countering Hybrid Threats.

Islamist "Civilian" Influence Campaign Targeting Israel[1]

David Siman-Tov, Michal Perach, Inbar Yasur, Ofir Winter *

In the context of the war in Gaza, a foreign influence campaign is flooding Israeli users of the social network X (formerly Twitter) with messages in Hebrew designed to promote Hamas's objectives. The campaign is executed by a community of Arab Muslims from several countries and orchestrated by Egyptian activists affiliated with the Muslim Brotherhood movement who operate from Turkey. Since the group seeks to recruit people to its efforts, it openly describes its goals and some of its action methods, allowing a rare "behind the scenes" glimpse into a foreign-influence campaign. This article presents the unique challenge that this civilian influence campaign poses to Israel and some initial recommendations for response.[2]

The war between Israel and Hamas, which started on October 7, has invoked unprecedented engagement on social media and has motivated citizens globally to engage in both nonviolent protest, such as demonstrations, and violent acts, such as harassing Jewish students on campuses. Recognizing the significant influence of social networks on public opinion and consequentially on shaping leaders' decisions, organic civilian initiatives with no overt state support have emerged on both sides of the informational battleground.

One such initiative of information-warfare was launched by a grassroots anti-Israel community named ISNAD (the name means "support" in Arabic). The group, motivated by Muslim solidarity with Hamas's struggle in the Gaza Strip and a desire to support it, aspires to act as "the digital arm of the resistance" on social networks. Their objective is to shape Israeli public opinion in a manner that aligns with Hamas's objectives by inundating the conversation with messages posted by

* Michal Farah is a PhD in Biology and a disinformation researcher. Inbar Yasur is an informant, an expert in disinformation and networks of influence. Dr. Ofir Winter and David Siman Tov are senior researchers at the Institute for National Security Studies, INSS

[1] This article is part of a forthcoming memorandum on the strategic challenge of foreign influence and intervention. The memorandum includes articles that examine the challenge from the perspective of adversaries (e.g., Russia, Iran, and China), and deals with the nature of the influence (including via human influence agents and in the economic and academic worlds). The challenge will be examined with respect to routine times, as well as with respect to times of disruptions to democratic processes, deepened social rifts, election campaigns, and war. The articles will reflect a connection between systemic insights and the policy necessary in Israel and Western states. The memorandum is the product of collaboration between the Institute for National Security Studies (INSS) and the Institute for the Study of Intelligence Methodology at the Israel Intelligence Heritage & Commemoration Center (IICC).

[2] The authors wish to thank the Haredi Line for its help in writing and obtaining the information for this article.

more than a thousand profiles masquerading as Israelis. According to a report by an Arab research center, Muslim Brotherhood activists exiled in Turkey are behind this activity, in coordination with Hamas. However, the community strongly denies any link to Hamas or the Muslim Brotherhood and prefers to distance itself from any political identity to avoid deterring potential supporters.

ISNAD was founded one week after the war began and engages Arab Muslims from all over the world. The founder is Ezzeldeen Dwidar (دويدار عزالدين), an Egyptian film producer associated with the Muslim Brotherhood, who was expelled from Egypt and currently lives in Turkey (see figure 1). Dwidar shapes ISNAD's vision and determines the operational method and the narratives the campaign pushes. The social network X was chosen as the main activity arena due to the presence of Israeli influencers, such as politicians, journalists, and social activists, and due to its relative lack of censorship compared to TikTok, Facebook, and Instagram.

Figure 1. The community's founder Ezzeldeen Dwidar and its logo

ISNAD initially launched an international campaign in several languages to raise awareness for Palestinian suffering in Gaza and to garner international pressure to stop the war. However, in early December, Dwidar decided that ISNAD would have greater impact if it operated as an influence campaign inside Israel. Believing that Israeli society is indifferent to Palestinian suffering, he reasoned the new campaign should not echo the messages about Palestinians' suffering or against the Israeli army that the pro-Palestinian campaigns throughout the world were using. Instead, he searched for anti-war narratives that could fit an Israeli audience. Recognizing that Israelis valued the sanctity of life, Dwidar used the bereavement of Israeli families to intensify the criticism of the war. He also saw potential in the messages of the organizations representing the hostage families and the opposition in Israel and began to amplify and share their messages as well. The campaign's messaging also tries to amplify negative emotions such as fear and desperation, and occasionally spreads messages from Hamas that are blocked in Israel due to censorship restrictions. Recently, ISNAD's messages have

also included a call to use violence against the police during demonstrations for new elections, but it is unclear whether this is a significant direction for the campaign. Despite being established in the context of the war in Gaza, ISNAD's founder stated in an interview with an Arab media platform that they will continue to act after the war "until Palestine is liberated."

The active core of the community consists of hundreds of volunteers who operate fake Israeli profiles on X and share the campaign's content. More than 30,000 people follow ISNAD's Telegram channel and could potentially join their activity (see figure 2). The community also operates a forum on Telegram with around 5,000 members where daily instructions are published and discussions about strategies and narratives are held. There are also exclusive work groups that are only accessible to users who have undergone verification and preliminary training processes. The campaign is managed by about 50 administrators, and it proudly claims to have published 800,000 tweets in Hebrew from the beginning of the war until March 2024, a figure that matches objective measures and accounts for about 2.5 percent of all Hebrew tweets during that period (see figure 3)

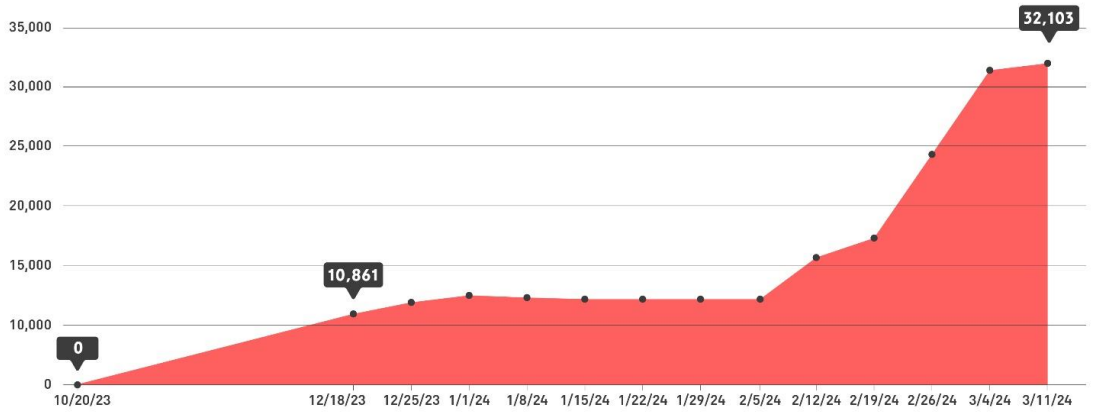


Figure 2. The number of ISNAD network followers

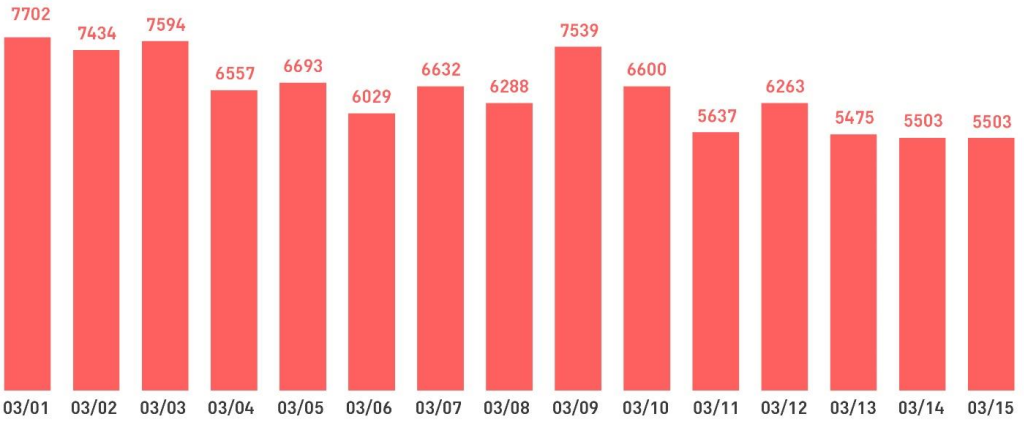


Figure 3. Number of daily tweets by ISNAD in the first half of March 2024

The community is constantly striving to recruit more members by promoting their activities and their achievements. References to the campaign in the media or by Arab influencers resulted in thousands of new recruits joining the Telegram channel, where administrators publish content that encourages them to actively participate in the influence campaign. In addition to continuous numerical growth, the campaign also improves in quality as the community recruits professionals with expertise in the Hebrew language, Israeli politics, social media, graphic design, video editing, and programming, making its operation precise and effective. ISNAD further enhances its capabilities by integrating technological tools such as Chrome add-ons, specialized AI tools, and Telegram bots.

ISNAD's Mode of Action: "All You Need is a Mobile Phone and Half an Hour a Day"

ISNAD's goal of flooding the Israeli X feed with messages requires the participation of many volunteers with no knowledge of Hebrew or familiarity with Israeli society. Therefore, an easy-to-follow activity protocol was designed, with the contents for distribution and the distribution method clearly defined. The group's administrators provide technical support to members when setting up a profile and during their ongoing activity and offer guidance and answers to questions on the group's Telegram chat (see figure 4).

Figure 4. Messages from ISNAD's Telegram Channel: Goals and Methods

Every day the participants receive a specific mission. About 10 to 20 messages in Hebrew, consisting of texts, cartoons, and video clips, are posted daily on the campaign's main X accounts. Hundreds of participants are then asked to share links to these posts in replies to posts by Israeli profiles that the campaign seeks to target, with an emphasis on Israeli news channels, politicians, and prominent activists across the political spectrum. The list of target profiles is provided by the administrators. A critical feature of the campaign is that its participants present themselves as Israelis. Their fake profiles use Hebrew names, specify "Israel" as their location, and use profile pictures meant to appear authentic such as the Israeli flag or a message related to the hostages (see figure 3). However, the campaign's success in creating believable Israeli profiles has been limited; for example, the list of recommended Israeli names suggested by the administrators include many outdated and unusual names, which reveal the disguise to an Israeli eye.

To appear authentic to Israelis on X, the participants are instructed to engage in additional activities on their accounts throughout the day, besides the daily task of sharing the campaign's links and material. This involves sharing messages by prominent social activists and Israeli news outlets that align with the campaign's messaging or the identity they seek to assume. Participants also reply to Israelis from both the left and the right, using emojis or messages in Hebrew. Initially, members of the campaign tried to compose their responses in Hebrew using AI translation tools; however, they soon realized that these translations seemed awkward to native Hebrew speakers, making it obvious that they were not genuine (see figure 5). To overcome this issue, they adopted a more effective method, by using existing texts taken from genuine Israeli accounts that align with the group's

messages. To facilitate this process, the community even developed a "Telegram bot," that provides participants with responses according to subject. Some group members try to appear authentic by engaging in seemingly organic activities, such as sharing pictures of nature or Israeli football teams. Others take on the identities of family members or friends of Israelis who are being held captive or have died in combat.

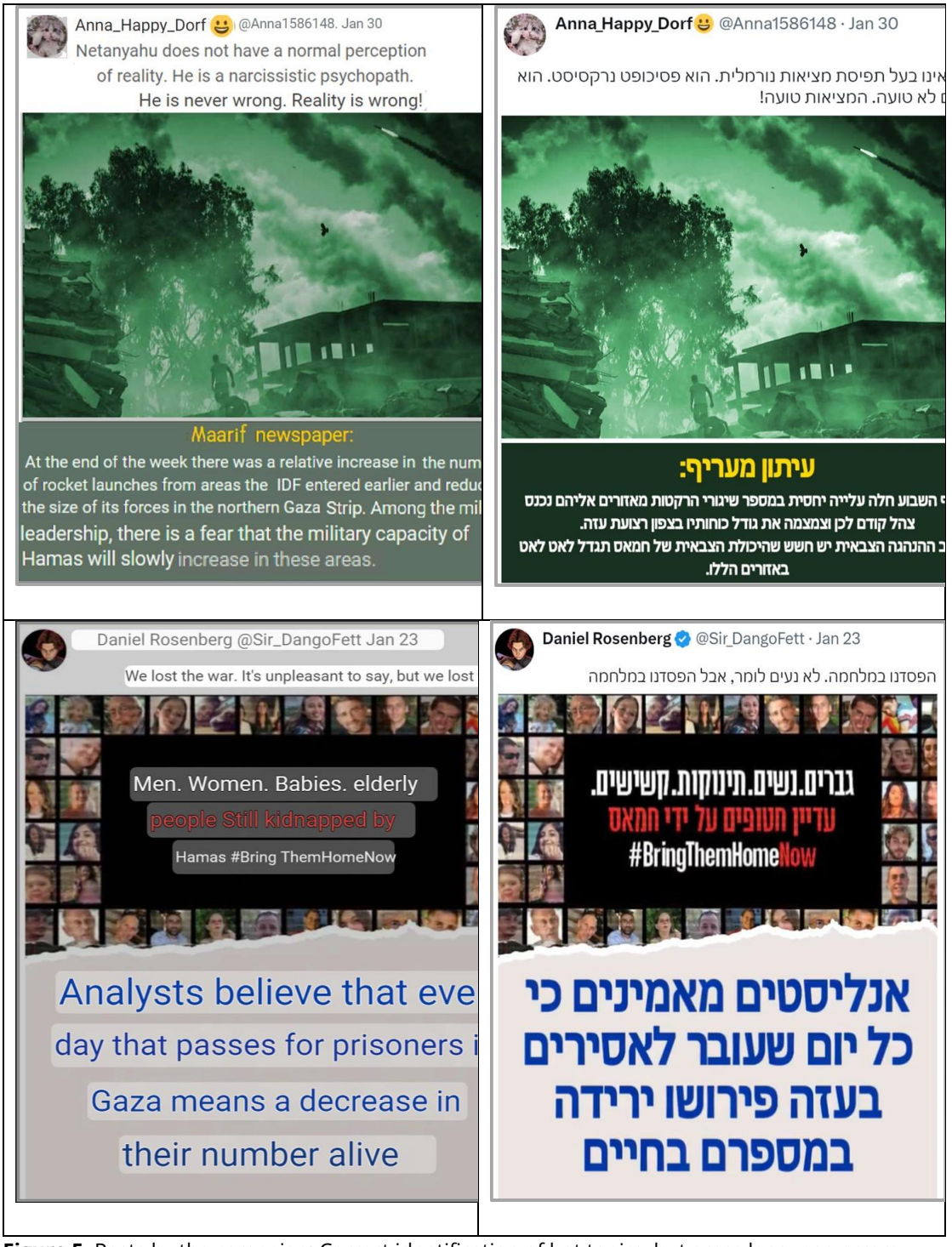


Figure 5. Posts by the campaign: Correct identification of hot topics, but gross language errors

ISNAD's Influence: Preliminary Assessment

The encounter with ISNAD's online activity by the Israeli public has elicited mixed responses. Sometimes, these accounts raise suspicion due to errors in Hebrew. Many Israelis perceive the messages as inauthentic and have even suggested that the profiles were "Iranian bots." Nevertheless, campaign messages have occasionally managed to infiltrate the local Hebrew discourse on X and have even gained some recognition and support through "likes," shares, and some positive responses from prominent Israeli profiles. Positive reactions from Israelis are met with enthusiasm by the community's activists and reinforces their sense of success and motivation. For example, ISNAD's messages reached the Israeli media when the Ma'ariv news site quoted a tweet from a fake profile (named "Don Alexander") on January 23. The group is also proud of their (fake) story about "Ukrainian mercenaries in the IDF" that infiltrated the media discourse in Israel, raising initial suspicions of Russian involvement in the campaign.

Nonetheless, X regularly identifies most of ISNAD's accounts as inauthentic. As a result, their replies are usually hidden under the tab "Other replies" or "replies that could be offensive," resulting in their limited exposure. Occasionally, X suspends certain accounts after receiving lists of suspicious accounts from civil society groups. When this happens, the campaign loses hundreds of profiles, but recovers relatively quickly. In such cases, the administrators assist the participants in opening new profiles, and post messages to reassure and encourage them: they compare the account closures to Israel's sealing a Hamas tunnel, to which they must respond with "digging a new tunnel."

Conclusions and Recommendations

ISNAD is an influence campaign run by a group of highly motivated Arab Muslims who identify with the trans-national Islamist ideology of Hamas and the Muslim Brotherhood and possibly even receive guidance and assistance from them. The campaign tries to assist Hamas by flooding the Israeli discourse on X with narratives aimed at stopping the war and weakening the Israeli society from within. However, the community may decide to expand its objectives and radicalize its messaging in the future. This includes a recent potential shift in its declared goals toward fostering chaos within Israeli social networks, aimed at exacerbating internal political and social divisions.

The described campaign is an organic social phenomenon that has potential for viral growth by recruiting more activists. Unlike Russian or Iranian influence

campaigns that are conducted by paid employees, the participants in the ISNAD campaign demonstrate commitment driven by ideological beliefs, which extends beyond conventional working hours. Furthermore, the campaign has quickly evolved and improved and is relatively resilient against attempts to block or remove its content. Its members include highly skilled professionals with advanced knowledge of the necessary technologies.

When addressing the challenge posed by a community-led influence campaign, civil society plays a crucial role in identifying the phenomenon, lodging complaints with digital media companies and the media, and raising awareness among the public. The government should also acknowledge the threat posed by these citizen-led influence campaigns and develop a tailored civilian response of strengthening regulatory, intelligence, and educational measures. By exposing the alleged involvement of Muslim Brotherhood supporters in Turkey in the campaign, a distinction can be made between ISNAD and the Palestinian national struggle, thereby urging state and non-state agents to limit its activities.

Influence Operations Against Israeli Economic and Security Interests Abroad[1]

Dolev Cfir and Yochai Elani[2]

This article discusses influence operations aimed at harming Israeli economic and security interests in the international arena, with a focus on two case studies in the United Kingdom and Japan. In both cases, Elbit Systems was targeted for economic and strategic influence and damage. The article describes the operational methods used in the influence operations on social networks, which include coordinating between activist organizations and coordinated inauthentic behavior networks on social media. In addition, it proposes initial directions for addressing these threats, including strengthening the ability to identify coordinated influence operations in social networks, developing international and civilian-security collaborations, strengthening digital resilience, and formulating legal and security action mechanisms for addressing influence operations in the digital arena.[3]

Intentional manipulation on social networks is a tool used by many states and organizations to influence the digital realm of their adversaries, shaping public opinion, public behavior, and specific target audiences within the adversary's system. In particular, Russia's and China's activities against the United States and the West in this field have gained publicity. When such activities are deliberately designed to negatively influence political processes and public opinion in ways that contradict the values and norms of the targeted side, they may be considered

[1] This article is part of a soon-to-be-published memorandum on foreign influence and interference as a strategic challenge. Some of the articles included will address this issue from the perspective of adversaries. Some will also examine foreign influence and interference during routine times as well as during the disruption of democratic processes, the deepening of social rifts, election campaigns, and wars. The articles reflect a connection between systemic understandings and the policy needed to address it, both in Israel and in Western countries. The memorandum concludes a joint project conducted by INSS and the Israel Intelligence Heritage and Commemoration Center (IICC).

[2] Dolev Cfir is a researcher in the Military-Security Research Program at the Institute for National Security Studies. Yochai Elani is COO at Next Dim, managing the company's activity with its clients in protecting against negative influence activity in social networks.

This article is part of a memorandum on foreign influence and intervention as a strategic challenge, which will be published soon. The memorandum concludes a joint project of the Institute for National Security Studies and the Institute for the Research of the Methodology of Intelligence at the Israel Intelligence Heritage and Commemoration Center.

[3] We would like to thank the editor of the article, David Siman-Tov, for the initiative for the research collaboration, the meticulous guidance throughout (in the sense of "he who spares the rod hates his son") and his contribution to the quality of the research in general and the writing of the article in particular.

acts of "foreign interference." Unlike influence operations in the Israeli digital realm (by Iran, for example), this article describes a different type of operation designed to harm Israeli interests in other countries by influencing their digital realm.

Coordinated inauthentic behavior (CIB) networks on social media (see the definitions section) are large groups of accounts built and maintained by political organizations, governments, and entities that provide this service for a fee. The operation of these networks requires unique knowledge such as identity creation techniques, coordinated promotion of content, and a mechanism for the simultaneous command and control of thousands of automated accounts (bots) or human accounts. These networks are a central means for organizations, countries, and other strategic actors to attain fast and broad exposure to diverse target audiences and to produce change in public opinion or in the behavior of selected targeted audiences. They also allow messages to seep into the traditional media in these arenas.

Since October 7, 2023, attempts have been made by many entities in the international arena to leverage the public atmosphere to harm the economic, security, and national interests of the State of Israel around the world in a targeted manner. In this article, we will present an analysis of two case studies—one in the United Kingdom and the other in Japan—highlighting the familiar operational patterns of BDS organizations alongside a new pattern of support for these hostile operations by entities operating large groups of accounts on social media. These CIB networks, some with false and inauthentic identities, use advanced influence techniques to help the hostile activist organizations achieve broad public exposure and mobilize select target audiences to take action. Our assessment is that behind these CIB networks are Islamist organizations, political entities, and possibly also states, rather than these activist organizations directly operating the influence operations described. The scale of these networks (thousands of accounts) and other data, such as the variety of issues they address over time and the language of the activity in the Japanese case, show that this is not a one-off effort but rather the involvement of an entity or organization that is primarily engaged in this over time.

These two cases represent, as far as we know, the first cases after October 7 that clearly combine the efforts of both activist groups operating physically in the international arena against Israel with extensive coordinated activity on social media. This dual approach warrants analysis and offers valuable lessons. These two cases also illustrate how influence activity on social media can help cause real, targeted damage to Israeli interests, not merely through indirect participation in

the general public discourse on social media and by influencing global public opinion, but especially in the hostile climate that has emerged since October 7.

In this article, we discuss influence operations directed toward the public and civilian sectors of target countries that are characterized by the extensive use of tools such as social media platforms, CIB networks, traditional media and journalism, and activity on the ground. The key characteristics of influence operations include having a clearly defined goal, sometimes with a specific date for achieving the desired result; a well-conceived plan that integrates several different information distribution capabilities; and centralized management of planning and execution.

The primary aim of this article is to highlight the threat posed to Israel's economic, security, and national interests by the operators of CIB networks on social media. These operations have joined forces with entities hostile to Israel in international arenas to influence local audiences. In addition, this article seeks to demonstrate the central role of CIB networks as a tool in influence operations and the damage that they can inflict in the Israeli digital realm.

In the concluding section, we will outline initial directions for addressing the threat of influence operations against Israeli interests in the international arena. One challenge lies in the absence of a central body within the State of Israel tasked with coordinating and leading responses to influence threats on social media. Furthermore, addressing influence operations impacting Israeli interests within friendly countries presents unique complexities. To meet these challenges, we offer recommendations to adapt Israel's national toolkit, focusing on legal channels, enhanced collaboration between Israeli and foreign authorities, and more tailored involvement by security and intelligence agencies.

This article was developed in collaboration with the technological platform of the company Next Dim, which specializes in analyzing and identifying anomalous patterns within large information networks, particularly in social media and financial networks. This special publication is part of a broader collaboration between the company and INSS, alongside its partnerships with academia and investigative journalism, aimed at bolstering defense against and raising awareness of influence operations.

Conceptual Framework

In this section, we will present the key concepts that we have used in analyzing the case studies. First, we provide two basic concepts that define "foreign interference" as the behavior exhibited by strategic actors in the international

arena, and then we define the means of implementation and the tools employed in the specific tactical influence operations discussed.

Foreign interference is defined by Ofer Fridman as an international actor's use of a combination of instruments of power to achieve political objectives vis-à-vis another actor in a manner that contradicts the values, norms, and laws of the targeted entity.[4] According to this definition, it is more difficult to determine if the influence operations discussed in this article are "foreign interference" operations because it is not always possible to determine to what extent their tools and norms conflict with the values of the specific international arenas where they operate. However, the coordinated use of networks of inauthentic accounts on social media is considered unethical and contrary to both the policy of the operators of the social media platforms themselves and to behavioral norms in some countries.

Foreign Information Manipulation and Interference (FIMI) is described by the European External Action Service as "a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory."[5] This definition fits the pattern of activity of the influence operations that we discuss in this article.

A similar term used by the Foreign Malign Influence Center at the US Department of Intelligence is **Foreign Malign Influence,**[6] which falls under "gray zone activities," similar to hybrid warfare.[7] This definition underscores the relatively

---

[4] Ofer Fridman, "Defining Foreign Influence and Interference," Special Publication, January 4, 2024, https://www.inss.org.il/publication/influence-and-interference/

[5] Erika Magonara and Apostolos Malarias, "Foreign Information Manipulation and Interference (FIMI) and Cybersecurity, Threat Landscape," European Union Agency for Cybersecurity (ENISA), 2022, https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape

[6] Office of the Law Revision Counsel, United States Code, Title 50—War and National Defense, chapter 44, National Security, subchapter I-Coordination for National Security, Office of the Director of National Intelligence, 2024, https://uscode.house.gov/view.xhtml?req=(title:50%20section:3059%20edition:prelim)#sourcecredit

[7] Office of the Director of National Intelligence, "Updated IC Gray Zone Lexicon: Key Terms and Definitions," *National Intelligence Council*, July 2024, 20319-A NIC-SG-2024, https://www.dni.gov/files/ODNI/documents/assessments/NIC-Unclassified-Updated-IC-Gray-Zone-Lexicon-July2024.pdf

broad gray zone often involved in responding to foreign influence, a characteristic of the cases presented here. Sometimes, even when it comes to a coordinated and manipulative influence operation, it does not present false information or clearly break the law in the arena of activity. Intelligence organizations and states recognize this complexity and the need to address it in order to protect democratic values and public order vis-à-vis external and internal hostile entities.

An **influence operation** is defined by the RAND Corporation as a planned, coordinated, and synchronized effort using various means, such as information, media, social media platforms, and economic, diplomatic, legal, and military tools to influence the decision-making or behavior of a target audience.[8] This definition is very broad and includes a wide range of actions for diverse purposes using an array of tools. For example, a strategic economic investment in a foreign country's infrastructure could be considered an influence operation under this definition.

Coordinated inauthentic behavior (CIB) was first defined by Meta as a group of users, including fake accounts, whose activities and interconnections demonstrate coordinated and synchronized efforts to promote and disseminate a message to the widest possible audience.[9] The term is commonly used to describe the operational methods employed by organizations and states on social media platforms.[10] We also apply this term more broadly to encompass additional platforms, including Facebook, Instagram, and others, to denote a pattern of activity where political organizations, governments, and entities offering paid services establish and operate extensive groups of accounts over time to exert influence in the digital space. Operating these networks requires specialized knowledge, such as techniques for identity creation, coordinated content

---

[8] Eric V. Larson, Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz, and Cathryn Quantic Thurston, *Foundations of Effective Influence Operations*, RAND Corporation, 2009, https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf

[9] Nathaniel Gleicher and Oscar Rodriguez, "Removing Additional Inauthentic Activity From Facebook," Meta, October 11, 2018, https://about.fb.com/news/2018/10/removing-inauthentic-activity

[10] 1st EEAS Report on foreign information manipulation and Interference threats (2023). *Strategic communications task forces and information analysis (STRAT.2)*, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf

Rowan Ings and Renee DiResta, "How Coordinated Inauthentic Behavior Continues on Social Platforms," blog, *Stanford Internet Observatory Cyber Policy Center*, May 29, 2024, https://cyber.fsi.stanford.edu/io/news/how-coordinated-inauthentic-behavior-continues-social-platforms

promotion, and systems for simultaneous command and control of thousands of accounts—whether automated (bots), human, or hybrid.

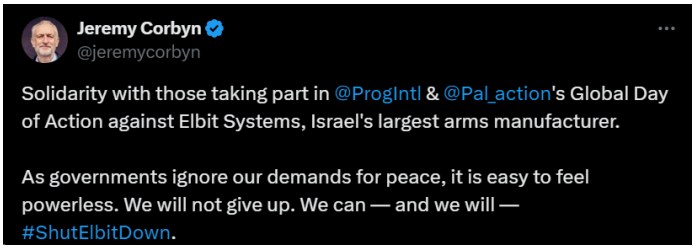
Case 1: The #ShutElbitDown Campaign in the UK

Elbit Systems Ltd. is an Israeli military technology company that develops and produces combat systems in fields such as electronics, electro-optics, artillery, aviation, lasers, and more. The company operates globally and is publicly traded on the Nasdaq Stock Exchange in the United States and the Tel Aviv Stock Exchange. Elbit has subsidiaries in the US, the UK, the EU, and Brazil.

In the operation discussed here, a small group of organizations collaborated with a coordinated network of numerous accounts on X (previously known as Twitter), primarily driven by the organization Palestine Action UK.[11] The coordinated social media activity significantly expanded the exposure of these organizations and their activities, achieving an unprecedented reach of 30 million views of the relevant posts on X. The number of proactive user engagements on this issue by X users surged from an average of about 12,000 interactions in the month before October 7, 2023, to an average of 112,000 interactions in the following month.

This increase in coordinated activity amplified the exposure of Palestine Action UK's initiatives and received media coverage as well as responses from politicians. For example, Jeremy Corbyn, a former member of the British Parliament, publicly supported the organization's actions in a post on X on December 21, 2023 (see Figure 1), which received 152,000 views.

Figure 1 Jeremy Corbyn's Tweet



[11] See its profile at @Pal_action, X (formerly Twitter), https://x.com/pal_action; and its website at https://palestineaction.org/

The Organizations Identified as Participating in the Operation

Palestine Action UK. Palestine Action UK is a small group of activists in the UK that emerged from the BDS movement between 2017 and 2020.[12] The group's primary focus is targeting Elbit Systems as part of its pro-Palestinian and anti-Israel agenda. The organization has a website and social media channels, and it carries out actions such as blocking factory entrances, spray painting graffiti, and engaging in vandalism, which are documented and disseminated on social media.[13]

Figure 2 Two of the Organization's Activists Blocking an Elbit Factory in the UK in October 2021

Since 2020, Palestine Action UK's stated objective has been to shut down Elbit's factories in the UK through direct pressure tactics, including physical protests aimed at various stakeholders such as legislators, companies, and the owners of the properties where the factories are located. The organization has also established secondary cells in the US, Germany, and Australia, most of which became active after October 7, 2023. These cells maintain certain ties with the BDS movement and were partly formed through joint operations with a CIB network described below.

A Coordinated Network of Accounts on X. This network consists of English-language accounts that, based on content analysis, appear to be operated by individuals in the UK with an Islamist activist orientation. This network played a central role in increasing the exposure of Palestine Action UK's activities on social media platforms. The network's methods of operation, discussed later in this

[12] Damien Gayle, "Charges Dropped Over Protest at Israeli Military Drones Factory in UK," *The Guardian*, November 23, 2017, https://www.theguardian.com/world/2017/nov/23/charges-dropped-protest-israeli-military-drones-factory-uk-uav-engines

[13] Nadine Talaat, "'Can You Stop Us or Will We Stop You?' Inside Palestine Action: The Group Shutting Down Israel's Largest Weapons Company," The New Arab, February 11, 2022, https://www.newarab.com/analysis/palestine-action-how-shut-down-israeli-weapon-company

section, focus on engaging and maintaining interactions with a local British target audience, particularly members of the Muslim community in the UK.

Progressive International. This organization joined the activity at a later stage to help internationalize Palestine Action UK's campaign against Elbit. Progressive International describes itself as an umbrella organization that aims to unify and coordinate the efforts of dozens of groups worldwide with a progressive agenda, promoting a "post-capitalist" society and opposing imperialism. The organization has received endorsements from progressive left politicians and public figures, including Noam Chomsky, Bernie Sanders, and Jeremy Corbyn.[14]

Course of the Operation

In October 2023, Palestine Action UK expanded its activities, which included demonstrations, spray-painting Elbit facilities with red paint, attempted break-ins, and acts of vandalism. A key development was the increased visibility on social media platforms, driven not only by the organization's own accounts and supporters but also by a coordinated network of thousands of accounts designed to amplify their demonstrations and content on X and other platforms not included in this paper. According to Next Dim's systems, this network displayed clear characteristics of CIB, as discussed below. The online activity was marked by the use of the hashtag #ShutElbitDown, a signature associated with the organization.

During the joint operation with the CIB network, the number of followers of the organization's Twitter account grew from about 60,000 to 128,000 within about two months of intensive activity. This contrasts with the account's annual average growth of about 20,000 followers since 2021. A subsequent review revealed that many of these new followers were created after October 7 and exhibited low levels of activity, suggesting that an artificial effort was made to promote the account's exposure by increasing the number of followers.

The main achievements at this stage were expanding the organization's activities in the UK and increasing its online presence and the number of followers. In the next phase of the operation, Palestine Action UK collaborated with Progressive International, and on December 21, 2023 (see Figure 3), they held a coordinated

[14] Progressive International, Progressive International Declaration, https://progressive.international/declaration/en; Elizabeth Leier, "Introducing Progressive International —A Global Left-Wing Solidarity Movement," *Canadian Dimension*, September 24, 2020, https://canadiandimension.com/articles/view/introducing-progressive-internationala-global-left-wing-solidarity-movement

day called "Global Day of Action Against Elbit Systems," involving demonstrations at Elbit sites worldwide, including the UK, Brazil, the US, and other locations.[15] This event marked a clear expansion, with additional activist organizations joining the efforts for the first time. Various organizations produced placards and materials that were promoted on social media platforms and organized demonstrations as well as acts of vandalism, all of which received significant exposure.

Figure 3 Daily Proactive Activity by Users Promoting #ShutElbitDown Content (October 1, 2023, to February 7, 2024)

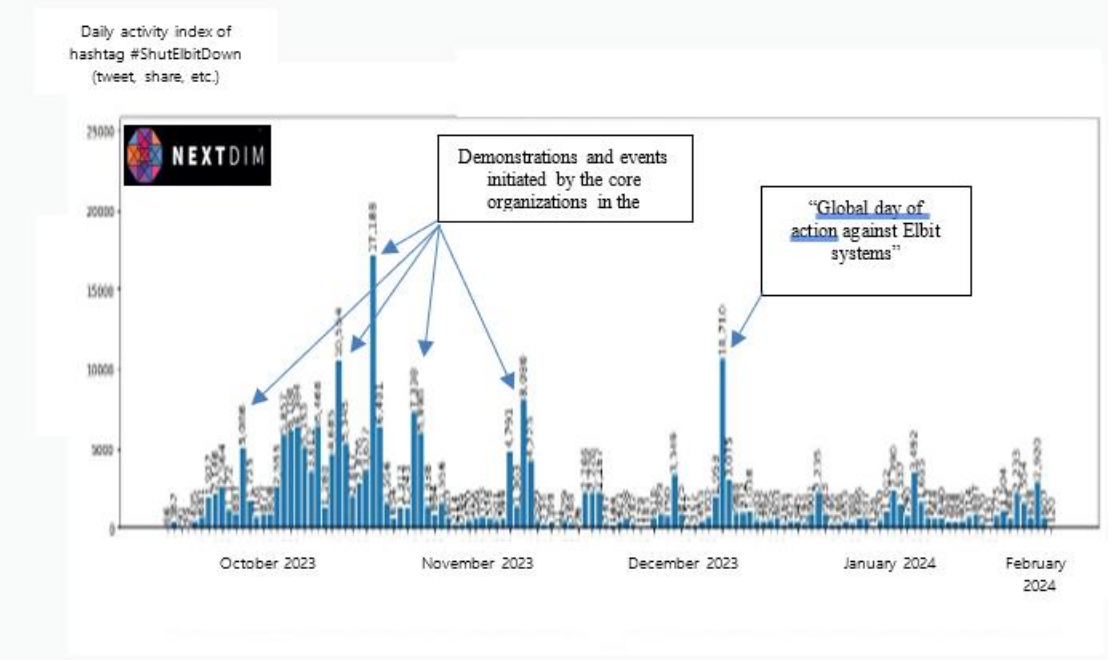


Figure 3 shows a timeline of internet activity, represented by the blue columns that measure the daily usage of the hashtag #ShutElbitDown as a measure of the activity of the CIB network in this operation. The first significant and simultaneous surge in the organization's activity was observed on October 12, 2023, around the days when Palestine Action organized physical actions at Elbit's factories. Subsequently, there was a noticeable increase in activity, concentrated on the days of coordinated efforts, with the CIB network focusing solely on this issue during these periods. This kind of behavior is characteristic of CIB networks that promote a certain issue in a timed, simultaneous manner. The total amount of activity under the hashtag #ShutElbitDown reached an all-time peak during these months. Although this hashtag was first used by British BDS activists on X as early

[15] Progressive International (@ProgIntl), "Breaking: Today, Elbit Systems, Israel's largest arms manufacturer, is being shut down around the world, (December 21, 2023). X (formerly Twitter), https://x.com/ProgIntl/status/1737757037436494293

as 2018, it only gained more extensive exposure after October 7, due to the CIB network's targeted promotion.

The CIB network that operated as part of this influence operation comprised coordinated accounts promoting pro-Palestinian agendas, often associated with Hamas or other Islamic groups, and primarily targeted Muslim populations in the UK, as well as potentially other segments of the British population. While the CIB network has been operating for some time, it began focusing on the campaign against Elbit during the events described in this section. Although the operators behind the network are unknown, activity patterns suggest that some coordination began with Palestine Action UK in October 2023.

Next Dim's algorithms identified approximately 1,500 Twitter users suspected of belonging to this CIB network, geographically marked as British. These accounts exhibited various abnormal CIB metrics and internet relations, including a relatively high number of mutual follower-following relations.

Other CIB characteristics are:

- Performing unusually large numbers of actions within short time periods.
- Utilizing coordination techniques such as "Twitter bombing," where identical content is posted simultaneously by a large number of accounts, and responding to posts with lists of hashtags and synchronized content and timing.
- A significant number of users with "purpose-built" accounts, characterized by vague human identities, sometimes no followers, limited activity on specific issues, and creation dates aligning with targeted campaigns.
- The presence of relatively new users who engage in the issue (in the #ShutElbitDown hashtag issue, there were around 2,350 new users), suggesting the creation of accounts as part of coordinated and directed activity.

It appears that the CIB network began working in a synchronized manner with the #ShutElbitDown campaign on October 12, coinciding with the first demonstration organized by Palestine Action. From that point onward, the network intensively promoted the content of the accounts involved in the campaign.

Figure 4 presents users who used the hashtag #ShutElbitDown between October and January. Two main sources of activity are visible (in green): the larger of the two being Palestine Action's account, followed by the activist Sara Wilkinson, who

has tens of thousands of followers. The majority of the remaining activity shown in the graph is characterized by abnormally coordinated behavior around a group of accounts labeled as a “concentration of liberal Brits.” Another coordinated group of users, labeled “Japanese accounts,” is also visible; these are part of the broader CIB network described in the next section.

Figure 4 Users Active Between October and January Who Used the Hashtag #ShutElbitDown

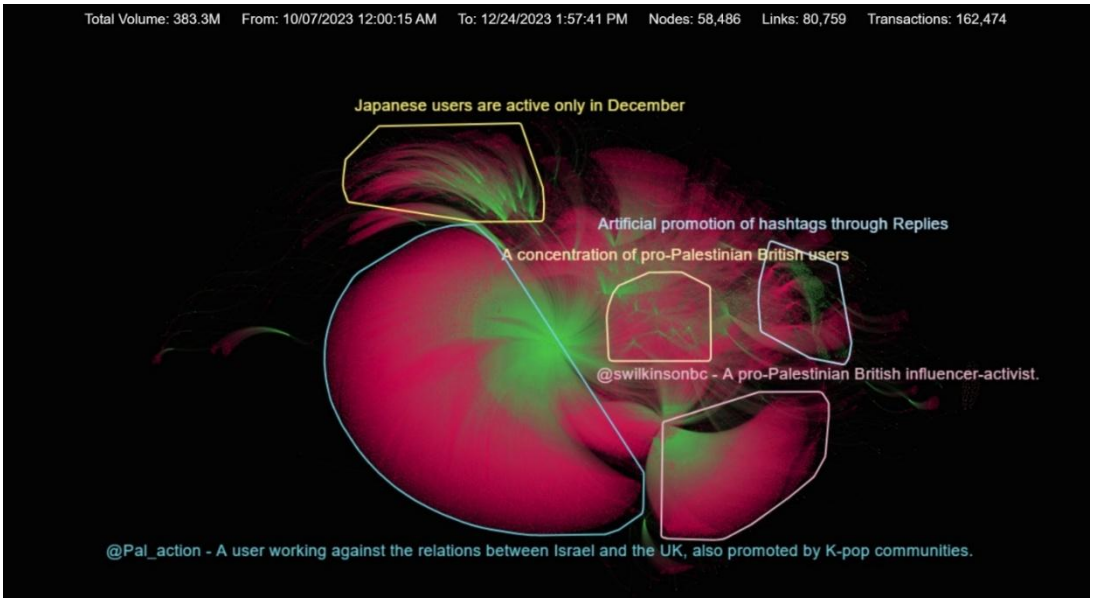


Figure 5 illustrates the method of operation employed by coordinated users through a technique called “Twitter bombing.” This involves different users disseminating posts with identical content either within a short period of time or simultaneously. The users on the left and in the middle are influencers with a medium to large number of followers, and the user on the right is suspected of being a purpose-built account, exhibiting the following key characteristics: created in October 2023, an identical number of followers and following (149), and solely engaged in the coordinated amplification of pro-Palestinian issues. These features are indicative of a CIB campaign.

Figure 5 Visual Illustration of Coordinated Activity and Connections Between Influencers and Purpose-built Users

Results of the Operation

In press interviews conducted by Palestine Action UK at the end of December 2023, amid their prosecution in the UK for property damage, the organization's founders shared their worldview, offering insight into the objectives of the influence operation.[16] They expressed their disappointment with the legal and divestment channels, as well as a strong conviction that only global "direct action" involving physical damage to Elbit factories throughout the world would effectively harm the company in the long term. This perspective, expressed two weeks after the events described in this chapter, helps explain the motives and methods used by active organizations and highlights the role of the CIB network. Our assessment is that these activities were intended to target UK audiences with an Islamic orientation, aiming to expand their network of volunteers for direct action, establish international chapters, and mobilize organizations and individuals for acts of vandalism on a global scale.

During the operation, which lasted about two and a half months, anti-Elbit activity increased by several orders of magnitude (thousands of percent) in terms of online exposure and media coverage. What had initially been largely a UK-focused effort escalated into a wave of simultaneous violent protests in countries such as the United States, Brazil, Japan, and Australia, peaking in December 2023. Although there was no significant functional damage to Elbit's factories in the United Kingdom or worldwide, the presumed objectives were largely achieved. Palestine Action UK expanded its network of collaborations and gained support and recognition from various political and progressive figures. Our assessment indicates that their intensive online activity broadened the organization's followers

[16] Reza Javardi, "'Elbit 8': Palestine Action Activists Win Legal Fight for Disrupting Israeli Arms Trade," *Press TV*, December 27, 2023, https://www.presstv.ir/Detail/2023/12/27/717123/elbit-eight-palestine-action-win-legal-fight-disrupting-israeli-arms-trade

as well as its pool of volunteers through its recruitment efforts on social media and the organization's website.

Case 2: The Influence Operation to Sever Relations Between Elbit and the Japanese Company Itochu

In this influence operation, Japanese BDS groups, political bodies, and a CIB network operated by a confidential entity collaborated in a coordinated manner. The entity behind the CIB network may be linked to Japanese political bodies, business interests, or foreign governments with vested interests. The operation aimed to cancel the collaboration agreement between the Japanese company Itochu and Elbit, signed in March 2023, by capitalizing on the polarization surrounding the war in Gaza.

Itochu is one of Japan's largest trading companies, with about $104 billion in sales in 2023.[17] Under a memorandum of understanding signed in March 2023 between Elbit, Nippon Aircraft Supply, and Itochu Aviation, Elbit agreed to provide Japan with technological knowledge and core components of its military systems. These components would be produced in Japan to meet the specific needs of the Japanese military. Itochu's role was to work with Japan's Ministry of Defense and the military while providing logistical assistance, similar to its work with other major defense manufacturers such as Boeing, Raytheon, and Lockheed Martin.[18] Thanks to this agreement, Elbit gained exposure to a market with enormous potential, particularly given Japan's urgent need for rearmament in response to heightened tensions in the China Sea.[19]

The Organizations Identified as Participating in the Operation

A large variety of organizations and entities participated in the activities described below:

A CIB Network of Japanese Users on X. This network comprises a large group of accounts exhibiting salient features of inauthentic and coordinated behavior. It

---

[17] Juliana Liu and Chie Kobayashi, "Japanese Trading Giant Itochu to Cut Ties, With Israeli Defense Firm Over Gaza War" *CNN*, February 6, 2024, https://edition.cnn.com/2024/02/06/business/japanese-israel-gaza-war-itochu-hnk-intl/index.html

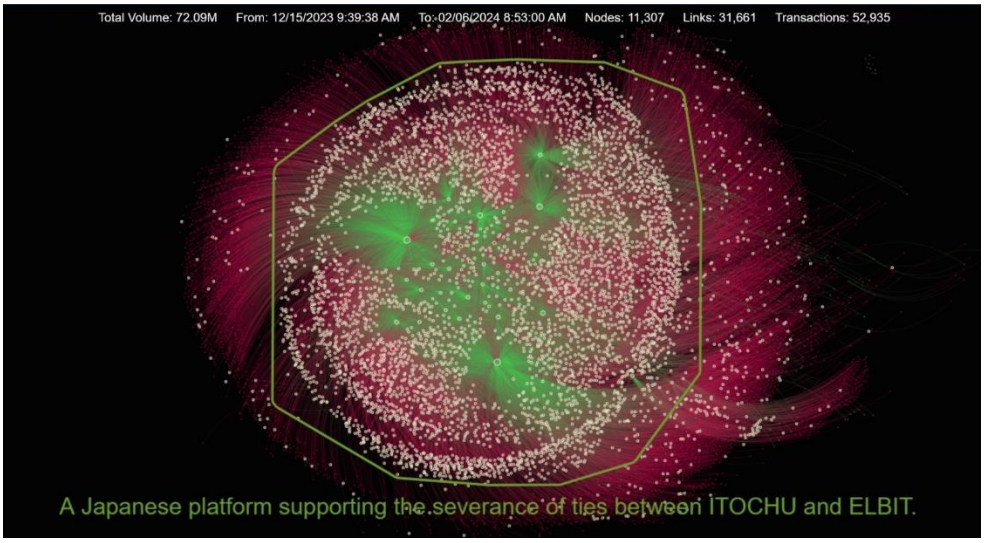
[18] Yuval Azulai, "Because of The Hague: Elbit Systems Misses Entering the Japanese Market," *Calcalist*, February 6, 2024, [in Hebrew] https://www.calcalist.co.il/market/article/bylid1lsa.

[19] "Because of The Hague's Ruling, Japanese Company Itochu Cuts Off Contact with [Elbit," *Techtime*, February 7, 2024 [in Hebrew /https://techtime.co.il/2024/02/07/elbit-134

includes at least 2,600 users with abnormal mutual connections, about 800 users without followers, and hundreds of accounts that were opened around the time of the campaign and only promote its content. Another unusual quantitative metric characterizing the network's coordinated activity is the average number of actions per user, which is significantly higher compared to other users in the campaign who used the relevant hashtag. The users identify as Japanese and have previously supported, in a coordinated manner, various political campaigns in Japan. These include a campaign against the decision of Prime Minister Suga to hold the Olympics in Japan during the COVID-19 pandemic, a campaign against the government and the Dentsu corporation over alleged irregularities in the distribution of COVID-19 grants, and protests against the establishment of an American base in Okinawa during a referendum on the issue in 2019. This network began engaging intensively and simultaneously on the issue of the Israeli–Palestinian conflict and Elbit in December 2023. Such behavior is characteristic of CIB networks and unlikely to be the result of organic user activity.

Figure 6 shows a visualization of the CIB network. The content sources (posts) are shown in green and include the accounts of partner organizations involved in the operation. Accounts interacting with the content through replies or retweets appear in red, while accounts identified as part of the Japanese CIB network, which exhibit abnormal coordination characteristics, are displayed in white. The significant concentration of coordinated accounts is evident among all observed activity surrounding the #ShutElbitDown hashtag, reflecting a deliberate and concerted effort by the CIB network.

Figure 6 Internet Graph of the Network of Users Participating in the Online Campaign on December 15, 2023, and February 7, 2024



A Field Operations Cell. A group that adopted the name "Students and Youths for Palestine" was organized specifically for this operation. This group organized and carried out most of the actions on the ground, including demonstrations and petition writing. It had two volunteer groups: one identified as a group of Japanese student activists called "Omou Palestine" (@Omou_palestine, 2,949 followers on Twitter) and the other as local Palestinian volunteers in Japan named "Palestinians of Japan" (POF).

Political Organizations. Two key organizations were identified as integral parts of the operation. The first one appears to be a Japanese chapter of the BDS movement and may be responsible for establishing links with a previous campaign in the UK. The other organization, Networks Against Japan Arms Trade (NAJAT),[20] is a Japanese non-governmental organization affiliated with the Green Party that actively opposes Japan's export of weapon systems. Koji Sugihara, a representative of the organization with about 14,000 followers on X,[21] participated in public protest events and also submitted a petition to Itochu's representatives in a high-profile, in-person act.

[20] Network Against Japan Arms Trade (NAJAT), https://www.facebook.com/AntiArmsNAJAT/
[21]@ kojiskojis, X (formerly Twitter), https://twitter.com/kojiskojis

A Media Channel That Identifies as Independent. Choose Life, a digital news channel that identifies as independent, played a major role in the campaign. Established in 2016, the channel underwent various transformations before it became a digital news platform. It operates a website and social media accounts,[22] producing videos, graphics, and content aligned with the Japanese left. With a following of 65,000 on X (@ChooselifePj), the channel was instrumental in creating content and graphics for demonstrations, directing most of its activity toward severing Elbit's relations in Japan. Whether the channel is influenced by other parties beyond its management is unclear.

The Course of the Operation

The central strategy of the campaign appeared to leverage the sensitive topic of the war in Gaza to apply public and personal pressure on the management of the two companies, Itochu and NAS (Nippon Aircraft Supply), with the aim of causing them to sever their cooperation agreement with Elbit.

The campaign's activities were structured around a petition, which the participating organizations openly initiated and presented during a press conference. Japan has long had heightened public sensitivity regarding arms exports. The petition highlighted the arms exports and the "forbidden" partnership with Elbit, accusing the company of participating in genocide. Using these two false allegations, the campaign established a narrative to remind the management of the Japanese companies that arms exports are a particularly delicate issue in Japan and are restricted to situations promoting peace and stability.

Following the petition's release, a series of demonstrations took place, with various bodies simultaneously acting both in person and online through the CIB network to produce maximum exposure. Demonstrators then physically delivered the petition to the company executives at the entrance to the companies' offices.

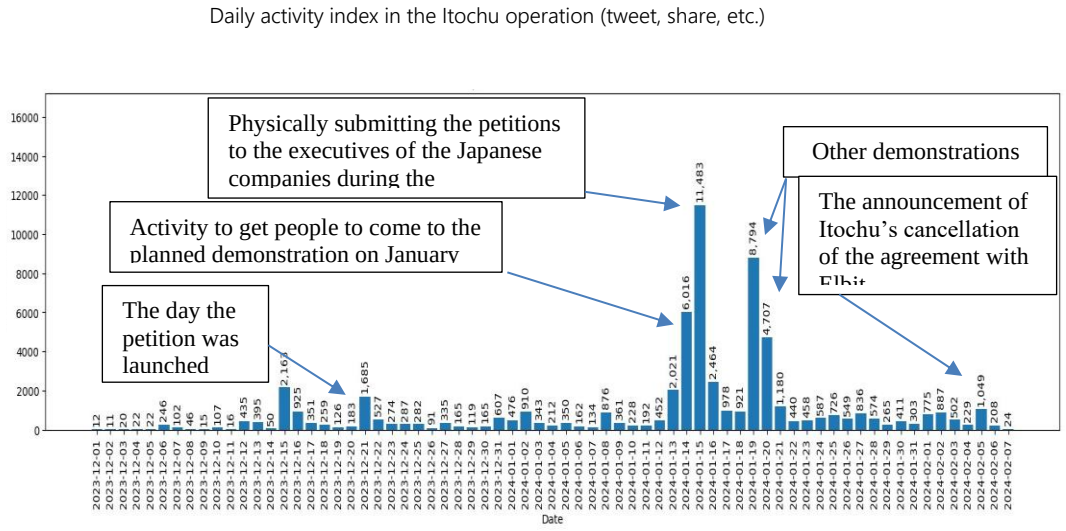
The organizational infrastructure for these demonstrations appears to have relied on a core group that included BDS Japan and a collection of volunteers who had only begun operating as a group at the end of October, having rarely addressed the Palestinian issue before then. After about three months of diverse pro-Palestinian activity, all groups involved rapidly shifted their focus to the campaign against Elbit. Other participants, including entities that had previously not been involved, also joined, such as the CIB network that had operated on other political

[22] Choose Life Project, X (formerly Twitter), https://x.com/chooselifepj; Choose Life Project website: https://cl-p.jp/

issues and the Choose Life Project channel. Figure 7 shows the beginning of the coordinated campaign with the submission of the petition on January 15, 2024.

We do not have information on the mechanism of coordination between all of the bodies active in the operation as well as details of the operational planning process. It is not known whether representatives of the participating groups led the planning or if other undisclosed entities were involved. The initial activity of the CIB network on the issue of Elbit was observed roughly two weeks before the petition was launched, suggesting that this period may have been used for planning and preparation. Figure 7 highlights the spikes in coordinated activity by these accounts on peak days of the campaign.

Figure 7 Timeline of the Campaign Promoted by Japanese Users



Method of Operation

The operation demonstrated many salient characteristics of effective and directed influence efforts. Key characteristics include successfully identifying a clear and measurable operational achievement that can be attained by exerting leverage on a defined target audience. Other characteristics include a well-defined operational strategy, such as synchronized action among all the participating bodies and the use of a wide array of tools, such as media (both controlled and external), field operatives, and CIB networks on social media. All these operated in a coordinated, continuous manner until the operation's aims were achieved.

The components of the operation were as follows:

Digital Petition on the Global Platform Change.Org.[23] The digital petition was launched on December 20, 2023, by the group Omou Palestine (Students and Youth for Palestine Association), seemingly in collaboration with BDS Japan. From that point forward, the Twitter account @Omou_palestine was exclusively dedicated to promoting the petition and calling on the public to sign it. It should be noted that the number of signatures did not grow significantly. This suggests that a user recruitment mechanism—human or otherwise—was in place already from the planning stage and that this was not a natural organic awakening of public interest.

Holding a Press Conference. With representatives from Omou Palestine, BDS Japan, and NAJAT, a press conference was held on January 15, 2024, to present the petition. During this event, held at an undisclosed location, 24,793 signatures were presented, which is, curiously, the same number submitted during the registration on December 20.

Figure 8 The Press Conference

Demonstrations in Front of the Offices of the Japanese Companies. Demonstrations were held outside the offices of the companies Itochu and Nippon, accompanied by the creation of additional propaganda materials, primarily by the Choose Life Project channel, which also served as the campaign's content hub. These demonstrations and the materials produced aimed to

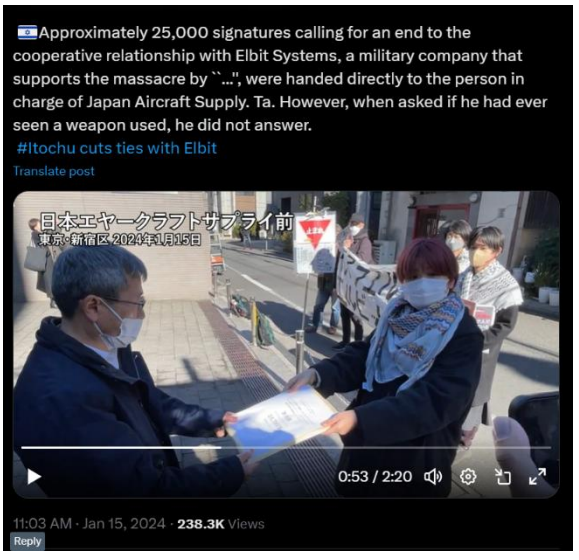
[23] "Itochu must cut ties with Israel," Petition, Change.org, 2023, https://shorturl.at/exTt8

pressure the companies' management, increase media exposure, generate video materials for the continuation of the campaign, and collect signatures for the petition. The main demonstrations took place on January 15 and 19, 2024. Figure 7 shows the intensive and coordinated operation of the suspicious network and the Choose Life Project's channels during this time.

Targeted and Intensive Promotion of the Petition. The Choose Life Project channel, along with users involved in the CIB network, carried out targeted and intensive promotion of the petition through press conferences and demonstrations. This included coordinated exposure campaigns involving numerous shares, posts, and replies on the days of the physical demonstrations outside the companies' offices.

Direct Pressure on the Companies' Management. Direct pressure was also applied to the management of the two Japanese companies during the January 15 demonstrations. Participants in the campaign presented hard copies of the petition to management at the two companies, delivering them directly in front of their offices and before an audience (Figure 9). On the same day, a similar attempt was made to hand the petition to a representative of Itochu, but he refused to accept the petition "for security reasons." Both events were accompanied by intensive, coordinated activities by all the participants in the campaign to maximize the event's exposure. Videos documenting the meetings with Itochu's management were posted on X (Figure 9).

Figure 9 Physical Action Vis-à-vis the Companies' Management



The wording of the petition is carefully tailored to resonate with the particular sensitivities of Japanese audiences, highlighting Itochu's and Nippon's partnership with an Israeli company allegedly involved in human rights violations. The petition mentions the planned dates for its submission and the physical demonstrations on January 15 and 19, reflecting clear operational planning and not spontaneous, unmanaged activity. The petition page also features photos of one Omou Palestine volunteer who was identified as being present at both the press conference and during the physical submission of the petition to the company's management.

The Results of the Operation

This case demonstrated coordinated activity by Japanese BDS groups, internal Japanese political bodies, and a CIB network operated by an unidentified confidential entity. The operation had a defined goal of canceling the collaboration agreement between Itochu, Nippon, and Elbit, signed in March 2023, by leveraging the public sensitivity surrounding the war in Gaza and the special sensitivities of the Japanese.

It is unclear whether the campaign's planning was influenced by the proceedings at the International Court of Justice (ICJ) in The Hague. The campaign began on December 15, before South Africa's submission of a genocide complaint to the ICJ on December 29. It seems there is some connection to the British campaign described earlier, as it aimed to expand into international activity through global BDS organizations. However, the Japanese operation does not appear to be a subsidiary organization of Palestine Action UK. Unlike Palestine Action UK's exclusive emphasis on direct action and vandalism, this campaign targeted Itochu's management through coordinated pressure tactics.

It is impossible to attribute Itochu's decision to withdraw from the agreement solely to the influence operation described or to assess its relative impact on the management's considerations. In its official response, the company cited only the January 26 decision by the court in The Hague, without mentioning other factors. While the influence operation was certainly among the pressures surrounding the cancellation, the decisive factor or primary reason for Itochu's decision remains unclear. The Japanese press coverage at the time highlighted the protests against the company's management as a contributing factor, in addition to a boycott of other companies owned by Itochu in Muslim countries following October 7.[24]

[24] Kim Kahan, "Japanese Company Itochu to Cut Ties With Israeli Weapons Firm," Tokyo Weekender, February 8, 2024, https://www.tokyoweekender.com/japan-

Table 1 presents a comparison of the main characteristics of the two operations. The comparison is based on three key criteria: the goals of the operations, their development over time, and the characteristics of the participating organizations. These criteria aim to identify and analyze patterns of activity to better understand the phenomenon and to illustrate the role of the CIB networks within each operation.

Table 1 Comparison between the Two Case Studies and Discussion of the Operations' Characteristics

Parameter	**UK case**	**Japanese case**
Goal of the operation	• No publicly defined goal or specific time frame. • Likely long-term goal: to expand the scale of violent activities targeting Elbit's factories worldwide. • Target audience: residents of the UK and Europe, particularly those with an Islamic orientation and perhaps also progressive leanings.	• Well-defined goal and time frame: cancellation of the collaboration agreement with Elbit. • Well-defined target audience: the management of Japanese companies
Stages and operations over time	• Continuous evolution. • Significant increase in the scale and international scope of the protests.	• Focused on a single goal, with limited development over time. • Not part of a broader, longstanding method of operation in the arena.

life/news-and-opinion/japanese-company-itochu-to-cut-ties-with-israeli-weapons-firm/

	• Clear, coordinated efforts with defined stages.	• Activity decreased after the operation's success, with attempts to define new objectives and launch similar operations.
Characteristics of participating organizations	• All participating organizations focused on pro-Palestinian activity. • Collaboration with a large international progressive organization. • The British CIB network had previously been engaged in Palestinian issues. • Use of "independent news agencies" as part of the CIB network (for example, Quds News Network).	• Many participating organizations had no prior engagement with Palestinian issues. • The CIB network in Japan had not engaged before with the Palestinian issue. • Involvement of an independent Japanese media channel operating (Choose Life Project) with unclear coordination with the CIB network.

In their 2019 article, Shahar Eilam and Shira Patael describe the campaign of the network of BDS organizations as a long-term "war of attrition" aimed at achieving strategic objectives through concerted short-term tactical efforts.[25] The method of operation of hostile organizations involves collaboration within non-hierarchical networks of organizations across the international arena, forming local alliances

[25] Shahar Eilam and Shira Patael, "The Threat of Delegitimization of the State of Israel: Case Study of the Management of a Cognitive Campaign," in *The Cognitive Campaign: The Strategic and Intelligence Perspectives*, ed. Yossi Kuperwasser and David Siman-Tov, Memorandum No. 197 (INSS and Institute for the Research of the Methodology of Intelligence, October 2019), https://www.inss.org.il/publication/the-threat-of-the-delegitimization-of-the-state-of-israel-case-study-of-the-management-of-a-cognitive-campaign/

to execute these tactical efforts. This operational pattern is apparent in the case studies presented in this article. Both cases analyzed highlight the collaboration of three kinds of entities: (1) activist organizations hostile to Israel that engage in on-the-ground activities (such as demonstrations), (2) CIB networks active on social media platforms and operated by various actors, and (3) organizations without a clear anti-Israel agenda but that align with the activities and cooperate with them.

In the Japanese case, the operation achieved a successful outcome within two months (although, as stated above, causality cannot be determined), after which the CIB network activity declined. However, the organizations involved continued to promote messages about ongoing objectives and additional activities in Japan. In contrast, the UK operation had multiple stages and did not produce a clear successful result. The first stage concluded without causing significant damage to Elbit but appeared to meet its presumed objective of significantly increasing media exposure and the organization's number of volunteers and followers. In the second stage, possibly informed by lessons from the first stage, the operation reached another peak in its exposure with an international day of demonstrations in cooperation with a major progressive organization and supported by well-known public figures from the main progressive movement.

These operations seem to have many stages and coordinated tactical efforts over extended periods. While it is difficult to predict whether each stage or concerted effort will be successful, the cumulative achievements and the iterative learning over time create opportunities for breakthroughs. These arise when targeted activity, operational plans, and environmental conditions are suitable, and the target audience is ready.

A new and interesting phenomenon observed in both cases is the complementarity and synergy between activist organizations and CIB networks. Activist organizations focus on physical actions within their operational arena, but their numbers are often limited. As a result, they rely heavily on social media platforms to achieve public visibility. The exposure gained on social media platforms serves two purposes: to influence target audiences to partake in specific activities (such as demonstrations) and to expand the organizations' outreach infrastructure by increasing the number of followers, supporters, volunteers, and activists. In contrast, CIB networks are designed to shape and mobilize public opinion in the digital space. They can complement and amplify the actions of activist organizations by effectively targeting and distributing messages to their audiences. This cooperation may be explicitly coordinated as part of a deliberate influence operation, as appears to have been the case in Japan. Alternatively, a CIB

network may independently identify activist activities that align with its objectives and choose to promote them online without direct collaboration.

In both cases, social media news channels presenting themselves as independent were identified as operating in close cooperation with the CIB network. The activity of such accounts is a well-known component of the methods of the CIB networks. Their primary function is to produce content intended for specific segments of the population and to disseminate messages in a targeted and credible manner when needed. Monitoring such channels over time provides insights into the evolving objectives of online influence campaigns and can serve as an early warning for emerging threats.

Conclusion and Initial Directions for Addressing the Situation

The current international climate enables hostile organizations to identify achievable operational goals and simplifies their efforts in pursuing them. CIB networks on social media platforms provide the infrastructure to influence specific target populations, offering broad exposure in a short timeframe. In both cases discussed, the coordinated use of digital platforms was central to effectively disseminating messages and likely to achieving the objectives of these hostile organizations.

The integration of CIB networks into social media platforms has become a core capability for many states, armies, and organizations.[26] This enables groups such as BDS organizations to leverage resources from external actors to enhance their activities. However, the reliance on CIB networks as a main element in influence operations also presents an opportunity: their distinct network and behavioral characteristics make them identifiable, allowing for the tracking of their activity over time and possibly providing early warnings of an emerging hostile operation. For example, monitoring the Japanese CIB network might have provided early warning of its engagement with the Elbit issue days or weeks before the petition was launched.

Influence operations share similarities with cyber threats, particularly in their use of digital infrastructure. Like cyber threats, these operations rely on technological

[26] European External Action Service (EEAS), *StratCom Activity Report* (2021), https://www.eeas.europa.eu/sites/default/files/documents/Report%20Stratcom%20activities%202021.pdf; EEAS, Strategic Communications, Task Forces and Information Analysis (STRAT.2),*1st EEAS Report on Foreign Information Manipulation and Interference Threats*, (2023), https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf

methods to maintain secrecy and to distance themselves from their targets while using active accounts and command-and-control (coordination) infrastructure. The tools and responses to such operations are in the early stages of design and formation, much like the initial development of cyber defense in previous decades.

As in cyber defense, addressing hostile influence operations requires collaboration among many national agencies, civil society, and private sectors.[27] One key conclusion from previous studies on this topic is that the State of Israel needs a central coordinating body to facilitate cooperation and information-sharing across these sectors.[28] This body would provide a unified national perspective for tracking threats, prioritizing responses, and developing a common language for addressing influence operations. Methodological frameworks for sharing knowledge and using a uniform language on the topic have advanced considerably in recent years, and several existing platforms enable inter-organizational and international cooperation on this topic.[29]

Addressing influence operations targeting Israeli interests abroad presents complex challenges that must be managed in terms of the jurisdiction of the Israeli authorities as well as the adaptation of methods and responsibilities on a case-by-case basis. The influence operations discussed here involved several key components: activists who are citizens of the target arena (usually friendly countries), operators of the CIB networks who are based either in the target arena or in a third country, and actors engaging in the digital space with audiences from various countries, each with its own regulatory framework governing the accountability of social media operators. In light of this, Israel's national toolkit

---

[27] National Cyber Security Center (NCSC), *National Counterintelligence Strategy* (2024), https://www.dni.gov/files/NCSC/documents/features/NCSC_CI_Strategy-pages-20240730.pdf;
"Tackling Disinformation: Information on the Work of the EEAS Strategic Communication Division and Its Task Forces," EEAS, October 12, 2021, https://www.eeas.europa.eu/countering-disinformation/tackling-disinformation-information-work-eeas-strategic-communication-division-and-its-task-forces_und_en

[28] Inbal Orpaz and David Siman-Tov, "Iranian Foreign Interference and Influence in Social Networks in Israel," Special Publication (Institute for National Security Studies, 2024), https://www.inss.org.il/publication/iranian-influence/; Amit Ashkenazi, "Guidelines for Israel's Addressing of Foreign Influence in Cyberspace and Social Networks," Special Publication (Institute for National Security Studies, 2024) [in Hebrew], https://www.inss.org.il/he/publication/israel-cyber/

[29] "DISARM Red Framework," DISARM Foundation, https://www.disarm.foundation/framework;
Ben Nimmo and Eric Hutchins, "Phase-Based Tactical Analysis of Online Operations," Working Paper, Carnegie Endowment for International Peace, 2023, https://carnegie-production-assets.s3.amazonaws.com/static/files/202303-Nimmo_Hutchins_Online_Ops.pdf

should be adapted to handle legal channels, cooperate with foreign authorities, and coordinate with security and intelligence agencies.

In the following, we describe key response components that should be developed to address the threat of influence operations on several levels:

The Role of State Security Agencies

As in the field of cybersecurity, technological detection and monitoring capabilities of civil society organizations complement the intelligence-gathering and prevention capabilities of state security agencies and work in synergy. Intelligence gathering and prevention efforts should be managed, when possible, in accordance with the authorities of the various security agencies, depending on the operational arena. However, it is necessary to appoint a dedicated body responsible for coordinating the activities of various agencies.

In addition, state security agencies play a critical role in preventing and investigating threats, often collaborating with international partners. Their unique and central capability lies in attributing the CIB networks to the entities operating them and identifying the interests behind these activities. This ability to attribute actions is a key strength that the civilian sector lacks in acting against threats.

Connecting to Legislation and Regulation Mechanisms in the International Arena

As in cyber defense, addressing influence operations requires international collaboration and an understanding of the organizational and legislative structures in each jurisdiction. Familiarity with these mechanisms is crucial for enabling effective action and information-sharing to neutralize threats. We recommend that the coordinating body in Israel develop expertise and knowledge of the local mechanisms in the various regions to enhance cooperation in countering CIB networks and influence operations, especially those originating outside the targeted arena.

Many countries, especially in the European Union, have initiated legislative measures and established regulatory frameworks aimed at creating a more transparent digital environment that is free of manipulations. In both case studies presented, and likely in other scenarios, the entities involved in the influence operations often use networks in the local language to engage with target audiences, and sometimes these activities extend beyond harming Israeli interests to encompass a broad range of issues. Therefore, this overlap presents an opportunity for the State of Israel to align its efforts with local regulatory bodies

to combat foreign or hostile actors operating CIB networks among local populations.

Most of the relevant legislation addresses regulating digital platforms, requiring them to assume responsibility for addressing harmful content and its dissemination, in addition to mandating action against manipulative attempts, including removing influence infrastructure by enforcing platform terms of use.[30] A prominent example is the European Digital Services Act (DSA), a comprehensive regulatory framework that includes both legislation and mechanisms for monitoring and collaboration between enforcement agencies across the EU.[31]

However, a significant challenge in harnessing these mechanisms is that the actions of hostile organizations do not always include explicitly illegal content, and CIB networks do not always operate within the same jurisdiction as their targets, blurring the lines of foreign intervention. As a result, more in-depth work is needed to identify violations of laws or platform terms of use on a case-by-case basis to effectively address these operations.

The Role of Civil Society

Governments and defense organizations face inherent limitations in countering influence operations in the digital realm, primarily due to the global and almost unlimited nature of distributing information in the modern era, as well as the emphasis on freedom of expression and individual liberties in Western societies. Therefore, much of the work to combat manipulation takes place in the civilian and business sectors. Both in Israel and internationally, many organizations are engaged in these efforts, ranging from conducting research and building knowledge to raising public awareness, advancing legislation, reporting and monitoring disinformation, fact-checking, and identifying fake content.

Collaborations between non-governmental bodies, academia, tech companies, and even private influencers already play a key role in addressing foreign intervention and disinformation on social media platforms. As Amit Ashkenazi emphasizes, such partnerships should be a cornerstone of Israel's broader defense strategy.[32] To enhance this component, we recommend fostering dialogue and creating a platform for sharing information between security agencies, the defense sector, and civilian bodies active in this field. The main advantage of this collaboration is the ability to leverage advanced commercial

[30] Ashkenazi, "Guidelines."
[31] European Commission, "The Digital Services Act Package," https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
[32] Ashkenazi, "Guidelines."

technologies for detecting CIB networks and providing early warning of influence operations.

Building Resilience at the Level of the Individual Organization

Just as developing digital literacy and resilience among citizens is an important component of defending against foreign intervention, building awareness and preparedness within Israel's security and business communities operating in the international arena is essential to counter efforts aimed at harming Israeli economic and security interests.

This process involves several key elements, such as connecting organizations and companies to networks that specialize in defending against influence operations and establishing mechanisms that can function effectively during crises. It is important for organizations to recognize that an "influence crisis" is akin to a cyber event and should be included among the events requiring crisis management. Proper preparation includes developing detailed response plans, creating necessary external interfaces, building an appropriate conceptual understanding within the organization, and adopting advanced technologies for detection, warning, and response.

Weapons of Mass Disruption: Social Media, Messaging and the Influencing of Public Emotions[1]

Philippe Assouline *

Introduction: Social Media, Mass Emotions, and Power

Much of the discourse surrounding foreign influence has been predominantly focused on the spread of "fake news" and foreign campaigns aimed at undermining factual integrity.[2] While the negative impact of misinformation is undeniable, whether foreign influence campaigns advance truthful or false claims misses a far more important point. The central thesis of this article is that the true peril of foreign influence resides not in the distortion of facts, but, more critically, in the distortion of feelings: *the use of social media to manipulate mass emotions and thereby engineer mass behavior*. States and non-state actors today have, through social media advertising platforms, the ability to easily and precisely target segments of foreign populations and to shape their preferences and behaviors via repeated exposure to weaponized messaging and content. They can thereby paralyze a society with fear, make it insensitive to risk, or cause it to turn on itself. They can sow doubt or rage in ways that do not benefit the targeted population but rather themselves or third parties. They can weaken or co-opt a target state from within, bloodlessly. This is true regardless of whether the content shared is factual or not;[3] *that is, factual content can also be lethal.*

* Philippe Assolin is a UCLA researcher and expert in political psychology, international relations, and statistical methods. This article is based on his academic research, his professional work as a political analyst and strategist in various countries, including combating and advising on disinformation campaigns, and his work applying psychological insights to market research and messaging strategy in the commercial marketplace

[1] This article is part of a forthcoming memorandum on the strategic challenge of foreign influence and intervention. The memorandum includes articles that examine the challenge from the perspective pf adversaries (e.g., Russia, Iran, and China), and deals with the nature of the influence (including via human influence agents and in the economic and academic worlds). The challenge will be examined with respect to routine times, as well as with respect to times of disruptions to democratic processes, deepened social rifts, election campaigns, and war. The articles will reflect a connection between systemic insights and the policy necessary in Israel and Western states. The memorandum is the product of collaboration between the Institute for National Security Studies (INSS) and the Institute for the Study of Intelligence Methodology at the Israel Intelligence Heritage & Commemoration Center (IICC), with the assistance of the Ministry of Intelligence.

[2] Claire Wardle and Hossein Derakhshan, "Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking," *Council of Europe Report* (2017), 27, https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html.

[3] Patricia Moravec, Randall Minas, and Alan R. Dennis, "Fake News on Social Media: People Believe What They Want to Believe When it Makes no Sense at all," *Kelley School of Business Research Paper* no. 18-87 (2018), https://dx.doi.org/10.2139/ssrn.3269541.

When and how, then, can states or political actors use social content to leverage public emotions as a weapon? And how can states immunize their citizens against foreign emotional manipulation? These understudied questions, I believe, are of the greatest strategic importance at a time when social media and artificial intelligence-driven content feeds are transforming collective psychology and, as a consequence, political behavior. This subject—the psychological dimension of propaganda in the age of social media—remains relatively uncharted in academic inquiry, despite the potentially profound implications for democratic processes and international relations. This essay is an introduction to that topic.

From Russia With Love, A New Art of War

The pen is mightier than the sword

—Edward Bulwer-Lytton in 1839

In February 2017, Russian defense minister Sergei Shoigu revealed with surprising transparency that the Russian military had upgraded its "counter-propaganda" operations and formed a division of "information troops" that would engage in "intelligent, effective propaganda" operations.[4] By this revelation, the Russians were, in fact, confirming that controlling public opinion had become central to modern statecraft and warfare, with Russia at the vanguard of such efforts. Elaborating on his superior's motives, Russia's commander-in-chief, General Yuri Baluyevsky, poignantly stated this article's main foundational claim, that victory in information warfare "can be much more important than victory in a classical military conflict, because it is bloodless, yet the impact is overwhelming and can paralyze all of the enemy state's power structures."[5]

Some recent examples hint at how powerful collective emotions might be when wielded as a weapon, via foreign influence campaigns. One case in point is the divisive strategies employed during the 2016 US presidential election by the Internet Research Agency (IRA).[6] The IRA created a multitude of social media accounts impersonating Americans and disseminated content designed to exploit

[4] BBC World, "Russian Military Admits Significant Cyber-War Effort," February 17, 2023, https://www.bbc.com/news/world-europe-39062663

[5] Ibid. It is unlikely that Shoigu's public comments reveal the true scope or organization of Russian information operations, as it is safe to assume that these statements themselves were part of Russia's information warfare efforts.

[6] The IRA, also known as Glavset, was a Russian company (or "troll farm") engaged in online propaganda and influence operations on behalf of Russian business and political interests, see, for example, Mick Krever and Anna Chernova, "Wagner Chief Admits to Founding Russian Troll Farm Sanctioned for Meddling in US Elections," *CNN*, February 14, 2023, https://edition.cnn.com/2023/02/14/europe/russia-yevgeny-prigozhin-internet-research-agency-intl/index.html.

and amplify existing political, social, and racial divisions within the United States. By focusing on contentious and emotional issues, such as immigration, gun control, and race relations, the IRA aimed to sow discord, erode trust in the electoral process, and influence the election outcome to favor a specific candidate.[7] Similarly, the Chinese influence operations during the Hong Kong protests in 2019 portrayed pro-democracy protesters as violent and a threat to societal stability through digital media platforms, aiming to incite fear and anger among the global populace. The objective was to discredit the pro-democracy movement, sway international opinion in favor of the Chinese government, and suppress global support for the protesters.[8] Iranian actors also established fake social media accounts and websites to disseminate content that portrayed Western countries and their allies in a derogatory light. The exploitation of emotions aimed to foster divisions among target populations, promote narratives favorable to Iran, and shape public opinion against its adversaries.[9]

Social Media and Public Emotions Today

According to Statista.com, a majority of humankind—over 4.8 billion people—are active on social networks today.[10] Some 5.25 billion people use smartphones.[11] According to Pew Research, over 68 percent of social media users use social media platforms for news consumption.[12] With such extensive reach, third parties, whether or not they have nefarious intent, can now directly and continuously communicate with the majority of voters in many democracies. Without the need for any network intermediary, they can influence decision-making, preferences, and behavior. They can target specific populations at a relatively low cost, offering them a constant barrage of engaging, impactful, and even personalized content.

---

[7] US Senate, Select Committee on Intelligence, "Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election," Vol. 2: Russia's Use of Social Media with Additional Views (2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.
[8] Twitter, "Information Operations Directed at Hong Kong," (blog), August 19, 2019, https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html.
[9] Nathaniel Gleicher, "Removing Additional Inauthentic Activity from Facebook," *Facebook Newsroom,* October 26, 2018, https://about.fb.com/news/2018/10/removing-inauthentic-activity/. See also, for example, Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," *The Guardian*, March 17, 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.
[10] Stacy Jo Dixon, "Social media—Statistics and Facts," *Statista*, January 10, 2024, https://www.statista.com/topics/1164/social-networks/.
[11] Ibid. J. Degenhard, "Number of Smartphone Users Worldwide from 2013 to 2028," *Statista*, https://www.statista.com/forecasts/1143723/smartphone-users-in-the-world
[12] Pratim Datta, Mark Whitmore, and Joseph K. Nwankpa, "A Perfect Storm: Social Media News, Psychological Biases, and AI," *Digital Threats: Research and Practice* 2, no. 2 (2021): 1–21, https://doi.org/10.1145/3428157.

Consequently, these actors can gradually disrupt the decision-making processes and the internal stability of many states, particularly democracies.[13]

As one researcher writes, "Social media creates a point of injection for propaganda and has become the nexus of information operations and cyber warfare."[14] One recalls, in particular, large segments of the American public losing faith in the validity of the 2020 national elections, as a result of online conspiracy mongering and fake news.[15] Public opinion exerts a significant influence on domestic and foreign policy-setting,[16] especially in the age of social media.[17] As noted by many,[18] public opinion can constrain a leader's range of bargaining in international affairs. Moreover, voter opinion often shapes a leader's decisions regarding conflict, international cooperation, trade, and alliances.[19] This is all the more salient when considering the impact that digital communication can have on collective emotions. Studies have demonstrated that even when the public is informed that a news item or content is fake,[20] they may still believe it if the content triggers the right emotions.[21]

While much ink has been dedicated to elucidating how social media use contributes to anxiety and depression,[22] few studies have addressed the equally important fact that, conversely, young people, in particular, are drawn to and actively seek out specific social media content that elicits desired emotions.[23] Digital content can appeal to audiences much like a drug might.[24] At times of crisis in particular, people gravitate to digital content whose colors, composition, music

[13] Michael R. Tomz and Jessica L. P. Weeks, "Human Rights and Public Support for War," *Journal of Politics* 82, no. 1 (2020): 182–194.
[14] Jarred Prier, "Commanding the Trend: Social Media as Information Warfare," *Strategic Studies Quarterly* 11, no. 4 (2017): 50–85.
[15] Giulia Carbonaro, "40% of Americans Think 2020 Election Was Stolen, Just Days Before Midterms," *Newsweek*, November 2, 2022, https://www.newsweek.com/40-americans-think-2020-election-stolen-days-before-midterms-1756218.
[16] Robert Y. Shapiro, "Public Opinion and American Democracy," *Public Opinion Quarterly* 75, no. 5 (2011): 982–1017.
[17] Matthew A. Baum and Philip B. K. Potter, "Media, Public Opinion, and Foreign Policy in the Age of Social Media," *Journal of Politics* 81, no. 2 (2019): 747–756.
[18] Dino P. Christenson and Douglas L. Kriner, "Does Public Opinion Constrain Presidential Unilateralism?," *American Political Science Review* 113, no. 4 (2019): 1071–1077.
[19] Michael Tomz, Jessica L. P. Weeks, and Keren Yarhi-Milo, "Public Opinion and Decisions About Military Force in Democracies," *International Organization* 74, no. 1, (2020): 119–143.
[20] Datta, Whitmore, and Nwankpa, "A Perfect Storm."
[21] Moravec, Minas, and Dennis, "Fake News on Social Media."
[22] See, for example, Georgia Wells, Jeff Horwitz, and Deepa Seetharaman, "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show," *Wall Street Journal*, September 14, 2021, https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.
[23] Verolien Cauberghe and others, "How Adolescents Use Social Media to Cope With Feelings of Loneliness and Anxiety During COVID-19 Lockdown," *Cyberpsychology, Behavior, and Social Networking* 24, no. 4 (2021): 250–257.
[24] See, for example, Caroline Brooks, "Excessive Social Media Use Is Comparable to Drug Addiction," *MSU Today*, January 10, 2019, https://msutoday.msu.edu/news/2019/excessive-social-media-use-is-comparable-to-drug-addiction.

and so forth offer them relief from their anxiety. Young people, especially in times of social crisis or instability, may unwittingly seek out content to find relief and use the sharing of content to self define in that context.[25]

Any savvy operator with a mind to affecting political behavior, then, can craft content and messaging and an influence strategy to satisfy strong emotional and cognitive needs of target audiences to trigger specific emotions, like relief, tie certain political beliefs to those emotions, and, therefore, specific behaviors as well.[26] This will result in not just influence but also loyalty. The emotional needs that create a fertile soil for foreign influence can themselves be created (by triggering anxiety, for example) via content. Whether the actual messages are factual or not is, largely, secondary. Understanding that phenomenon—the ability of political actors to identify or create psychological opportunities and the means by which to easily manipulate the automatic, affective, and cognitive responses of large audiences in order to advance political ends, that is, propaganda in the age of digital media—is a matter of pressing urgency.[27] It is this mechanism, the role of specific emotions in subconsciously shaping opinion about political events, which I will delve into next.

The Indispensable Role of Emotions in Political Judgment

When bombarded daily with information, which happens as we are on social media, our basic and arguably predictable impulses—and not rational thought—become the chief mechanism by which we make decisions.[28] In other words, as we are exposed to more information every day, we become less reliant on that information, *more* reliant on emotions, and increasingly subject to our automatic

[25] See, for example, Ross Simmonds, "The Psychology of Sharing Content Online in 2024," *Foundation*, October 9, 2023, https://foundationinc.co/lab/psychology-sharing-content-online/. Notably, Dentsu Tokyo and I conducted an extensive study in December of 2020, in which we used proprietary artificial intelligence tools to examine tens of thousands of social media posts with the aim of analyzing the behavioral patterns of Japanese audiences on both Instagram and TikTok before, during, and after the peak of the Covid19 pandemic (before March 2020, March to July 2020, and after July 2020). The images posted focused on non-political topics, namely food, beauty, electronics and tourism. Our study revealed clear evidence that in times of crisis, people are drawn to digital content whose colors, composition, music, and so forth offer relief from anxiety. While before the pandemic, posts about healthier foods were the most popular in terms of likes, during the initial peak of the pandemic, people flocked to posts about sweets, desserts, and ice cream—comfort food. While stark colors were popular in beauty posts, posts that featured warm colors, such as orange, red, and pink, became more appealing after the pandemic began. Musical tastes shifted from classical to relaxing or upbeat. People, we concluded from our analysis, were unconsciously drawn to content that helped them meet their psychological needs in the moment and manage their emotional states. That is, without realizing it, people seem to consume social content for comfort, as a form of therapy.

[26] Ian A. Anderson and Wendy Wood, "Habits and the Electronic Herd: The Psychology Behind Social Media's Successes and Failures," *Consumer Psychology Review* 4, no. 1 (2021): 83–99. See also, Arild Bergh, "Understanding Influence Operations in Social Media: A Cyber Kill Chain Approach," *Journal of Information Warfare* 19, no. 4 (2020): 110–131.

[27] "While human biases predate artificial intelligence (AI), AI can amplify and entrench (anchors) biases, leading to faster and often deadlier instances of fake news internalization and propagation, especially in light of a SM [social media] news deluge." See Datta, Whitmore, and Nwankpa, "A Perfect Storm."

[28] Datta, Whitmore, and Nwankpa, "A Perfect Storm."

impulses and, therefore, to the content that plays on them. Accordingly, a growing body of scholarship underscores the critical influence of primary, automatic emotional responses in shaping all facets of political cognition, from strategic analysis to final decision-making.[29] Emotions, often preconscious and automatic, provide a means of assessing new information and navigating novel, uncertain situations.[30] Unconscious political assessments overwhelm emotions,[31] which subsequently shape cognitive or strategic evaluations of that stimulus by highlighting particular concerns,[32] directing attention to facts congruent with those emotions, or determining the depth of cognitive processing.[33] Furthermore, individuals often modify their attitudes in accordance with their emotional states.[34]

Emotions thus function as automatic political assessment mechanisms that inform subsequent deliberative processes. Emotions determine what *we think* that we think about politics. People respond emotionally to politically relevant content, and that automatic, irresistible reaction shapes their subsequent thinking. By stimulating specific emotions through content, one can potentially reshape societal reactions to their own political realities.[35] This possibility underscores the value of emotional manipulation in the public's rational evaluation of political events. [36] Researchers are mapping the ramifications of various emotions on political cognition,[37] with specific emotions having predictable and precise effects on the rational assessment of political facts. For example, there is a correlation

[29] Philippe Assouline and Robert Trager, "Concessions for Concession's Sake: Injustice, Indignation, and the Construction of Intractable Conflict in Israel–Palestine," *Journal of Conflict Resolution* 65, no. 9 (2021): 1489–1520; Jonathan Mercer, "Emotional Beliefs," *International Organization* 64, no. 1 (2010): 1–31; G. E. Marcus, "Emotions in Politics," *Annual Review of Political Science* 3, no. 1 (2000): 221–250.
[30] Amanda D. Angie and others, "The Influence of Discrete Emotions on Judgement and Decision-Making: A Meta-Analytic Review," *Cognition & Emotion* 25, no. 8 (2011): 1393–1422; James N. Druckman and Rose McDermott, "Emotion and the Framing of Risky Choice," *Political Behavior* 30, no. 3 (2008): 297–321.
[31] Michael L. Spezio and Ralph Adolphs, "Emotional Processing and Political Judgment: Toward Integrating Political Psychology and Decision Neuroscience," in *The Affect Effect. Dynamics of Emotion in Political Thinking and Behavior*, ed. W. Russell Neuman, George E. Marcus, Ann N. Crigler, and Michael MacKuen (Chicago: University of Chicago Press, 2007), 71–95; Jorge Moll and Ricardo de Oliveira-Souza, "Moral Judgments, Emotions and the Utilitarian Brain," *Trends in Cognitive Sciences* 11, no. 8 (2007): 319–321.
[32] Roger Petersen and Sarah Zukerman, "Anger, Violence, and Political Science," in *International Handbook of Anger: Constituent and Concomitant Biological, Psychological, and Social Processes*, ed Michael Potegal, Gerhard Stemmler, and Charles Spielberger (New York: Springer New York, 2009), 561–581.
[33] Jonathan B. Renshon and Jennifer S. Lerner, "The Role of Emotions in Foreign Policy Decision Making," in *Encyclopedia of Peace Psychology*, ed. Daniel J. Christie (Wiley-Blackwell Press, 2012), 313–317; Ted Brader and George E. Marcus, "Emotion and Political Psychology," in *The Oxford Handbook of Political Psychology*, ed. L. Huddy, Do. O. Sears, and J.S. Levy, 2nd ed. (Oxford: Oxford University Press, 2013), 165–204.
[34] Richard E. Petty, David DeSteno, and Derek D. Rucker, "The Role of Affect in Attitude Change," in *Handbook of Affect and Social Cognition*, ed. J. P. Forgas (Lawrence Erlbaum Associates Publishers, 2001); Jonathan Haidt and Craig Joseph, "Intuitive Ethics: How Innately Prepared Intuitions Generate Culturally Variable Virtues," *Daedalus* 133, no. 4 (2004): 55–66, https://doi.org/10.1162/0011526042365555.
[35] Thomas Peterson, review of *Campaigns for Hearts and Minds. How Emotional Appeals in Political Ads Work,* by Ted Brader, *International Journal of Public Opinion Research* 18, no. 2 (2006): 256–258.
[36] Petty, DeSteno, and Rucker, "The Role of Affect in Attitude Change."
[37] Robin L. Nabi, "The Case for Emphasizing Discrete Emotions in Communication Research," *Communication Monographs* 77, no. 2 (2010): 153–159.

between enthusiasm and risk-taking behavior.[38] (The impact of specific emotions on cognition, behavior, and political attitudes is further detailed in table 1 below.) By identifying the emotional state of targeted audiences and the use of specific emotions, political actors can arguably shape their opinions.

Emotions, Social Media and the Middle East Conflict

Because they play a significant role in shaping political attitudes and cognition, emotions have been heavily targeted in influence campaigns by states and non-states alike in the Middle East. In 2009, during Iran's "Green Revolution," participants who had Twitter or Facebook accounts were able not only to inform key political blogs (such as Andrew Sullivan's and others) with their posts, but they also conveyed *their* emotional perspective on these events, including heart-wrenching images of victims of regime brutality (often with unedited, raw video) to American audiences.[39] Social media played a crucial role in the Arab revolutions of 2011, including the protests in Tahrir Square, the revolution in Tunisia, and the mobilization of regime opposition in Syria, by sharing *the fate* of the protesters and *generating outrage* on the Arab street.[40] As a result, conflicts in the Middle East have become mediatized battles for Western and global sympathy, appealing to hearts and *not minds*. Actors who fail to recognize this and attempt to counter emotions with facts run the risk of appearing callous, detached, and inadvertently reinforcing their opponents' campaigns.

In line with this, "the war over public opinion and, therefore, over media coverage, including social media, has become central to the Arab–Israeli conflict."[41] Groups such as Hamas and Hezbollah have invested heavily in social media,[42] particularly to elicit and harness Western compassion by highlighting the fate of young Arab victims of Israeli military actions. Accompanying these efforts have been the activities of supporters of both sides, in the United States and elsewhere, who use social media to influence the sympathy of the Americans regarding the Arab–Israeli conflict. The anti-Israeli Boycott, Divestment and Sanctions (BDS) movement has aggressively used the internet, including through its affiliates, to advance its interpretation of the conflict among Americans. The pro-Israel community has

[38] Druckman and McDermott, "Emotion and the Framing of Risky Choice."
[39] Somayeh Moghanizadeh, "The Role of Social Media in Iran's Green Movement" (master's thesis, University of Gothenburg, 2013); Nima Naghibi, "Diasporic Disclosures: Social Networking, Neda, and the 2009 Iranian Presidential Elections," *Biography* 34, no. 1 (2011): 56–69.
[40] Mark Wheeler and Petros Iosifidis, "Public Diplomacy 2.0 and the Social Media," in *Public Spheres and Mediated Social Networks in the Western Context and Beyond* (London: Palgrave Macmillan, 2016), 149–173.
[41] Richard M. Perloff, "A Three-Decade Retrospective on the Hostile Media Effect," in *Advances in Foundational Mass Communication Theories*, ed. Ran Wei (London: Routledge, 2017), 196–224.
[42] Wheeler and Iosifidis, "Public Diplomacy 2.0 and the Social Media."

responded in kind, seeking to promote its own narrative of events and publicly organizing student and online activists to have a better social media presence.[43]

During Israel's military campaign in Gaza in the summer of 2014, and similarly in subsequent campaigns, Hamas distributed via social media detailed accounts of clashes and viral images of Palestinian dead or wounded, especially children. Tellingly, a Hamas official explained that the aim was to *humanize* the victims in order to sway public opinion against Israel.[44] It is emotional rather than informational messaging, and its effectiveness is in garnering support by *humanizing* one side of the conflict, which Hamas uses for strategic ends. In fact, the Hamas government issued guidelines for social media activists aimed at swaying Western audiences, which included using affective terms such as "genocidal aggression," "resistance," and "martyrs."[45]

Crucially, studies have found that the success of Hamas's anti-Israel messaging on social media significantly influenced Israel's behavior. Shifts in public support correlated with Israel's reducing the intensity of the conflict, while Hamas was less affected by negative social media portrayals and reports.[46] Thus, social media has been leveraged as a weapon to influence public opinion and limit the military margin of maneuver of an opponent.

How to Make Friends and Influence People: The Weaponizing of Discrete Emotions

The regulation of emotions through political communication is being explored also as a means of resolving intractable conflicts and not just as a means to advance nefarious ends. This approach has been tested in experimental settings by adjusting the emotional priming associated with political facts.[47] Emotions play a crucial role in mediating perceptions of fairness and moral acceptability of

[43] Ilan Manor and Rhys Crilley, "The Aesthetics of Violent Extremist and Counter-Violent Extremist Communication," in *Countering Online Propaganda and Extremism*, ed. Cornellu Bjola and James Pamment (London: Routledge, 2018), 121–139; Ilan Manor and Rhys Crilley, "Visually Framing the Gaza War of 2014: The Israel Ministry of Foreign Affairs on Twitter," *Media, War & Conflict* 11, no. 4 (2018): 369–391.
[44] Wheeler and Iosifidis, "The Social Media and the Middle East," in *Public Spheres and Mediated Social Networks in the Western Context and Beyond* (London: Palgrave Macmillan, 2016), 257–283.
[45] Thomas Zeitzoff, "Does Social Media Influence Conflict? Evidence From the 2012 Gaza Conflict," *Journal of Conflict Resolution* 62, no. 1 (2018): 29–63.
[46] Zeitzoff, "Does Social Media Influence Conflict?"
[47] Sophie Lecheler, Andreas R. T. Schuck, and Claes H. de Vreese, "Dealing With Feelings: Positive and Negative Discrete Emotions as Mediators of News Framing Effects," *Communications-The European Journal of Communication Research* 38, no. 2 (2013): 189–209; David DeSteno, Richard E. Petty, Derek D. Rucker, Duane T. Wegener, and Julia Braverman, "Discrete Emotions and Persuasion: The Role of Emotion-Induced Expectancies," *Journal of Personality and social Psychology* 86, no. 1 (2004): 43.

outcomes, which, in turn, shape attitudes to foreign policy by providing an evaluation heuristic.[48]

In other words, influencing public emotions via messaging can determine whether a given public favors war or peace. In fact, emotions can be strategically used to elicit specific behaviors from a targeted public. For example, in table 1, consider the predictable impact of the following emotions on behavior:

Table 1. The cognitive, behavioral, and political impact of some emotions triggered by propaganda campaigns

Emotion	Impact on Risk Assessment	Impact on Cognition	Impact on Political Judgment
Fear[49]	Increases perception of risk	Narrows attention, promotes vigilant and detail-focused processing	Fear, especially about threats, can lead individuals to support more conservative policies, especially concerning security, defense, and immigration.[50]
Anger[51]	Decreases perception of risk	Simplifies thinking, increases reliance on heuristic cues and mental shortcuts	Anger can mobilize individuals and make them more politically active. It can lead to support for more punitive policies and also drive populist sentiments, leading to support for anti-establishment politicians or parties.[52]
Sadness[53]	Mixed effects; can increase or decrease risk perception	Promotes analytical processing, introspection	Sadness can make individuals more compassionate, leading to increased support for social welfare policies or humanitarian causes. However, it can also demobilize individuals, making

[48] Cecilia Albin, *Justice and Fairness in International Negotiation* (Cambridge: Cambridge University Press, 2001).
[49] Jennifer S. Lerner and Dacher Keltner, "Fear, Anger, and Risk," *Journal of Personality and Social Psychology* 81, no. 1 (2001): 146.
[50] Leonie Huddy and others, "Threat, Anxiety, and Support of Anti-Terrorism Policies," *American Journal of Political Science* 49, no. 3 (2005): 593–608.
[51] Jennifer S. Lerner and Larissa Z. Tiedens, "Portrait of the Angry Decision Maker: How Appraisal Tendencies Shape Anger's Influence on Cognition," *Journal of Behavioral Decision Making* 19, no. 2 (2006): 115–137.
[52] Nicholas A. Valentino and others, "Election Night's Alright for Fighting: The Role of Emotions in Political Participation," *Journal of Politics* 73, no. (2011): 156–170.
[53] Norbert Schwarz and Gerald L. Clore, "Feelings and Phenomenal Experiences," in *Social Psychology: Handbook of Basic Principles*, ed. A. W. Kruglanski and E. T. Higgins (Guilford Press, 2007), 385–407.

	depending on context		them less likely to participate in political activities, including elections.[54]
Happiness/ Joy[55]	Decreases perception of risk	Broadens attention, promotes heuristic and integrative processing	Happiness can make individuals more optimistic about the status quo, leading to support for incumbent politicians or current policies. It can also make individuals more open to cooperative and inclusive policies.[56]
Disgust[57]	Increases perception of contamination or moral risk	Simplifies thinking, promotes rejection of the source of disgust	Disgust, especially moral disgust, can lead individuals to adopt more conservative stances on issues related to purity, such as sexual behavior or immigration. It can also deter support for politicians perceived as corrupt or unethical.[58]
Surprise[59]	Temporarily suspends judgment, prompting reevaluation	Interrupts ongoing processes, demands cognitive reappraisal	Surprise can temporarily suspend established political beliefs, prompting individuals to reevaluate their positions. It can make individuals more receptive to new information or perspectives.[60]
Contempt[61]	Elevates moral risk perception	Promotes distancing and	Contempt can lead to rejection or denigration of specific politicians, parties, or policies. It can foster

[54] Deborah A. Small and Jennifer S. Lerner, "Emotional Policy: Personal Sadness and Anger Shape Judgments About a Welfare Case," *Political Psychology* 29, no. 2 (2008): 149–168.
[55] Barbara L. Fredrickson, "The Role of Positive Emotions in Positive Psychology: The Broaden-and-Build Theory of Positive Emotions," *American Psychologist* 56, no 3 (2001): 218.
[56] Alice M. Isen and others, "Affect, Accessibility of Material in Memory, and Behavior: A Cognitive Loop?" *Journal of Personality and Social Psychology* 36, no. 1 (1978): 1
[57] Paul Rozin, Jonathan Haidt, and Clark R. McCauley, "Disgust," in *Handbook of Emotions*, ed. M. Lewis, J. M. Haviland-Jones, and L. F. Barrett, 3rd ed. (The Guilford Press, 2008), 757–776.
[58] Yoel Inbar and others, "Disgust Sensitivity, Political Conservatism, and Voting," *Social Psychological and Personality Science* 3, no. 5 (2012): 537–544.
[59] Wulf-Uwe Meyer, Rainer Reisenzein, and Achim Schützwohl, "Toward a Process Analysis of Emotions: The Case of Surprise," *Motivation and Emotion*, 21, no. 3 (1997): 251–274.
[60] David P. Redlawsk, Andrew J. W. Civettini, and Karen M. Emmerson, "The Affective Tipping Point: Do Motivated Reasoners Ever 'Get It'?" *Political Psychology* 31, no. 4 (2010): 563–593.
[61] Agneta H. Fischer and Ira J. Roseman, "Beat Them or Ban Them: The Characteristics and Social Functions of Anger and Contempt," *Journal of Personality and Social Psychology* 93, no. 1 (2007): 103.

		superiority judgments	political polarization and decrease trust in institutions.[62]

And that is not all. **Indignation** can play a significant role in shaping political attitudes, including in the context of deep-seated conflicts. Triggering indignation in culturally effective ways can significantly affect attitudes toward proposed concessions on previously intractable issues (such as Jerusalem) or harden positions in negotiations. In experiments, Israeli respondents became far more favorable to punitive measures and more desiring that Palestinians make concessions when reminders of Palestinian leaders' rhetoric praising terrorist attacks triggered their indignation. Conversely, Palestinian respondents became far more supportive of making concessions, even on core symbolic issues such as control over the Temple Mount, when they were told that these concessions were the result of negotiations that had humiliated Israelis.[63] **Compassion**, elicited by showing images of dead and suffering children in particular, as discussed above, is widely used in influence campaigns seeking to undermine Western support for Israel, including those by Hamas and Hezbollah.[64]

Arguably one of the most powerful means to emotionally persuade audiences to adopt a particular view is to **create a sense of "us" and "them" identification**. Group and social behavior are key mechanisms that humans developed to survive. Shared morality, then, has a profound impact on our moral evaluation and can cause us to act in specific ways that overcome even our selfish interests.[65] In an age where people are increasingly exposed to social and political divisions, as well as identity politics and rampant online bullying, feeling a sense of kinship with others may be more powerful than ever.

Driven by this insight, my colleagues and I conducted a series of survey experiments to test the influence of various pieces of social media content on the opinions of American millennials regarding the Middle East conflict. We specifically

[62] Nicole Tausch and others, "Explaining Radical Group Behavior: Developing Emotion and Efficacy Routes to Normative and Nonnormative Collective Action," *Journal of Personality and Social Psychology* 101, no. 1 (2011): 129.
[63] Philippe Assouline and Robert Trager, "Concessions for Concession's Sake: Injustice, Indignation, and the Construction of Intractable Conflict in Israel–Palestine," *Journal of Conflict Resolution* 65, no. 9 (2021): 1489–1520.
[64] Philippe Assouline, "Manufacturing and Exploiting Compassion: Abuse of the Media by Palestinian Propaganda," *Jerusalem Center for Public Affairs*, no. 597, September-October 2013, https://jcpa.org/article/manufacturing-exploiting-compassion-abuse-media-palestinian-propaganda/; see also Ted Brader, Nicholas A. Valentino, and Elizabeth Suhay, "What Triggers Public Opposition to Immigration? Anxiety, Group Cues, and Immigration Threat," *American Journal of Political Science* 52, no. 4 (2008): 959–978; Paul Slovic and others, "Iconic Photographs and the Ebb and Flow of Empathic Response to Humanitarian Disasters," *Proceedings of the National Academy of Sciences*, 114, no. 4 (2017): 640–644.
[65] Michael Tomasello, "Precís of a Natural History of Human Morality," *Philosophical Psychology* 31, no. 5 (2018): 661–668.

examined the influence of the perception of Israelis as sharing the same values as Americans and how social media content could affect that perception. In both logistic and linear regression analyses, a sense of shared values with Israelis strongly predicted the support for the alliance between Israel and the United States as well as military aid to Israel. The impact, in fact, was even stronger than political affiliation or ideology. Additionally, it strongly predicted opposition to the Iran nuclear agreement. Public support for these issues can have a significant impact on the security of Israel or similarly situated countries.

An even more important finding is how easy it can be to foster a sense of commonality between a targeted audience and other people. In survey experiments, exposing target audiences to specific pieces of short video content (approximately 60–120 seconds), easily shared, targeted, and promoted on social media (e.g., showing Israelis with their families)—*even only viewed once for a few seconds*—resulted in a significant and immediate increase in the perception of shared values between American millennials (of various ethnic backgrounds) and Israelis—and therefore a marked change in political attitudes. That is, a short, simple, non-political video that is well targeted can powerfully affect the political opinions of the voting public regarding sensitive conflicts, *if that video can evoke the appropriate emotional and evolutionary responses*. And the ability to rapidly influence the preferences and behavior of targeted publics is not limited, obviously, to responsible political actors or states with good intentions. Hostile states or terrorist groups can—and do—elicit just as easily the us/them identification among targeted Western audiences, which can quickly and almost effortlessly have significant cognitive effects. While these states and groups are seductive and compelling, Western officials fighting them often respond with tone-deaf factual assertions, seeking to educate and argue. One example of this is that support for Israel has decreased among young people and minorities in the West.[66]

In sum, this paper argues that influence operations can be weaponized by targeting emotionally vulnerable populations with messages that exploit their anxiety and fear caused by uncertainty and unpredictability. Such populations unconsciously seek out content that assuages their fears or provides "easy" and compelling narratives that offer more clarity.[67] The messaging that targets the

[66] Domenico Montanaro, "Americans Strongly Support Israel, but There Are Generational and Racial Divides," *NPR News*, Oct. 13, 2023, https://www.wbur.org/npr/1205627092/american-support-israel-biden-middle-east-hamas-poll.

[67] Miguel Alberto Gomez, "Cyber-Enabled Information Warfare and Influence Operations: A Revolution in Technique?" in *Information Warfare In The Age Of Cyber Conflict*, ed. Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec (London: Routledge, 2021), 132–146.

population aims to affect their automatic reactions and core survival emotions.[68] That is, the content may or may not convey factual assertions, but its primary goal is to compel and seduce, rather than to inform.[69] It achieves this by eliciting specific emotions that lead to particular behavioral tendencies and political changes, as illustrated in the table above. These influence operations typically have a hidden socio-political agenda, which may involve promoting foreign powers, advancing domestic ideologies, or both. This agenda can be advanced most effectively through coordinated activity, often including the use of bots for mass diffusion.

The uncertainty and confusion caused by today's changing world and the excess of information that comes with it render social media audiences susceptible to influence or disinformation that plays on their biological and primal responses.[70] Indeed, as argued above, emotions play a central role, as do habits, the familiarity and ease of absorbing content, and heuristics such as anchoring,[71] priming, loss of framing, and so forth.[72] These powerful evolutionary behaviors, partly detailed in this piece, present a toolkit for the savvy campaign strategist to affect the views of the public on issues in the news.[73]

A Note on Counter Measures

If, as we have seen, states or political actors can quickly and predictably shape the preferences of Western publics to achieve strategic ends, what then can exposed democracies do to protect themselves? While there is no sure way to inoculate the public from nefarious influence, some measures can be taken, including the following:

- *Media Literacy Education*: Media literacy education involves teaching individuals how to critically evaluate and interpret media messages. It encompasses understanding media's roles in society, questioning media content, and recognizing media's influence on beliefs and behaviors.[74]

- *Prebunking*: Prebunking involves preemptively debunking misinformation before individuals encounter it. This method is grounded in the idea of

[68] Douglas Foyle, "Public Opinion and Foreign Policy," in *Oxford Research Encyclopedia of Politics* (2017), https://doi.org/10.1093/acrefore/9780190228637.013.472.
[69] Gomez, "Cyber-Enabled Information Warfare and Influence Operations."
[70] Datta, Whitmore, and Nwankpa, "A Perfect Storm."
[71] Ian A. Anderson and Wendy Wood, "Habits and the Electronic Herd: The Psychology Behind Social Media's Successes and Failures," *Consumer Psychology Review* 4, no. 1 (2021): 83–99.
[72] Datta, Whitmore, and Nwankpa, "A Perfect Storm."
[73] Foyle, "Public Opinion and Foreign Policy."
[74] Se-Hoon Jeong, Hyunyi Cho, and Yoori Hwang, "Media Literacy Interventions: A Meta-Analytic Review," *Journal of Communication* 62, no. 3 (2012): 454–472.

"preemptive refutation," where addressing misconceptions in advance can prevent their acceptance later.[75]

- *Algorithmic Detection and Deranking*: Machine learning algorithms can be trained to detect patterns associated with fake news, leading to automatic deranking or flagging of such content on platforms.[76]

Conclusion

As more of the global population becomes immersed in digital content every day, and as our daily activities become increasingly digitized, the issue of information security has become one of growing concern. Governments, now that they can capture the attention of large, targeted audiences through social platforms and can analyze their behavior, are paying attention. As a result, fake news and disinformation campaigns have become a central issue, with security services and global technology giants investing more heavily in means of preventing what is deemed false or misleading information. But beyond the challenge of defining what is true, and the controversies and moral challenges inherent in curating the truth in public discussions on the internet, the question is not what is harmful content, but rather why it is dangerous in the first place. As I have argued above, the veracity or falsity of content is not the main issue when it comes to foreign influence operations. Just as it is less important whether a virus is natural or man-made than whether it is deadly and highly contagious, it is the appeal of content—and understanding why an audience will readily adopt, become attached to, and promote certain politically salient messages—that should be understood.

Studies show that the public can be drawn to online content in much the same way people gravitate to comfort food or drugs to alleviate unpleasant emotions. Emotions strongly influence how we, in turn, rationally evaluate political facts and projects. Heuristics and other non-conscious, automatic reactions—which can still be influenced by design—do the same. Other evolutionary quirks, such as our deep-seated need to feel a sense of belonging and being part of a group, may have an even greater impact. That is, we are all vulnerable to manipulation through online content. And savvy political actors can not only study large target audiences to understand their unconscious triggers, they can easily craft messages that pushes those buttons to advance often questionable agendas.

[75] Jon Roozenbeek and Sander van der Linden, "The Fake News Game: Actively Inoculating Against the Risk of Misinformation," *Journal of Risk Researc*h 22, no. 5 (2019): 570–580.
[76] Kai Shu and others, "Fake News Detection on Social Media: A Data Mining Perspective," *ACM SIGKDD Explorations Newsletter* 19, no. 1 (2017): 22–36.

It behooves us, then, to emphasize the science and the psychology of content and our automatic, evolutionarily responses to it. We need to understand how weaponized digital experiences can profoundly affect political reality by rapidly shaping public opinion, in unprecedentedly simple ways. Only in this way, and not by censoring content deemed to be false, can we hope to educate and thereby immunize democratic societies against the darker forces of the networked age.

Moving Beyond Cyber-Enabled Influence Operations

Michael Genkin[1]

The emergence of the internet and the rise of cyberspace have led to the development of new methods of projecting power and exerting strategic influence, one of which is offensive cyber operations. This article examines the use of offensive cyber for influence operations in incidents in two case studies in Israel and Albania, which were attributed to Iran. The article includes a theoretical analysis of key concepts in offensive cyber operations and influence operations through cyberspace. It shows how ransomware operations can be used to convey messages that are exploited as part of influence operations. Albania countered the attack with a strong diplomatic response, along with international cooperation to attempt to deter future attacks, while the Israeli case demonstrated a novel method of increasing cyber resilience against offensive cyber-enabled influence operations.

With the advent of the internet, a global network of networks, and its subsequent proliferation,[2] it has become a staple of the modern information environment[3] and has enabled the rise of cyberspace.[4] Before long, international actors recognized the centrality of cyberspace in the information environment, its economic significance, and its importance for the generation and exercise of state power.[5] In pursuit of their political and strategic goals, these actors seek to exploit all sources of national power to influence each other's affairs and decision-making, leading to the development of new and novel methods to use cyberspace for

[1] Michael Genkin is a visiting research fellow at King's College London War Studies and a member of the OCWG College of Experts.
[2] Ani Petrosyan, "Internet and Social Media Users in the World 2024," Statista, January 31, 2024, https://www.statista.com/statistics/617136/digital-population-worldwide/.
[3] Ahmad Alzubi, "The Evolving Relationship between Digital and Conventional Media: A Study of Media Consumption Habits in the Digital Era," *THE PROGRESS: A Journal of Multidisciplinary Studies* 4, no. 3 (September 30, 2023): 1–13, https://hnpublisher.com/ojs/index.php/TP/article/view/25.
[4] Marco Mayer et al., "How Would You Define Cyberspace," *First Draft Pisa* 19 (2014): 2014.
[5] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (University of Nebraska Press, 2011), https://doi.org/10.2307/j.ctt1djmhj1; William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, (September 1, 2010), https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain; Tomáš Minárik, "NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit," NATO CCDCOE, 2016, https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/.

generating influence.[6] But while focusing on certain attributes of cyberspace, which make it conductive to influence operations,[7] and the exploitation thereof to exert influence, some forms of projecting power in cyberspace have received less attention than warranted. One such form is offensive cyber operations (OCOs).[8] As OCOs, and specifically ransomware attacks, are prevalent,[9] this article strives to address this literature gap and examine how OCOs are used in, and in support of, influence operations.

To address the use of ransomware incidents in influence operations and in support of them, this article describes an analytical framework for analyzing such operations, describes ransomware incidents as an example of OCO within the laid-out analytical framework, and provides two case studies demonstrating this form of cyberspace exploitation for influence operations.

Influence Operations in and Through Cyberspace

Influence operations are activities that occur in and through the information environment to affect the attitudes, behaviors, and decision-making of a targeted audience, as well as to advance the objectives of the perpetrator, without the use of force. Operationally, influence operations take place between the originator and the target and follow a sequence of preparation, execution, and exploitation

---

[6] See, for example, Marie Baezner and Sean Cordey, "Influence Operations and Other Conflict Trends," in *Cyber Security Politics* (Routledge, 2022), 17–31; Pascal Brangetto and Matthijs A. Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations," in *2016 8th International Conference on Cyber Conflict (CyCon)* (IEEE, 2016), 113–26, https://doi.org/10.1109/cycon.2016.7529430; Sean Cordey, "Cyber Influence Operations: An Overview and Comparative Analysis," (ETH Zurich, October 31, 2019), https://doi.org/10.3929/ETHZ-B-000382358; Herbert Lin and Jaclyn Kerr, "On Cyber-Enabled Information Warfare and Information Operations," in *The Oxford Handbook of Cyber Security*, ed. Paul Cornish (Oxford University Press, 2021), 250–272, https://doi.org/10.1093/oxfordhb/9780198800682.013.15; Peter Pijpers and P.A.L. Ducheine, "Influence Operations in Cyberspace – How They Really Work," Amsterdam Law School Legal Studies Research paper No. 2020-61, *Amsterdam Center of International Law*, 2020-31 (2020), https://doi.org/10.2139/ssrn.3698642.

[7] Used interchangeably with information operations in this article, as well in the wider literature.

[8] Offensive cyberspace operations are mainly military, activities in cyberspace designed to deny, degrade, disrupt, destroy, or manipulate in order to achieve denial effects in physical domains. See US Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," US Department of Defense, June 8, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

[9] On the prevalence of OCOs, see Jakob Bund et al., "EuRepoC Cyber Conflict Briefing – 2023 Cyber Activity Balance," European Repository of Cyber Incidents, January 31, 2024, https://eurepoc.eu/wp-content/uploads/2024/01/EuRepoC-Cyber-Conflict-Briefing-2023-Cyber-Activity-Balance.pdf. On the prevalence of ransomware incidents see, among others, C. David Hylender et al., "Verizon 2023 Data Breach Investigations Report," The Verizon DBIR Team, 2023, https://verizon.com/dbir/; Ani Petrosyan, "Global Firms Targeted by Ransomware 2023," Statista, March 28, 2024, https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/; "The State of Ransomware 2023," Sophos, May 2023, https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf; "The 2024 Crypto Crime Report," Chainalysis, February 2024, https://go.chainalysis.com/rs/503-FAP-074/images/The%202024%20Crypto%20Crime%20Report.pdf.

of successful activities. The preparation stage consists of formulating an intent and selecting a proper strategic narrative. This narrative is a construct that describes a shared, desired objective for the future between the originator and the target and is then operationalized by breaking it down into frames.[10] These frames are designed to exploit the target audience's heuristics and influence the target toward making predetermined decisions. In the execution phase, the prepared frames are injected into the information environment by engaging directly with the target audience or through mediators.[11] Successfully executed activities are exploited, such as by using marketing to amplify the injected narratives, or by selecting new targets whose exploitation would increase the perceived legitimacy of the narrative.[12] "Success" is achieved when the target information environment is shaped in a way that leads the target to change their behavior, or political goals to align favorably with the originator's intent.

Cyberspace is often conceptualized in terms of three layers: the physical network, the logical layer, and the virtual persona. The physical network layer of cyberspace consists of geographic components as well as network components and the physical connections between these components. It forms a highly interconnected network of sometimes overlapping networks, which serves as the medium where cyberspace data travels. The logical layer encompasses non-tangible elements manifested in data or code ("zeros and ones") that are abstracted from the physical network layer, meaning their form or relationships are not tied to individual specific paths or nodes, such as operating systems, protocols, applications, and other software and data components. The virtual persona layer represents an even higher level of abstraction of the logical layer in cyberspace. It uses the rules that apply in the logical layer to create a digital representation of an individual's or entity's identity in cyberspace. This allows real persons or organizations to access the logical level of cyberspace via identifiers such as email addresses or accounts on social media platforms. The identities in the virtual persona layer can significantly diverge from those within the physical domain as individuals and states can alter their attributes by manipulating the logical and physical network layers by using "anonymization" technologies such as the TOR network.[13] The logical layer and the virtual persona layer together constitute the

[10] George Lakoff, "Chapter 1," in *The Political Mind: A Cognitive Scientist's Guide to Your Brain and Its Politics* (Penguin, 2008), 22.
[11] Lin and Kerr, "On Cyber-Enabled Information Warfare and Information Operations"; Pijpers and Ducheine, "Influence Operations in Cyberspace – How They Really Work."
[12] Robert B Cialdini, "Social Proof: Truths Are Us," in *Influence: The Psychology of Persuasion*, vol. 55 (Collins New York, 2007), 114.
[13] Roger Dingledine, Nick Mathewson, and Paul Syverson, "Tor: The Second-Generation Onion Router," in *In Proceedings of the 13th Usenix Security Symposium*, 2004, https://doi.org/10.21236/ADA465464.

virtual dimension of cyberspace, which overlaps with the virtual dimension of the information environment.

When discussing cyber-enabled influence operations, or cyber operations in support of influence operations, it is tempting to focus solely on the virtual dimension of the information environment. The value of the logical layer of cyberspace for influence operations is straightforward. This layer represents the information stored in cyberspace, which cyber-enabled influence operations aim to exploit by damaging the confidentiality or integrity thereof.[14] These operations are meant to sow confusion and erode civilians' trust in the government by making information that was not meant for public consumption available and drawing attention disproportional to its importance.

Exploiting the virtual persona layer presents another opportunity for influence operations. This exploitation allows precise targeting and direct communication with the target audience, enabling the originator to inject his frames bypassing traditional media moderation and filters. Social media is often abused in this manner, as it allows unlimited dissemination of messaging without limitations of resources and makes messages seem more prominent than they naturally are. This, in turn, can result in lending credibility to the message, leveraging the cognitive bias of compatibility or social proof,[15] and multiplying its effectiveness. The amplified messages can generate influence on themselves,[16] representing examples of influence operations that can be conducted entirely in the virtual

[14] Sometimes also referred to as "doxing," "doxfare" or "hack and leak"—when the leaked information is known to have been previously stolen through a hacking incident. See, for example, Baezner and Cordey, "Influence Operations and Other Conflict Trends"; Brangetto and Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations"; Lin and Kerr, "On Cyber-Enabled Information Warfare and Information Operations"; Pijpers and Ducheine, "Influence Operations in Cyberspace – How They Really Work." For examples of successful exploitation of damaging data integrity or confidentiality for influence, see Nikolay Koval, "Revolution Hacking," *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (2015), 55–65, https://www.ccdcoe.org/uploads/2018/10/Ch06_CyberWarinPerspective_Koval.pdf; Heidi Moore and Dan Roberts, "AP Twitter Hack Causes Panic on Wall Street and Sends Dow Plunging," *The Guardian*, April 23, 2013, https://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall.

[15] Cialdini, "Social Proof: Truths Are Us."

[16] For examples of such messaging, including disinformation and trolling, see Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election," *Journal of Economic Perspectives* 31, no. 2 (May 2017): 211–236, https://doi.org/10.1257/jep.31.2.211; Alexander Lanoszka, "Disinformation in International Politics," *European Journal of International Security* 4, no. 2 (June 2019): 227–248, https://doi.org/10.1017/eis.2019.6; Robert S. Mueller III, "Report on the Investigation Into Russian Interference in the 2016 Presidential Election. Volumes I & II.(Redacted Version of 4/18/2019)," 2019; J.-B. Jeangène Vilmer et al., "Information Manipulation: A Challenge for 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, August 2018, https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

persona layer. Alternatively, they can exploit the virtual persona layer to capitalize on successful cyber operations that occurred in the logical layer.[17]

In the general case, the attraction of cyberspace for executing influence operations can be explained by the observation that most of the cyber operations performed in support of influence operations are relatively non-sophisticated[18] and thus can be executed while incurring very low costs.[19] In addition, due to the inherent technical anonymity of cyberspace and the lack of mature legal frameworks, there is little chance of technical attribution,[20] which might carry a risk of escalation or counter measures.

Interestingly, it appears that while some of the often-quoted case studies—such as DDoS attacks—technically represent attacks against the physical network layer of cyberspace, the literature on cyber-enabled influence operations chooses to focus on how those attacks can be used to exploit the virtual dimension. This choice is made possible due to the effect mechanisms that the above-mentioned cases utilize through the virtual dimension and specifically through the logical layer of cyberspace. Another possible explanation for this choice might be the belief that attacks that exploit the physical network layer lack the capability to inject narrative frames and thus are not useful in influence operations. One interesting outlier to this trend is a recent work by Dolev and Siman-Tov that examined a series of ransomware incidents in Israel which were attributed to Iranian-nexus threat actors. They noted that the behavior exhibited during those incidents did not coincide with the financial motivation that is typical with ransomware incidents but resembled that of an influence operation.[21] This article builds upon this premise and expands it to a study of the applicability of effects through the physical network layer of cyberspace for, and in support of, influence operations.

---

[17] Pijpers and Ducheine, "Influence Operations in Cyberspace – How They Really Work."
[18] At least from the purely technical implementation point of view.
[19] Baezner and Cordey, "Influence Operations and Other Conflict Trends"; Lin and Kerr, "On Cyber-Enabled Information Warfare and Information Operations"; Max Smeets, "The Strategic Promise of Offensive Cyber Operations," 2018.
[20] Clara Assumpção, "The Problem of Cyber Attribution Between States," E-International Relations (blog), May 6, 2020, https://www.e-ir.info/2020/05/06/the-problem-of-cyber-attribution-between-states/; Florian J. Egloff, "Contested Public Attributions of Cyber Incidents and the Role of Academia," *Contemporary Security Policy* 41, no. 1 (January 2, 2020): 55–81, https://doi.org/10.1080/13523260.2019.1677324; Oliver Fitton, "Cyber Operations and Gray Zones: Challenges for NATO," *Connections* 15, no. 2 (2016): 109–19, https://www.jstor.org/stable/26326443; Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37, https://doi.org/10.1080/01402390.2014.977382.
[21] Boaz Dolev and David Siman-Tov, "Iranian Cyber Influence Operations against Israel Disguised as Ransomware Attacks," INSS Special Publication, January 27, 2022, https://www.inss.org.il/publication/cyber-iran/.

Ransomware as a Medium of Influence

Ransomware is a subset of malware designed to damage the availability of data by restricting access to it until a requested ransom amount from the attacker is satisfied.[22] Not content with simply deploying malware and hoping the victim will comply with the ransom demand,[23] the threat actors perpetrating those incidents innovated in two significant ways. One was by shifting to "locker ransomware," which renders the system non-functional by displaying a "ransom note" until the ransom is paid, thus disrupting the availability of the affected system as well and creating a messaging opportunity that is hard to ignore. The second was by moving to "double extortion" tactics where the threat actor damages the confidentiality of the victim's data by exfiltrating it before restricting access, thus creating an additional incentive for the victim to pay the ransom unless the data would be leaked to the public.[24] This evolution makes ransomware a potentially interesting tool to employ in influence operations, as the "locker ransomware" provides an opportunity to exploit the logical layer of cyberspace to inject an influence frame into the targeted information environment, while denying the target the ability to avoid the injected frame due to the disruption caused on the physical network layer of cyberspace. Finally, through their disruptive effects in cyberspace, well-designed ransomware incidents might also generate denial effects in the physical domain.[25] Due to the disruption caused on the logical and physical network layers through damaging system and data availability, and the possible denial effects through cyberspace, ransomware attacks can be considered a form of OCOs. Combining "locker ransomware" with "double

[22] Amin Kharraz et al., "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks," in *Detection of Intrusions and Malware, and Vulnerability Assessment*, ed. Magnus Almgren, Vincenzo Gulisano, and Federico Maggi, vol. 9148, Lecture Notes in Computer Science (Cham: Springer International Publishing, 2015), 3–24, https://doi.org/10.1007/978-3-319-20550-2_1.

[23] Early ransomware attacks opted to restrict access to data only, leaving the system itself functional but causing the victims to be unaware of the incident taking place until they attempted to use the ransomed data. Additionally, victims of such incidents might also have a backup of the data and resort to restoring it from the backup rather than pay the ransom.

[24] Catalin Cimpanu, "Reveton Ransomware Distributor Sentenced to Six Years in Prison in the UK," ZDNet, April 9, 2019, https://www.zdnet.com/article/reveton-ransomware-distributor-sentenced-to-six-years-in-prison-in-the-uk/; Kevin Savage, Peter Coogan, and Hon Lau, "The Evolution of Ransomware," August 6, 2015, https://its.fsu.edu/sites/g/files/imported/storage/images/information-security-and-privacy-office/the-evolution-of-ransomware.pdf.

[25] Sara Morrison, "The Chaotic and Cinematic MGM Casino Hack, Explained," Vox, September 15, 2023, https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware; Jack Beerman et al., "A Review of Colonial Pipeline Ransomware Attack," in *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, 2023, 8–15, https://doi.org/10.1109/CCGridW59191.2023.00017; Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/; Ax Sharma, "BlackCat (ALPHV) Claims Swissport Ransomware Attack, Leaks Data," BleepingComputer (blog), February 15, 2022, https://www.bleepingcomputer.com/news/security/blackcat-alphv-claims-swissport-ransomware-attack-leaks-data/.

extortion" tactics takes this even further allowing both an additional messaging channel, as well as cover, which might improve the ability to effectively exploit, what would otherwise be a classic hack-and-leak operation. Ransomware also offers an interesting case showing uncoordinated, or loosely coordinated, actors who are able to achieve effects that might amount to those of an influence operation in shifting policy priorities due to cumulative, second- and higher-order effects such as undermining citizens' trust in government services or causing a diversion of resources.[26]

Armed with an understanding of ransomware incidents as a form of OCO and an analytical framework for assessing influence operations, this article now proceeds by applying the presented analytical framework to two case studies—the July 2022 e-Albania ransomware incident and the 2022–2023 "BlackShadow" campaign against Israel.

Case Study #1: The e-Albania Ransomware Incident

On July 15th, 2022, just before the World Summit of Free Iran—an event affiliated with Mujahedeen-e-Khalq (MEK)[27] that was planned to take place at the end of July near the Albanian city of Durres—the Albanian National Agency of Information Society (AKSHI) was attacked by a threat actor calling himself "HomeLand Justice," purporting to be an Albanian group opposed to the government's support of the MEK. The incident involved the deployment of ransomware that caused disruption to the e-Albania portal, as well as multiple websites and services of the Albanian government. In a later statement the prime minster of Albania claimed that the aim of this cyberattack was to paralyze public services, erase digital systems, hack into state records, steal government intranet electronic communications, and stir chaos and insecurity in the country.[28]

To help mitigate the attack the Albanian government enlisted the support of its NATO ally—the United States—in the form of the FBI and US Cyber Command personnel who were deployed to assist with forensic investigations and perform a "hunt forward" mission in the Albanian networks, respectively. In addition, they turned to the private sector, specifically the Microsoft DART and Mandiant incident

[26] Jamie MacColl et al., "The Scourge of Ransomware: Victim Insights on Harms to Individuals, Organisations and Society," RUSI, January 2024, https://static.rusi.org/ransomware-harms-op-january-2024.pdf.
[27] People's Mujahedeen Organization of Iran is an Iranian opposition organization based in Albania, posing as a future government-in-exile.
[28] "Videomessage of Prime Minister Edi Rama," Albanian Government Council of Ministers, September 7, 2022, https://www.kryeministria.al/en/newsroom/videomesazh-i-kryeministrit-edi-rama/; Luke Jenkins et al., "ROADSWEEP Ransomware Targets the Albanian Government," Mandiant, August 4, 2022, https://www.mandiant.com/resources/blog/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against.

response teams.[29] At the center of the incident was a disruption caused by a new ransomware malware, which was used to display a political message on the encrypted systems—"Why should our taxes be spent on the benefit of DURRES terrorists?"—followed by an extensive social media campaign based on materials that were exfiltrated from the AKSHI networks prior to the disruptive phase of the attack. As a result of its investigation, Microsoft DART was able to attribute the "HomeLand Justice" threat actor to the Iranian Ministry of Intelligence and Security (MOIS), based on forensic artifacts and prior public attribution. This attribution was echoed by Albanian Prime Minister Edi Rama, who stated that "the July cyberattack was carried out by multiple hacker groups linked to the Islamic Republic. Four groups were identified, one of which was a notorious international cyber-terrorist group with a history of targeting countries like Israel or Saudi Arabia."[30.]

Following the July cyberattack, on September 7th, 2022, the Albanian government issued an unprecedentedly strong reaction by formally attributing the attack to the Iranian state. They announced the severance of all diplomatic ties with Iran and ordered the Iranian diplomatic staff in Albania to leave the country within 24 hours.[31] The Albanian response was followed by statements of support from the United Kingdom, NATO, the European Union, and the United States[32] Furthermore,

---

[29] Cyber & Infrastructure Security Agency, "Iranian State Actors Conduct Cyber Operations Against the Government of Albania," September 23, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a; Cyber National Mission Force Public Affairs, "'Committed Partners in Cyberspace': Following Cyberattack, US Conducts First Defensive Hunt Operation in Albania," U.S. Cyber Command, March 23, 2023, https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/; Jenkins et al., "ROADSWEEP Ransomware Targets the Albanian Government"; Microsoft Threat Intelligence, "Microsoft Investigates Iranian Attacks against the Albanian Government," Microsoft Security Blog, September 8, 2022, https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/.

[30] "Videomessage of Prime Minister Edi Rama."

[31] Florion Goga et al., "Albania Cuts Iran Ties over Cyberattack, U.S. Vows Further Action," Reuters, September 7, 2022, https://www.reuters.com/world/albania-cuts-iran-ties-orders-diplomats-go-after-cyber-attack-pm-says-2022-09-07/; "Videomessage of Prime Minister Edi Rama."

[32] Council of the EU, "Cyber-Attacks: Declaration by the High Representative on Behalf of the European Union Expressing Solidarity with Albania and Concern Following the July Malicious Cyber Activities" (Council of the EU, September 8, 2022), https://www.consilium.europa.eu/en/press/press-releases/2022/09/08/cyber-attacks-declaration-by-the-high-representative-on-behalf-of-the-european-union-expressing-solidarity-with-albania-and-concern-following-the-july-malicious-cyber-activities/; Foreign, Commonwealth & Development Office and The Rt Hon James Cleverly MP, "UK Condemns Iran for Reckless Cyber Attack against Albania" (GOV.UK, September 7, 2022), https://www.gov.uk/government/news/uk-condemns-iran-for-reckless-cyber-attack-against-albania; NATO, "Statement by the North Atlantic Council Concerning the Malicious Cyber Activities against Albania" (NATO, September 8, 2022), https://www.nato.int/cps/en/natohq/official_texts_207156.htm; The White House, "Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania," September 7, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/07/statement-by-nsc-spokesperson-adrienne-watson-on-irans-cyberattack-against-albania/.

the US Department of the Treasury's Office of Foreign Assets Control (OFAC) imposed sanctions on MOIS and on the Minister of Intelligence, Esmail Khatib, by freezing their assets.[33]

Analyzing this sequence of cyberattacks against Albania as an influence operation we can easily discern the following: While we cannot fully know the strategic intent of this influence operation, the chosen frames used both in the message presented by the ransomware[34] and the following social media exploitation[35] claimed to protest "government corruption" and "support of terror," with later social media frames including claims that the attack was directed against the government and not Albanian citizens. It is tempting to assume the easy proposition that the strategic goal behind the attack was to deny the MEK the political support of the Albanian government. Another thesis that one might propose is that, as the attack followed a series of attacks against Iran,[36] some of which were attributed to the MEK, the strategic goal was to retaliate as well as establish a deterrent threat coercing the Albanian government to act and limit the ability of the MEK to execute cyberattacks against Iran.[37] Finally, from the target response to the operation—to the diplomatic denouncing—it is clear that the target viewed this operation as harmful.

The Albanian government's response to the attack comprised a series of attempts to gain initiative and deter further attacks. Its initial effort was defensive and aimed to stop further attack activity inside the AKSHI networks and recover service availability. The next stage was to issue a punishment, for which Albania shortly considered invoking Article 5 of the NATO charter,[38] but it finally settled, likely after

[33] U.S. Department of the Treasury Office of Foreign Assets Control, "Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities" (U.S. Department of the Treasury, September 9, 2022), https://home.treasury.gov/news/press-releases/jy0941; A. J. Vicens, "U.S. Sanctions Iranian Ministry of Intelligence in Response to Albanian Cyberattack," CyberScoop (blog), September 9, 2022, https://cyberscoop.com/microsoft-albania-iran-cyberattack/.
[34] Jenkins et al., "Roadsweep Ransomware Targets the Albanian Government."
[35] Microsoft Threat Intelligence, "Microsoft Investigates Iranian Attacks against the Albanian Government."
[36] This thesis, as well as some following analysis, assumes that the political attribution of the attack made by Edi Rama in his "Videomessage of Prime Minister Edi Rama" to be correct.
[37] the grugq, "Albanian Cyber War," Substack newsletter, The Info Op (blog), September 7, 2022, https://grugq.substack.com/p/albanian-cyber-war; Mahmoud Hakam, "Major Cyber Attack on Tehran's Islamic Culture & Relations Organization," Iran News Update (blog), July 4, 2022, https://irannewsupdate.com/news/iranian-opposition/major-cyber-attack-on-tehrans-islamic-culture-relations-organization/; AP News, "Iran Exiles Claim Disrupting Tehran's Surveillance Cameras," AP News, June 2, 2022, https://apnews.com/article/politics-iran-middle-east-dubai-united-arab-emirates-f9b79784cba77adcf8c88dafde11ee84; A. J. Vicens, "Deep Dive into Hack against Iranian State TV Yields Wiper Malware, Other Custom Tools," CyberScoop (blog), February 18, 2022, https://cyberscoop.com/iran-state-tv-hack-predatory-sparrow-indra/.
[38] Maggie Miller, "Albania Weighed Invoking NATO's Article 5 over Iranian Cyberattack," Politico (blog), October 5, 2022, https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347.

achieving significant enough technical attribution of the originator,[39] on an exceptionally strong direct diplomatic response combined with economic sanctions applied by the US Treasury Department against the suspected attackers. The subsequent September 2022 attack by "HomeLand Justice" against the TIMS system showed that, albeit considered strong, the Albanian response was not enough to deter further attacks.

Operationally, the e-Albania incident utilized software—specifically ransomware malware—to disrupt entities and services at the physical network, logical, and virtual persona levels of cyberspace, making this incident an OCO. From the vantage point of an influence operation, during the e-Albania incident the originator exploited the logical layer for injecting their narrative frames and tried to exploit the virtual persona layer as well, albeit without any visible evidence of successful exploitation. In addition to the injection of frames, the originator exploited the logical layer to exfiltrate sensitive information—to be leaked at later stages of the influence operation—but again, at least as far as visible evidence shows, failed to exploit and capitalize on.

Case Study #2: 2020–2023 "BlackShadow" Campaign Against Israel

The focus of the second case study is a series of attacks by a self-proclaimed cybercrime group called "BlackShadow," which began in December 2020 and was ongoing as of December 2023. The first incident involving "BlackShadow" targeted the Israeli insurance company Shirbit and was not a ransomware attack but rather a hack-and-leak incident.[40] It lacked specific narrative frames and can only be considered an influence operation in the most rudimentary sense of undermining public confidence in the state and sowing chaos.[41] As the incident came to light, Shirbit representatives claimed that it was a cyberterrorism attack against Israel and not financially motivated. This claim was further corroborated by a report from an Israeli cybersecurity company, ClearSky, which was leaked by an Israeli financial magazine.[42] The ClearSky report suggested a possible connection to Iran

---

[40] Tzvi Joffre, "Government to Reconsider Using Shirbit Insurance After Large Cyberattack," *Jerusalem Post*, December 7, 2020, https://www.jpost.com/israel-news/government-to-reconsider-using-shirbit-insurance-after-large-cyberattack-651382.

[41] Brangetto and Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations"; Koval, "Revolution Hacking"; Lin and Kerr, "On Cyber-Enabled Information Warfare and Information Operations."

[42] Amitai Ziv, "Cyber Attack on Shirbit—Who Is Behind It and Why?" [in Hebrew] *TheMarker*, December 4, 2020, https://www.themarker.com/technation/2020-12-04/ty-article/.premium/0000017f-db42-df9c-a17f-ff5a9c540000?lts=1713292167615; "1.12 סקירת אירוע סייבר בחברת שירביט" (Tel Aviv, Israel: ClearSky Cyber Security, December 1, 2020), https://img.haarets.co.il/bs/0000017f-db52-d856-a37f-ffd215bd0000/cd/b5/edfbba34893bebc024fc4a688593/20201204-101626.pdf.

or OpIsrael,[43] based on the use of the corresponding hashtag in the initial "BlackShadow" social media messaging and the acquiring of what it assumed, with medium confidence, to be the malware used during the incident. Other cybersecurity companies later attributed this malware to an Iranian-nexus activity due to technical and operational similarities.[44] While the threat actor claimed the attack was financially motivated, their tactics went beyond the usual techniques employed by ransomware actors to pressure victims into paying the ransom, including directly contacting media outlets and publishing parts of the negotiation correspondence.[45] This unusual conduct led Shirbit to claim the incident as an "act of cyber-terrorism," although the Israeli state security and cybersecurity agencies had minimal involvement, limited to acknowledging the attack and publishing some revised cyber-hygiene guidelines for Israeli companies by the Israel National Cyber Directorate (INCD).[46]

Following the appearance of "BlackShadow" in the Shirbit incident, the threat actor proceeded to conduct additional hack-and-leak operations against Israeli targets, which failed to generate significant media attention. In August 2021, "BlackShadow" introduced a new tactic by utilizing ransomware against an Israeli target for the first time in an incident involving Bar-Ilan University.[47] While this attack did not receive much media attention, reports claimed the involvement of the INCD and the Israeli security services in responding to the incident. Similar to previous "BlackShadow" victims, Bar-Ilan University claimed that the incident was a cyberterrorism event and blamed Iran for it. Interestingly, while the Israeli

[43] OpIsrael is an annual coordinated cyber-attack where hacktivists attack Israeli government and even private websites with DDoS attacks and more David Shamah, "As Cyber-War Begins, Israeli Hackers Hit Back," *The Times of Israel* (blog), April 7, 2013, http://www.timesofisrael.com/as-cyber-war-begins-israeli-hackers-hit-back/.

[44] Amitai Ben Shushan Ehrlich, "From Wiper to Ransomware: The Evolution of Agrius," SentinelOne LABS, May 25, 2021, https://assets.sentinelone.com/sentinellabs22/evol-agrius; "An In-Depth Look at APT33," CyberWarCon, 2019.

[45] Dolev and Siman-Tov, "Iranian Cyber Influence Operations against Israel Disguised as Ransomware Attacks."

[46] INCD Spokesperson, "Data Breach Event at Shirbit," Israel National Cyber Directorate, December 1, 2020, https://www.gov.il/en/pages/news_shirbit.

[47] Amitai Ben Shushan Ehrlich, "New Version of Apostle Ransomware Reemerges in Targeted Attack on Higher Education," SentinelOne (blog), September 30, 2021, https://www.sentinelone.com/labs/new-version-of-apostle-ransomware-reemerges-in-targeted-attack-on-higher-education/; "Mass Data Leak after Bar Ilan University Refuses to Pay Hacker $2.5m," *Times of Israel* (blog), September 9, 2021, https://www.timesofisrael.com/liveblog_entry/mass-data-leak-after-bar-ilan-university-refuses-to-pay-hacker-2-5m/; Amitai Ziv, "Cyberattack Hits Israel's Bar Ilan University: 'Data Is Being Erased Right Now,'" *Haaretz*, August 15, 2021, https://www.haaretz.com/israel-news/tech-news/2021-08-15/ty-article/.premium/cyberattack-on-israeli-university-data-being-erased-right-now/0000017f-e396-d75c-a7ff-ff9ff65a0000; Amitai Ziv, "Does Crime Pay? A Conversation with a Hacker Targeting Israel," *Haaretz*, September 1, 2021, https://www.haaretz.com/israel-news/tech-news/2021-09-01/ty-article/.premium/does-crime-pay-a-conversation-with-a-hacker-targeting-israel/0000017f-f15d-dc28-a17f-fd7f7f3d0000.

security services remained silent about the attribution, Dolev and Siman-Tov[48] echoed this claim based on their familiarity with the response effort during the "BlackShadow" incidents. They noted that the conduct of the threat actor was not typical of a ransomware operation but included "trash-talking" the negotiators and simplistic political messaging in broken English, indicating a motive different from extorting ransomware payment.

After the Bar-Ilan University incident, the "BlackShadow" threat actor continued to target Israeli entities, such as the diamond industry in March 2022,[49] and the tech and education sectors through 2023.[50] These attacks involved wiper and ransomware operations but, again, failed to generate significant public attention. Ultimately, in October 2023, another threat actor—calling itself "Malek Team"—appeared, executing a technically successful hack-and-leak operation against the Ono Academic College, leaking multiple items of personally identifiable and sensitive information, and causing some interference with the college services.[51] Later, in December 2023, the same actor executed a hack-and-leak operation against Ziv Medical Center, again leaking a myriad of private and sensitive information, but with no evidence of disrupting the functioning of the medical center.[52] Following this incident, the INCD swiftly attributed it and the "Malek Team" threat actor to the Iranian government and specifically to the same actor as "BlackShadow." In addition, in a first, the attribution statement explains that the deviation from the regular "BlackShadow" modus operandi of disrupting their

[48] Dolev and Siman-Tov, "Iranian Cyber Influence Operations against Israel Disguised as Ransomware Attacks."
[49] Adam Burgher, "Fantasy – a New Agrius Wiper Deployed through a Supply-Chain Attack," WeLiveSecurity (blog), September 7, 2022, https://www.welivesecurity.com/2022/12/07/fantasy-new-agrius-wiper-supply-chain-attack/.
[50] Or Chechik et al., "Agonizing Serpens (Aka Agrius) Targeting the Israeli Higher Education and Tech Sectors," Unit 42 (blog), November 6, 2023, https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/; Marc Salinas Fernandez and Jiri Vinopal, "Agrius Deploys Moneybird in Targeted Attacks Against Israeli Organizations," Check Point Research (blog), May 24, 2023, https://research.checkpoint.com/2023/agrius-deploys-moneybird-in-targeted-attacks-against-israeli-organizations/; Bill Toulas, "Iranian Hackers Use New Moneybird Ransomware to Attack Israeli Orgs," BleepingComputer (blog), May 24, 2023, https://www.bleepingcomputer.com/news/security/iranian-hackers-use-new-moneybird-ransomware-to-attack-israeli-orgs/.
[51] Check Point Research, "The Iron Swords War," Check Point Blog (blog), October 18, 2023, https://blog.checkpoint.com/security/the-iron-swords-war-cyber-perspectives-from-the-first-10-days-of-the-war-in-israel/; Ryan Gallagher, "War Tests Israeli Cyber Defenses as Hack Attempts Soar," Bloomberg, October 18, 2023, https://www.bloomberg.com/news/newsletters/2023-10-18/war-tests-israeli-cyber-defenses-as-hack-attempts-soar.
[52] Daryna Antoniuk, "Iran-Linked Hackers Claim to Leak Troves of Documents from Israeli Hospital," The Record by Recorded Future (blog), December 4, 2023, https://therecord.media/ziv-hospital-israel-hackers-claim-to-leak-data; Inon Ben Shushan, "Hackers Steal IDF Patient Records from Cyberattack on Israeli Hospital," *Jerusalem Post*, December 3, 2023, https://www.jpost.com/israel-news/defense-news/article-775843; Ministry of Health Spokesperson, "Joint Announcement by Ziv Medical Center, the Ministry of Health and the Israel National Cyber Directorate," Ministry of Health, November 28, 2023, https://www.gov.il/en/pages/27112023-01.

targets by using ransomware or wiper malware in the Ziv Medical Center incident was due to interference from the Israel Security Agency[53] and the Israel Defense Forces, which also participated in the attribution.[54]

Analyzing the "BlackShadow" campaign as an influence operation shows that contrary to the "HomeLand Justice" campaign against Albania, it is harder to discern a specific narrative or strategic intent, as the chosen frames change frequently, sometimes even during the same incident. Such behavior might be in line with a strategic goal of "sowing chaos" or weakening social cohesion by creating civilian distrust in national institutions.[55] Tactically, the "BlackShadow" campaign evolved throughout its duration from a classic cyber-enabled influence operation, taking the form of a series of hack-and-leak incidents, to the deployment of OCO capabilities.

The long-lasting nature of the "BlackShadow" campaign allows for the examination of the evolution of the INCD and Israel's response efforts. Notably, in the incidents that took place from December 2020 to March 2023, the INCD chose to "update" on incidents taking place and extended support to the investigation of the incidents, while emphasizing the role of the private sector in the investigation and response effort.[56] Specifically, it left the attribution effort entirely in the hands of the private sector. This changed significantly with the incidents in October 2023, when the INCD claimed a leading role in the investigation and response to the cyber incidents that were part of the "BlackShadow" campaign, together with other Israeli national-security organizations. Moreover, the INCD chose to publicly and formally attribute those incidents to Iran and even linked the "Malek Team" persona to the "BlackShadow" campaign.[57] One might speculate that some, if not most, of the reasoning behind this change was the securitization of those incidents both by the Israeli public and the threat actor, due to the outbreak of the war

[53] Commonly known as the Shin Bet.
[54] INCD Spokesperson, "Iran and Hezbollah behind an Attempted Cyber Attack on an Israeli Hospital," Israel National Cyber Directorate, December 18, 2023, https://www.gov.il/en/pages/ziv181223.
[55] Brangetto and Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations"; Koval, "Revolution Hacking"; Lin and Kerr, "On Cyber-Enabled Information Warfare and Information Operations."
[56] Ben Zion Gad, "'Black Shadow' Hackers Leak Data from Israeli LGBT App," *Jerusalem Post*, October 31, 2021, https://www.jpost.com/israel-news/iranian-hackers-breach-israeli-company-cyberserve-683529; INCD Spokesperson, "Data Breach Event at Shirbit"; Tzvi Joffre and Tamar Uriel-Beeri, "Black Shadow Hackers Strike Again, Leak Documents in New Cyberattack," *Jerusalem Post* (blog), March 13, 2021, https://www.jpost.com/jpost-tech/israeli-car-financing-company-hacked-private-information-held-for-ransom-661865; Ziv, "Cyberattack Hits Israel's Bar Ilan University."
[57] INCD Spokesperson, "Iran and Hezbollah behind an Attempted Cyber Attack on an Israeli Hospital"; Ministry of Health Spokesperson, "Joint Announcement by Ziv Medical Center, the Ministry of Health and the Israel National Cyber Directorate"; "קבוצת התקיפה האיראנית Black Shadow," Israel National Cyber Directorate, April 9, 2024, https://www.gov.il/BlobFolder/reports/alert_1727/he/ALERT-CERT-IL-W-1727.pdf.

between Israel and Hamas in the Gaza Strip. In this regard, it is interesting to note that when reporting on the Ziv Medical Center incident, the Israeli press chose to treat it as the "fourth attack against an Israeli hospital,"[58] even though it was the first incident of its kind involving the "BlackShadow" threat actor, while the other incidents were attributed to various actors. As such, the Israeli press demonstrated an example of the cumulative effect of cyber incidents, which, moreover, was caused by loosely, if even, coordinated threat groups.

This provides another possible aspect of the reasoning behind the INCD's decision to take a leading role and formally attribute these incidents to Iran. By formally and visibly attributing those incidents to an enduring rival, it is plausible to assume that the INCD aimed to break the cumulative effect by differentiating between the previous criminal ransomware incident and this incident. In addition, it may have sought to capitalize on a possible "rally around the flag"[59] effect by signaling that the government is successfully handling the response and protecting the people when the attacker is a rival state. This also blunts the influence operation by making the Israeli public wary of the messaging from an enemy state.

Another notable choice by Israeli authorities in response to the "BlackShadow" campaign was the privacy protection regulation and the Privacy Protection Authority to limit the spread of leaked materials.[60] This potentially limits the ability to exploit the virtual persona layer for amplifying the leaks and generates resilience against attempted influence operations.

Discussion and Conclusions

This paper set out to examine whether OCOs, and especially ransomware incidents, play a role in influence operations, and the answer is likely "yes." Specifically, OCOs deny the target from easily brushing off hack-and-leak operations, thus minimizing the significance of an incident by using the coercive

[58] Ben Shushan, "Hackers Steal IDF Patient Records from Cyberattack on Israeli Hospital"; Milàn Czerny, "Start-up Nation? Israel's Cyber Defense Collapsed on October 7 and Iranian Hacker Groups Keep Attacking," Ynetnews, January 22, 2024, https://www.ynetnews.com/business/article/hjynr11jk6; Omer Kabir, "Iran and Hezbollah Were behind Cyberattack on Israeli Hospital, Says National Cyber Directorate," CTech by Calcalist, December 18, 2023, https://www.calcalistech.com/ctechnews/article/h1owft6it.

[59] Shingo Hamanaka, "The Ground Operation Sent Citizens into a Frenzy: The Rally around the Flag Effect during Operation Protective Edge," *Global Security: Health, Science and Policy* 5, no. 1 (2020): 142–52; Alan J Lambert, John P. Schott, and Laura Scherer, "Threat, Politics, and Attitudes: Toward a Greater Understanding of Rally-'round-the-Flag Effects," *Current Directions in Psychological Science* 20, no. 6 (2011): 343–48; Sharon Matzkin, Ryan Shandler, and Daphna Canetti, "The Limits of Cyberattacks in Eroding Political Trust: A Tripartite Survey Experiment," *British Journal of Politics and International Relations*, 2023, 13691481231210383.

[60] Ministry of Health Spokesperson, "Joint Announcement by Ziv Medical Center, the Ministry of Health and the Israel National Cyber Directorate."

nature of the disruption to call attention to an audience. This attention can be—and is—exploited to inject framed messages that serve the narrative and strategic intent of the OCO perpetrator. The cases examined in this article show the versatility of OCOs as an element in the wider scope of influence operations, ranging from furthering specific strategic intents to wider goals such as "sowing chaos." In both cases examined, the target of the influence operation deemed the influence attempt unwelcome, which is not surprising given the coercive nature of OCOs.

The perceived malicious intent of the influence operations analyzed can also be inferred from the significance of the attribution of the operation by both targeted nations and the strong diplomatic response in the Albanian case, which involved denouncing the Iranian state for the attack. While the instruments chosen for responding to the disruption and the influence effects differed in the two cases, both targets emphasized the importance of public-private cooperation in mitigating the disruption and restoring service availability. Additionally, both attributed the operations, with each target giving different weight to the responsibility of the national agencies, based on the strategic context and national capacity, with international cooperation acting as a complement when national capacity was lacking.

This might amount to an alternative rationale for the call to improve cyber resilience, especially vis-à-vis ransomware attacks, but further examination is needed. The unique properties of cyberspace—the ability to exploit vulnerabilities to modify cyberspace itself, the vulnerability-rich nature of cyberspace, and its susceptibility to cumulative effects—mean that restricting an adversary from a single incident or increasing the cost for them is not a viable strategy. It is believed that it is not possible to fully protect a nation against cyberattacks as long as an adversary maintains his initiative and persists in efforts to exploit vulnerabilities. Given enough time, the adversary is bound to succeed in generating enough gains to achieve a strategic level effect and "succeed" in the influence operation. The cases presented offer another approach. The Albanian case proposes a comprehensive strategy involving strong policy, cyber-defense, as well as operational and diplomatic measures to regain initiative and deter the adversary from further activity. In contrast, the Israeli case moves the resilience efforts to the virtual persona level to try to mitigate the possibility of exploiting amplification and multiplication effects, which are characteristic of this level of cyberspace and strive to make OCOs in support of influence operations less attractive.

This study makes several contributions. First, it expands our understanding of using cyberspace for influence operations by introducing OCOs, and specifically

ransomware, as a method of exploiting both the physical network and logical layers of cyberspace for influence operations. Second, it identifies an additional cyberspace vulnerability, resulting from its susceptibility to cumulative effects and the inherent challenges of attribution, which allows for an additional method of amplifying certain narratives in influence operations, potentially at lower costs than initially assumed. Finally, it explores possible policy responses to the exploitation of OCOs for influence operations and proposes that these responses enjoy cumulative effects, similar to other activities in cyberspace. Further work is needed to determine the specific design of responses that could maximize the utility against OCOs used for influence operations.

Acknowledgments

The author thanks A.C. and O.S. for their useful and thoughtful remarks during the brainstorming sessions that led to this work, albeit the planned collaboration failed to materialize due to Hamas's October 7 attack on Israel and the subsequent war that followed.

Proposed Principles for National Israeli Policy against Foreign Influence in Cyberspace and on Social Media

Amit Ashkenazi[1]

This paper proposes principles for an Israeli defense policy against foreign influence in cyberspace. In spite of the growing risks, particularly combined cyber warfare that integrates cyber attacks and influence operations, Israel has not yet formulated an overall strategy to counter foreign influence operations, that include spreading false or misleading content.

The main argument of this paper is that although dissemination of malicious and fake content through cyberspace presents a security threat, thus warranting national security attention, a purely security-oriented policy response is insufficient. Holistic policy for countering influence operations requires harnessing market oriented regulation and civilian agencies focused on content dissemination platforms. The European Union's comprehensive policies in this area, and specifically the EU Code of Conduct on Disinformation serve as a solid basis to promote policy in this area. It is suggested to promote the application of relevant EU rules that apply to content distribution in the EU, in Israel, to prevent the distribution of disinformation and misinformation. Such a holistic approach, spanning both national security activity and rules as to content distribution, was taken counter foreign influence during the national Knesset elections, and will be described to illustrate this approach.

"Foreign Influence" and "Foreign Interference" in Cyberspace and the Need for a Defensive Strategy

In recent years, and particularly during the "Swords of Iron" War, there has been a rise in malicious influence operations targeted at Israel. These operations aim to spread disinformation, and exert foreign influence via the internet and social media. While Israel has developed a comprehensive national cybersecurity strategy to protect organizations against cyberattacks essential activities,[2] it has not yet developed overall policy for dealing with "information warfare", at the content level, including "foreign influence" and the spread of disinformation.

The main argument in this paper is that although dealing with "foreign influence" is a national security challenge, in view of the features of content dissemination in cyberspace, activity of a purely security nature is not sufficient. The paper opens with a description of the existing state of play and the challenges of promoting a content focused defense policy. It then proposes ways of dealing with these challenges, based on relevant principles from European legislation. It highlights that effective national policy must be holistic, at both content and institutional levels, and combine security related activity with regulatory activity. To illustrate this approach preparations to counter foreign influence during the national elections are described. The paper ends with concrete policy recommendations.

[1] Amit Ashkenazi is a lawyer, researcher and consultant in the fields of policy, law and technology (cyber, privacy, artificial intelligence). In the years 2014-2022 he set up and managed the Legal Department of the National Cyber Directorate and was responsible for the NCD's legal policy, while in the years 2008-2014 he set up and managed the Legal Department of the Privacy Protection Authority. Amit has recently advised on the artificial intelligence policy drawn up by the Ministry of Science, and the UN CTECH venture of the United Nations. The author wishes to thank David Siman-Tov, Dr. Asaf Wiener and Dr. Gallia Lindenstrauss for their assistance and comments.

[2] "Computer attacks" in cyberspace refers to activity at the technological level whose purpose is to damage systems, including essential infrastructures, or espionage, such as information theft.

The Challenges in Tackling Foreign Influence; the Current Situation in Israel; Gaps in the Field

Cyberspace consists of a technological layer of computers and networks, and the content distributed over the. While cyberspace supports large scale global economic activity, trade, and dissemination of information, it is also an arena of hostile activities by states and non state actors. Such activities can be targeted at the technical layer, such as attacks against critical information infrastructures, or at the content layer, such as spreading disinformation and influence operations. Certain states have developed an integrated offensive approach, that includes activity at both the technological and content layers.[3]

"Foreign influence," spreading manipulative content covertly by a state in order to influence what happens in another state, is a significant threat to national sovereignty and democratic governance. Cyberspace and its many channels of content dissemination, enables conducting such activity at scale, and creating serious threats to important public interests, that include the proper functioning of government, trust in public institutions, as well as affecting governance itself. Spreading manipulative content enables influencing public opinion, affecting how people act and vote in elections, creating political or public instability, causing panic and undermining public trust in general in government. It also enables deriving advantages in the context of military conflict and influence activities of politicians, organizations and individuals. Thus these threats require state intervention to defend the public sphere, as well as national sovereignty and security from hostile activity.

At the same time, the development of any state intervention in this area faces several unique challenges:

(1) **Defining the problem in a coherent manner - the need for a uniform concept of "foreign influence" and "foreign interference".** At present there are various concepts of "foreign influence" in terms of the goals of the activity and its characteristics, but they have different elements. At the Israeli national level there is no one public definition.

(2) **The risks of state intervention in online content.** Given the importance of cyberspace for freedom of speech, free movement of information and public discourse, and state intervention, even for defensive purposes, raises concerns of unintended consequences of misuse of power. This raises a common concern in the area of government powers – what is more dangerous, hostile foreign activity or the powers used to protect citizens from that activity?

(3) **The lack of a regulatory framework in Western states to deal with dissemination of online content, unlike television and radio.** Unlike television and radio, online content dissemination platforms developed are not subject to state regulation of their content. In other words, the distribution of content on the internet requires no license and is not subject to regulatory supervision. While this structure supports innovation and development of novel content dissemination platforms, it affects the ability of states to regulate distribution of harmful or

[3] See for example: Shane Huntley, *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape*, Google Threat Analysis Group, February 2023. https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/

prohibited content. In addition, online platform are generally exempt, in many countries, for the content they distribute[4], unlike the rules that apply to non-cyberspace content distributors.[5]

(4) **Online content distribution rules are largely defined and enforced by the platforms themselves.** The lack of a regulatory regime and the limited liability, enables the platforms to define content distribution policies in their contracts with their users, such as "terms and conditions", "acceptable use policy", "advertising rules", etc. These contracts define permitted and prohibited content, based on the platforms' business model, which does not necessarily align with national or international legal definitions.

(5) **The online ecosystem has many distribution channels and almost no supervision.** In the permissive legal environment described above, a rich ecosystem of information distribution has developed. This ecosystem is based on a wide variety of interactions between users, speakers and addressees based on algorithms with very little legal or regulatory supervision. These interactions include paid advertising, and various user supported distribution mechanisms, such as the ability to share content, add hashtags, endorse content and more. These algorithm-user distribution mechanisms are calibrated according to the interests of the platforms—to increase views and user attention. In this sense platforms face a constant tension between encouraging user interaction and content distribution, and ethical considerations relating to some types of popular but problematic or even illegal content. The operation of these complex mechanisms, and the tradeoff between more content distribution, safety and unethical content, is generally not public.

(6) **The limited ability of a specific jurisdiction to affect online content distribution and global platforms.** Content that is published online is instantly distributed globally, thus challenging the ability of one jurisdiction to take effective legal measures. When large platforms are involved, the challenge is that these are multinational corporations whose policies on content are in general not affected by Israeli law or the Israeli user market. Thus under the present legal regime, any influence on platform policies is largely dependent on voluntary cooperation between them and state authorities or civil society. As a result, it appears that any attempts to develop domestic legal interventions may be futile. This is disconcerting because of the central role of these platforms in the dissemination of information to the general public. There is a gap between the size and scope of the information ecosystem in cyberspace, the economic incentives applying to it, and its central role in public discourse on the one hand, and the available effective legal tools to protect public interests on the other hand.[6] While platforms continually engage in removing content that is against their policies, these policies are designed to promote platform interests, high amongst them more user interaction.

[4] In brief, in 1996, Section 230 of the Communications Decency Act in the United States defined a very broad exemption for intermediaries that distribute content produced by others, from any obligation for such content. Eric Goldman, "The Ten Most Important Section 230 Rulings," *Tulane Journal of Technology & Intellectual Property*, Vol. 20, 2017, Santa Clara Univ. Legal Studies Research Paper, Available at SSRN: https://ssrn.com/abstract=3025943.

[5] The main reason given for these arrangements is the wish to allow free movement of information, and the claim that platforms are not realistically able to monitor such huge quantities of data. As a result, imposing the obligation of monitoring or checking content will lead to a situation of "censorship." On this matter see: Shocken v. The Hebrew University, Roter, Survey of Supplier's Liability. [more publication info needed. Not in the Hebrew version] See also: Niva Elkin Koren. "The New Brokers in the Virtual Town Square." *Mishpat U'Memshal* 6 (2), 2003 [Hebrew]. And The Davidi Committee, "Summary of the Committee's Work on Adapting the Law to the Challenges of Innovation and Technological Acceleration, on the Subject of Illegal Content in the Digital Space. https://www.gov.il/he/Departments/Guides/davidi-committee-main?chapterIndex=12.

[6] Professor Niva Elkin Koren already identified this in 2004, in her article *The New Brokers in the Virtual Town Square*.

Israel's existing partial approach to influence operations and dissemination of harmful content is a result of this complexity. While security and law enforcement organizations work to provide protection in cyberspace, including taking action against harmful content of various types, there is no overall strategy or policy.

First, the Israeli government has not published an agreed definition or common terminology to define foreign influence activities in cyberspace, and has not tasked a lead organization to deal with it. While the General Security Services, the State Attorney, and the National Cyber Directorate are active in dealing with certain aspects of influence operations, there is no overarching policy, and a lead organization to synchronize efforts. This is in contrast to the Israeli national cybersecurity strategy which set up a dedicated agency and comprehensive policy for national readiness against cyber attacks.[7]

Second, state agencies have very limited powers to act against illegal content on online platforms. These powers focus mainly on the blocking or removal of harmful content from local internet service providers.[8] With respect to online platforms, such as social media, state agencies can only inform the platforms about content that violates platform policy, but at present can not mandate blocking or removal of such content.

Third, most of the state agencies legal activity is directed at content that incites violence.[9] While important to prevent further incitement and escalation, it does not deal comprehensively with content that is disguised as legitimate discourse, which is part of foreign influence attempts.

This incomprehensive and partial operational and legal activity situation is reflected in the Israeli Supreme Court ruling in the Adalah human rights organization petition against government content takedown notices.

In the petition Adalah claimed that the State Attorney's procedure to notify platforms of content that is illegal according to Israeli law, requires specific authority in law. This is because such notifications lead to taking down of content, which infringes upon freedom of speech, thus requiring a specific legal basis for state activity.

In response, the government described its notification procedures, which is aimed at an alternative enforcement procedure to deal with criminal offenses related to the publication and distribution of illegal content. The government explained that such notices are only sent after the State Attorney Cyber department has examined the content, and determined that its publication amounts to a criminal offense under Israeli law.[10] While the usual next step is prosecuting the publisher, this is not feasible in publications over the internet. Thus the State Attorney has developed a procedure

[7] See: Government Resolution 3611 of August 7, 2011, "Promoting national capability in cyberspace." https://www.gov.il/he/departments/policies/2011_des3611; Government Resolution 2444 of February 15, 2015: "Promoting national preparations for cyber defense." https://www.gov.il/he/departments/policies/2015_des2444; Government Resolution 2443 of February 15, 2015: "Promoting national regulation and government leadership in cyber defense." https://www.gov.il/he/departments/policies/2015_des2443; Government Resolution 219 of August 1, 2019, "An examination of smart regulation in cyberspace and rules and powers to give instructions during a cyber-attack at its height taking account of economic considerations." https://www.gov.il/he/departments/policies/dec219_2021; Law of Security Regulation in Public Bodies, 5758-1998; Law of Dealing with Serious Cyber Attacks in the Digital Services and Digital Storage Sectors (Emergency Regulation – Iron Swords), 5784-2023.

[8] See: Law on Powers to Prevent the Commission of Offenses Through an Internet Site, 5777-2017.

[9] See the report of the Internet Association for Cyber Activity in the State Attorney's Office. *The Activity of the Cyber Department of the State Attorney to Remove Content from Social Media, Trends and in Depth Statistics* (October 2023). https://www.isoc.org.il/regulating-digital-services/israel/voluntary-content-removal-trends.

[10] The usual response of the law enforcement authorities is to put the speaker on trial, but because of the features of the discourse on the internet it is not possible to file an indictment against the speaker, who is either unknown or located in another country.

to notify the platform about the illegal content, in order to prevent further exposure to the content, and to limit its influence and harm. The government stressed in its response that it asks the platforms to remove the content only if the content is also in breach of the platform's own terms of use.[11] According to the government position, the State merely "notifies" the platform that it is hosting content that breaches its terms of use. In other words, the State does not use compulsory powers but acts in accordance with the platform's terms of use.

This position highlights the problems with the current legal framework. Even in cases where the State Attorney department believes that certain content violates Israeli law, they must prove to the platforms that this content is also in breach of the platforms' terms of use, which are not part of national law but are a legal arrangement defined by a private company.

The Supreme Court rejected the petition, and accepted the government position that voluntary notification is non binding on the platforms. As part of the ruling, the court pointed out that when illegal content is distributed by virtual "bots", freedom of speech is not implicated.

The ruling recognizes that in order to protect freedom of speech in cyberspace and to protect authentic public discourse, the State must take protective action, using a variety of tools.

The ruling also recognizes the important role of platform terms of use, and even their unique legal status, in moderating content. Judge Melzer illustrated this with a diagram based on Prof. Jack Balkin's "Pluralist Model of Speech Regulation". [12]

Following Proffesor Balkin, Judge Meltzer highlights that tradtional content distribution is subject to state regualtion, online content distribution is subject to "private governance". Private governance includes the technologies and legal policies regarding user behaviour and distribution of content which are drafted and enforced by the platforms themselves.

Thus in the Adalah case, the Supreme Court recognized *de facto* binding legal status of this "private governance."[13] The practical implication, is that in cases of illegal content, the position of the State Attorney according to domestic law, in effect is subject to "private governance" determined by the platforms. This reflects powerful protection of freedom of expression on the platforms, but raise challenges when the state wishes to protect the public interest in cyberspace, and sees the public interest in a way which is different than the platform.

[11] During 2023, a similar debate took place in the USA, in which a district court received a similar petition against the State, seeking to prevent it from notifying alleged breaches to the social networks' policies. The American Supreme Court delayed implementation of the order until October 20, 2023. Without going into all the differences between the procedures, it is interesting to note the variety of governmental bodies that are in contact with the platforms on this subject. In Israel, on the other hand, there is a centralized approach whereby, on this sensitive subject, there is a single point of contact with the platforms, and this apparently has significant advantages. Amy Howe, "Justices Allow Federal Government Continued Communication Over Social Media Content Moderation," *SCOTUSblog*, October 20, 2023. https://www.scotusblog.com/2023/10/justices-allow-federal-government-continued-communication-over-social-media-content-moderation/.

[12] Balkin, Jack M., Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation (September 9, 2017). UC Davis Law Review, (2018 Forthcoming), Yale Law School, Public Law Research Paper No. 615, Available at SSRN: https://ssrn.com/abstract=3038939 or http://dx.doi.org/10.2139/ssrn.3038939
Balkin, Jack M., Free Speech is a Triangle (May 28, 2018). Columbia Law Review, 2018, Forthcoming, Yale Law School, Public Law Research Paper No. 640, Available at SSRN: https://ssrn.com/abstract=3186205

[13] Although in other contexts the Supreme Court has expressed criticism of the legal contractual framework that regulates the actions of the platforms. For example, Class Action 46065-09-14 Ben Hamo v Facebook (External file Civil Appeal 5860/16). Decision of July 5, 2023. Civil Appeal 1901/20 Troim Miller Ltd. v. Facebook Ireland.

During 2017-2018 the government promoted a bill to enable Israeli courts to require platforms to take down or block illegal content.[14] The bill defined the conditions for for removing content and the removal process. The bill did not directly define "foreign influence" or "misinformation," but the bill did reffer to the national security implications of distributing illegal content.[15] The bill was not approved. It should be pointed out that the bill focused only on the removal of content ex post. The bill did not address at all platform capabilities or obligations to identify or deal with harmful content in advance. Thus the policy promoted by the bill left these issues to the platforms' "private governance".

To summarize, the current legal situation in Israel is lacking with regard to effective tools to deal with foreign influence , because it relies on voluntary cooperation with the platforms, according to their terms of use. Moreover, the government sponsored bill to take down illegal content only focused on ex post enforcement, thus not adderessing the active role of platforms in distributing content. Thus even if the bill was approved it would not have provided an adequate tool to deal with influnce operations. While the Attorney General's department is investing many efforts, from a practical point of view, the ability to monitor and take down content ex post is not effective enough given the speed and quantity of content distribution on platforms.

Developing policy to deal with foreign influence and disinformation

Given the rising challenges and threats, a lead agency should be tasked with developing a comprehensive policy to mitigate foreign influence and dissemination of disinformation. Developing a clear and uniform policy will improve preparadenss. In addtion, formulating clear policy in this area is important to develop the neccesary legal frameworks. Ariculating government powers in this area enables ensuring that such powers do not create unnessecary risks to fundamental rights .

The need for holistic policy to counter online "foreign influence," "foreign interference," and disinformation

This part will elaborate the need for a holistic policy, combining strategic-security and legal-technological viewpoints to effectively address "foreign influence," "foreign interference," and disinformation.

The strategic viewpoint examines "foreign influence" as part of the adversary's goals, measures and tools in general. The techno-legal viewpoint examines the arena in which the activity takes place and the unique features of online content production and distribution. The combination of these two viewpoints examines how adversaries conduct foreign influence operations, and the available and necessary tools to deal with them. Clarifying these issues enables designing appropriate legal tools that balance security needs with the risk of excessive state intervention in content.

[14] Proposed Government Law: Bill to Remove Internet Content Whose Publication Constitutes an Offense, 5777-2016, Government Bill 1104, December 28,2016.
https://main.knesset.gov.il/activity/legislation/laws/pages/lawbill.aspx?t=lawsuggestionssearch&lawitemid=2011567.

[15] In the version prepared for the Second and Third Reading, the following clause was proposed: "A District Court Judge, duly authorized by the President of the District Court may, at the State Attorney's request, issue an order obliging the publisher of content, or the owner, manager or operator of an internet site on which content is published, to remove the content from the internet site, if he is persuaded that publication of the content on the internet site constitutes a criminal offense, and that in the circumstances there is a real possibility that its continued publication will harm the safety of a specific or non-specific person or state security, or cause serious harm to the national economy and essential infrastructures, in this Law – an order to remove content." It may be assumed that the distribution of content by a hostile foreign element for influencing purposes, will meet these conditions.

The security-strategic viewpoint: definitions and a shared taxonomy for threats of foreign influence and foreign intervention

The starting point is the need to have common understandings of the problem and its features. This is why a clear definition of "foreign influence" is important. It is also required to ensure that all the relevant entities are using the same language to conceptualize the threat and shape suitable responses.

Ofer Fridman explains that "foreign influence" should be seen as part of the toolset used by an international player to influence another international player in the international arena. Fridman thus defines "foreign influence" as the "use of all available sources of national power (diplomatic, informational, military, economic, religious and so on) by an international player to influence another player, in order to achieve a political objective." Fridman goes on to define "foreign interference" as a specific type of foreign influence.[16] According to this approach, "foreign influence" is deemed "foreign interference" when the use by one player of national power to influence another player is seen by the second player to be contrary to its values, norms or laws.

The broader view of "foreign interference" proposed by Fridman helps frame online operations within the bigger picture. This includes assessing the overall objectives of adversaries, and accordingly assessing the means used in their activity in cyberspace. In other words, the way in which an enemy seeks to use foreign influence in cyberspace must be examined through the broader prism of its aims and the tools at its disposal. For example, if one country wishes to achieve influence on the economic activity of another country (for example, by investing in strategic economic areas), it can be assumed that it will also make use of cyberspace to spread messages that support these activities, or criticize competing activities.

Thus, the strategic viewpoint highlights the importance of an integrated national approach to deal with adversary operations in cyberspace. It is important to have coherent and consistent concepts that are shared by the whole system, and involves all relevant intelligence organizations. Integration also facilitates effective preparation to identify and counter influence operations.

Finally, the government needs to be able to require taking down or blocking of illegal content, not only on a voluntary basis. Therefor legislation to grant the security services the proper authority, through the State Attorney, to demand removal of content, should be promoted. The legislation should include authority to require removal of disinformation.

The need for a holistic approach—the interface between security and regulation

As described above, dealing with harmful content only ex post does not deal effectively with the massive amount of content spread online. There is a significant difference in the quantity of content identified and removed by the platforms themselves, according to their own policies, and the far fewer requests for removal submitted by the State. In order to have a real impact on content dissemination, it is vital to influence "private governance", affecting the actions taken by platforms to identify malicious activity and take preventive action. This is critical for the protection of the online arena and, ultimately, the ability to exercise freedom of expression in the online arena. In order to tackle influence operations and disinformation, the state needs to be more active in the way that platforms deal with content in general. An additional legal tier, focused on platform activities ex ante, is needed to complement the legal tier focused on taking down content ex post.

[16] Ofer Fridman, "Defining Foreign Influence and Interference," Special Publication, January 2, 2024, Institute for National Security Studies and the Institute for the Study of Intelligence Methodology. https://www.inss.org.il/publication/influence-and-interference/

Yet security agencies are not the adequate institutions for this type of activity.[17] Security agencies generally operate in a clandestine manner, they are not experts in regulating private sector companies, and they may be in conflicts of interest regarding other missions they may have. This highlights the need for a holistic policy, **in which security activity against the adversary** is complemented by civilian regulation directed **at the arena in which it** operates.

D. The civilian tier - Dealing with Foreign Influence through Accountability of Platforms in Israel

(1) Promoting accountability of platforms in Israel based on applying EU rules

The previous chapter claimed that effectively dealing with influence operations and disinformation requires taking action ex ante, and not just ex post. Thus a second regulatory legal tier is necessary to complement the security oriented legal tier. While the regulation of content on social networks is broader than the current context of foreign influence, as described above, it is essential in order to enable the effective implementation of a strategy to protect against foreign influence.

This approach also aligns with previous Israeli Ministry of Communications public committee report in 2022 that there is a **need for a fundamental change in public policy regarding content distribution on online platforms.** [18] This position highlights that experience has shown that leaving content distribution policy to the exclusive discretion of the platforms does not necessarily promote freedom of speech, or balance freedom of speech with other values in a publicly accepted manner. The committee report discusses the EU Digital Services Act and how to address the unique challenges of distributing content on the various platforms.[19] The report proposes to impose risk management duties on platforms so that they mitigate misuse of the platform, such as distribution of fake or offensive content.

The Ministry of Communications report recommendations support the conclusion that in order to effectively protect against foreign influence, it is necessary to create a civilian regulatory tier that applies to the governance of content on platforms. This tier will complement the activity of the State Attorney's Office activities in removing content.

Indeed, extreme caution is required for any government activity in this area. However, given the rising threat of foreign influence, such platform governance obligations become more important. In addition, it is important to make platform "private governance" more accountable and transparent. This can support preventing dissemination of harmful content, as well as to locate such content.

It is proposed to develop this civilian layer carefully by following one of the key elements of the EU DSA, the principle of risk management, and more specifically the Code of Practice on

[17] See, for example, the Supreme Court's statement regarding the authorization of the Shin Bet to assist in locating coronavirus patients, HCJ 2109/20, Shahar Ben Meir et al. v. Prime Minister.
[18] Ministry of Communications, *Report of the Advisory Committee to the Minister of Communications to Examine the Regulation of Digital Content Platforms,* December 14, 2022, https://www.gov.il/he/Departments/publications/reports/14122022.
[19] European Commission, The digital services act package, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

Disinformation.[20] The Code was formulated in a lengthy process with the platforms voluntarily, and now applies to Very Large Online Platforms. The importance of the Code is not just in its content, but also because of the process through which it was developed. It was not unilaterally dictated by the legislature, but was developed with the platforms, taking into account the unique characteristics of their activity.

The Code covers the main platform activities in distribution of online content, and provides a common basis for the creation of platform obligations. In other words, it describes in legal language the various methods in which content is disseminated by the platforms. The Code sets a series of requirements that respect platform discretion in the distribution of content, but requires accountability on the part of the platforms in order to reduce risk.

The Code also imposes transparency obligations aimed to shed light on platform "private governance". The Code aims to empower users, the research community, and the "fact-checkers" community to support freedom of expression while minimizing external interference in content. At the same time, the Code includes measures to enforce commitments through a transparency center, a permanent task force, and enforcement of the Code.[21] To sum, the Code lays the groundwork for affecting platform private content governance. The Code does so in a way which takes into account the unique features of the online space.

The Code can serve to develop the regulatory tier in Israel to help deal with foreign influence and false information. It is a detailed arrangement that has been formulated for many years with the large platforms, it reflects their accepted rules of conduct. Therefore, it is proposed to promote the application in Israel of an EU style obligation to manage risks, on platforms that have been designated as "very large online platforms." [22] and by referencing the Code. In practice this means the application of these specific duties that such platforms have in the EU, to the Israeli ecosystem. It should be clarified that this proposal does not cover all of the EU DSA, but just the obligation to manage risks against misuse.

Relying on the EU scheme has several advantages. The first advantage is that the scheme serves as a policy blueprint and thus a "shortcut" to develop a common policy discourse on distribution of content on platforms. The second advantage is that this approach is by definition interoperable with emerging global rules. A third advantage is that the adoption of the EU scheme, serves as a global "guardrails" against the risk of the development of an unbalanced domestic policy, that does not adequately protect freedom of speech.

(2) Promoting accountability of platforms in Israel based on applying EU rules – institutional aspects

[20] European Commision, The 2022 code of practice on disinformation, https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.
[21] Periodic publication of activity in accordance with the code: https://disinfocode.eu/reports-archive/?years=2023.
[22] European Commission, Digital services act: Commission designates first set of very large online platforms and search engines, 25.04.23, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413.

The previous sections described the need for a civilian regulatory tier, and pointed out to the EU Code as a normative baseline. The next question is defining the public institution tasked with promoting the application of these obligations. In other words, in order to promote risk management and dealing with false content, it seems that a mechanism should be established for the purpose of maintaining a dialogue, including some sort of oversight, with the platforms in order to ensure that these obligations are properly implemented in Israel.

As described above, the security establishment is not the natural candidate for this role. To complicate the issue further, there is currently no single regulatory authority for the internet. The Ministry of Communications committee proposed to assign this role to a newly established independent media authority. A comprehensive study by the Israel Democracy Institute focused on the importance of platform responsiveness to user requests, and thus proposed assigning oversight of platforms to the Consumer Protection Authority, at the Ministry of Economy.

Due to the uniqueness of this domain, and challenges in Israeli regulation of online activities, the present proposal suggests taking a gradual hybrid approach, that harnesses civil society and existing regulatory agencies. Under this approach, policy should create incentives **for the adoption of the Code described above**, and strengthen the existing public discourse and on monitoring of these obligations by civil society organizations, primarily the Israel Internet Association.[23] Thus the proposal is to "nudge" platforms to compliance through civil society dialog, while tasking relevant regulatory agencies to apply their powers to support these efforts. This hybrid approach will be unpacked in the following paragraphs.

The first part of the proposed approach is based on the role, experience and legitimacy of the Israel Internet Association. The IIA is an independent non-profit organization that manages the ".il" top level domain, with experience and reputation in the online arena in Israel. The IIA promotes the proper and safe functioning of the Internet for all its users, and thus has the legitimacy and the professional knowledge to facilitate the development of platform content related obligations. It is proposed that the IIA will lead civil society efforts to encourage platforms operating in Israel **to voluntarily apply in Israel their obligations under the Disinformation Code of Conduct, and specifically risk management obligations.** A possible result of such a move is a voluntary commitment by the platforms to proactively locate and prevent infringing content, regardless of the request by the security agencies, retroactively. This move is expected to have a positive impact on the content arena in cyberspace, and thus on the prevention of content aimed at foreign influence.

The second part of the proposed approach aims to utilize existing regulatory authorities to oversee the proper application of these norms in Israel. While there is no single agency tasked with regulation of online activities, three regulatory agencies have authorities that can be applied to online activity and specifically platforms.

[23] See: https://en.isoc.org.il/, and specifically https://en.isoc.org.il/the-internet-safety-hotline, and https://en.isoc.org.il/about/news-room/october-2023.

These agencies are the Privacy Protection Authority, the Consumer Protection Authority and the Competition Authority. The Privacy Protection Authority is Israel's data protection authority, overseeing collection and processing of personally identifiable information (PII). Processing of PII is a central activity of the platforms, in order to develop user profiles sell targeted advertising services. The Consumer Protection Authority is in charge of consumer protection, including online. The Consumer Protection Authority deals with consumer disclosure obligations, which are important to users. The Competition Authority deals with companies that have market power, and is relevant because of the market power of online platforms, which raises concerns that their content policies are used in an anti competitive manner. Each of these agencies relates to a different segment of the platforms' activity, and the integration of knowledge and regulatory tools can properly deal with the challenge they pose. This approach builds upon existing collaborations in the online space by these three agencies. [24] This model of cooperation has precedent in the United Kingdom as well. [25] Finally, each of these agencies has a certain degree of regulatory independence from government ministries, and has competence with respect to only a certain segment of the field of activity. This structure reduces the risk of disproportionate state interference in online content. By coordinating efforts this group could promote the adherence of platforms to the norms described above. This approach also enables immediate policy deployment, on the basis of existing legislation.

To integrate between security efforts and regulatory efforts, this team needs to develop working relationships with the security and intelligence agencies and the National Cyber Directorate. Such relationships have been developed in the context of cybersecurity, and enable sharing information about hostile activities.

(3) Platform Users - Promoting Digital Literacy– Training and Awareness Raising

One of the challenges in dealing with foreign influence operations is that some legitimate actors in the domestic political arena may use questionable techniques to influence the public to support their positions. Political parties, politicians or public activists that spread disinformation, create legal and operational complexity. Therefore, it is necessary to educate these actors on the implications of such activity, in order to reduce the risk that their activities will increase exposure to foreign influence. An example of this is the voluntary code of conduct regarding the use of digital advertising in an election campaign developed by the Israel Democracy Institute.

Additional measures include training and increasing awareness of users, speakers, and distributors of content about the way platforms distribute content. In this context, the availability of information about how the platforms operate and distribute content, is important. Such information also enables civil

[24] The Ministry of Justice, the Privacy Protection Authority, the *Privacy Protection Authority, the Competition Authority and the Consumer Protection and Fair Trade Authority recommend adopting the right to data portability in Israeli law*, 03.01.2021, https://www.gov.il/he/departments/news/data_portability.

[25] UK information commissioner's office, ICO and CMA set out blueprint for cooperation in digital markets, 19.05.2021, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2021/05/ico-and-cma-set-out-blueprint-for-cooperation-in-digital-markets/.

society organizations to promote public discussions about these issues, also promoting platform accountability.

Finally, the state has various tools to develop user digital literacy and awareness to disinformation, directly in the education system or in cooperation with civil society organizations. Digital literacy and awareness is mentioned last due to the because of the assumption that "educating" users and consumers will be more effective only after addressing the strong forces shaping the online arena.

In general, it seems that digital literacy, which includes both ethics in the use of social networks and a broader understanding of the ecosystem, should be integrated in the education system. The Ministry of Education has dealt with these issues, but it seems that there is room for broader engagement, including designated training programs. Due to the central role of cyberspace in modern life, it is important to deal with these skills in a systematic pedagogical approach. Civil society, such as the Israel Internet Association, as well as industry, can serve as a testing ground for developing effective training content and methods. Finally, the older population, which is part of the electorate, should also be approached. Studies have shown that older population are also vulnerable to false information online. It is important to develop a wide range of tools that will suit different sectors of the population.[26]

Exploring the holistic approach –Dealing with "Foreign Influence" in Elections

This part will explore the different elements of the holistic approach described above through the case study of dealing with the risk of foreign influence in elections.

The main pivot for the holistic approach is the Central Elections Committee, which is an independent institution headed by a presiding Supreme Court judge. The Central Elections Committee is tasked with managing the election process, and protecting, among other things, the "integrity of the elections."

The Central Elections Committee decided to deal with foreign influence following publications about state sponsored influence operations aimed at interfering in the presidential elections in the United States[27] and Europe. [28] As described above, opponents use foreign influence on an ongoing basis and in a variety of contexts, but there is a special sensitivity in this activity in the run-up to an election campaign, due to the attempt to influence voters and public opinion. This lead the Central Elections

[26] See, for example: Alice Huguet, Julia H. Kaufman, Melissa Kay Diliberti, Social media posts have power, and so do you stop the spread of false and misleading information during voting season, RAND Corporation, 2024, https://doi.org/10.7249/TLA2909-1.
[27] See, for example: U.S. Department of Justice, Special Counsel Robert S. Mueller, III, Report on the investigation into Russian interference in the 2016 presidential election, Volume I, March 2019, https://www.justice.gov/storage/report.pdf.
[28] Eric Brattberg & Tim Maurer, Russian election interreference, Europe's counter to fake news and cyber attacks, May 2018, https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435.

Committee to develop its activities to deal with the risk of foreign interference in election campaigns in Israel.[29]

The Central Elections Committee developed a holistic approach, which included cooperation between security agencies and civilian agencies. The approach deals both with threats in the technological field[30] and risks of interference through influence operations.

On the organizational level, the committee convened intelligence, security, law enforcement, cyber defense, regulation, and the State Attorney's Office for discussions on preparedness and coordination. These discussions strengthened cooperation networks and knowledge sharing before and during the elections.

In this context, it should be noted that the National Cyber Directorate, which is responsible for cyber defense, i.e., the prevention of computer attacks and information theft, acted to assist the Central Elections Committee in protecting the integrity of the election process in terms of cyber security.

Like other national cybersecurity authorities, the INCD does not deal with online content, and therefore the INCD did not deal directly with aspects related to influence operations. The INCD acted under a specific mandate developed under the authority of the Central Elections Committee. According to this mandate, the Central Elections Committee and its authorized representatives take all decisions on matters of principle or substance, while the INCD acts as a national technical and operational expert assistant. The INCD also set up the coordination mechanisms between relevant agencies, that included all the authorized representatives from among the security and enforcement agencies, including representatives of the Cyber Department in the State Attorney's Office, thus supporting a comprehensive management approach for the Chair of the Elections Committee.

The importance of rules that apply to platform content distribution mechanisms is exemplified by the Chair of the Central Elections Committee (a presiding Supreme Court Justice) ruling on the need to identify political advertising. The Chair of the Central Elections Committee has broad powers to protect election integrity, and under these unique powers he decided to require that advertisements on behalf of political parties on online platforms will disclose their source.[31] The Chair of the Central Elections Committee, Justice Melcer clarified that the purpose of this decision is to prevent the ability of adversaries to disguise their content within legitimate political discourse. It is interesting to note that a previous attempt to legislate this type of rule was opposed by some political parties. The decision is important in that it establishes a rule that is intended to deal directly with foreign influence. No less important, the decision is also directed at the platforms, and states that if a platform does not take measures to identify the advertiser of a political ad, it will also be considered responsible for the

[29]See, for example, Foreign Influence on the Content of Political Discourse: A New Strategic Challenge, *INSS Insight No. 1129*, January 14, 2019, https://www.inss.org.il/he/publication/foreign-influence-on-political-discourse-a-new-strategic-challenge/.

[30]For an overview of the activities of the Elections Committee on this issue, see: State Comptroller, *Annual Report 2022*, Information Systems and Cyber Protection in the Elections for the 21st, 22nd and 23rd Knessets - Information Systems Auditing, 09.03.2022 https://www.mevaker.gov.il/sites/DigitalLibrary/Pages/Reports/7413-23.aspx

.

[31]Central Elections Committee for the 21st Knesset, 8/21 Shachar Ben Meir v. Likud Party et al., http://bit.ly/489jMz1.

infringement. This ruling demonstrates the connection between security goals and a proportionate regulatory legal toolkit.

Conclusion

The departing point of the article is that a new and integrated conceptualization of the phenomenon of foreign influence in cyberspace is required. Dealing with foreign influence in cyberspace requires a combination of two main perspectives – a strategic-security perspective and a techno-legal perspective. The strategic perspective examines "foreign influence" in the cyber arena as part of the goals, means and tools of **the adversary** in the field of foreign influence in general. The techno-legal perspective examines **the arena of operation**, cyberspace, and the unique characteristics of the production, distribution, and regulation of content in the cyber arena, and accordingly the prevention of the distribution of harmful content therein. The combination of these perspectives makes it possible to define how foreign influence is expressed in cyberspace, what tools exist and are required to deal with it.

Effectively dealing with content identified as part of foreign interference requires a balanced approach including the establishment of explicit proportional authority, to instruct platforms to remove or block such content. Such ex post measures need to be complemented with ex ante measures targeted at content distribution. Thus from a practical point of view, it is necessary to increase the level of accountability and risk management of the platforms, in accordance with the arrangements they have agreed to around the world. This activity should be carried out in the public sphere, between civil society and civil authorities, and the platforms, and not through the security agencies.

A strategic approach that connects the activities of the security agencies with civil society makes it possible to adapt the state's defense efforts to the unique features of the online environment. The implementation of a unified strategy that connects the security and civilian dimensions, and that creates orderly and transparent interfaces to the platforms, will support a more effective approach to this challenge.

The following policy principles are proposed:

1. A central security organization should be entrusted with developing national strategy for dealing with "foreign influence" in a manner that takes into account its hybrid characteristics. This strategy needs to lay out a plan for national preparedness, including agreed definitions of "foreign influence", and interfaces between the security establishment, which aims to deal with adversaries, and the civilian system.
2. In order to prevent the phenomenon of "camouflaging" foreign influence within the internal discourse, it is necessary to bring about more responsibility for the use of content distribution platforms by politicians and other public figures.
3. Legal arrangements to deal with influence operations should be promoted, as detailed below:
    1. Approving legislation that enables courts to require online platforms to block or delete content

i. The current legal framework only enables state authorities to notify platforms about illegal content, and is subject to platform policies. Therefore a law that enables state authorities to request judicial approval to block or delete illegal content is needed.

2. Increasing online platform accountability for content distribution
    i. Adding EU style Risk Management Obligations for Very Large Online Platforms
        1. It is proposed to base the regulatory tier on the rules developed in the EU, under which a content distribution platform is required to establish a risk management policy against misuse of its platform. More specifically it is proposed to promote the application of the EU Code of Conduct on Disinformation in Israel.
        2. The advantage of this approach is that it reflects an accepted arrangement in countries around the world, and reduces the risk of disproportionate government intervention in regulating content.
        3. It should be emphasized that the adoption of the Code is only a starting point, and not a complete solution.
    ii. Oversight of risk management by platforms
        1. It is proposed to promote voluntary oversight of these obligations though civil society, lead by the Israel Internet Association.
        2. At the same time, it is proposed to develop an integrated regulatory collaboration to oversee platform activity, that includes the Privacy Protection Authority, the Consumer Protection Authority, and the Competition Authority. Each of these authorities has regulatory powers that are relevant to promote platform accountability in this area.
        3. The security establishment should collaborate with these civilian agencies in areas that are relevant to mitigating influence operations.
4. Efforts to educate the general public about the dangers of false information, and in particular the manner in which its dissemination or use may also serve a state adversary, must be increased.
5. A permanent public-private partnership to promote digital literacy should be established to synchronize efforts by civil society and the state in this area.

Israel Ministry of Science & Technology

ISRAEL INTELLIGENCE HERITAGE & COMMEMORATION CENTER (IICC)

THE INSTITUTE FOR THE RESEARCH OF THE METHODOLOGY OF INTELLIGENCE

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב