The Cognitive Campaign:
Strategic and Intelligence Perspectives

Yossi Kuperwasser and David Siman-Tov, Editors

Memorandum
197

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

Intelligence in Theory and in Practice
Issue No. 4, October 2019

The Institute for the Research of the Methodology of Intelligence

The Cognitive Campaign: Strategic and Intelligence Perspectives

Yossi Kuperwasser and David Siman-Tov, Editors

Institute for National Security Studies

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

The Institute for the Research of the Methodology of Intelligence (IRMI) at the Israeli Intelligence Community Commemoration and Heritage Center was established in 2016. Its goal is to serve as a space for developing and discussing intelligence methodologies for the Israeli Intelligence Community and to help connect it to the relevant methodological discourse in other intelligence communities, in academia, and in the private and public sectors.

IRMI research and other activities are based primarily on the vast experience of practitioners, those who are active within the Israeli Intelligence Community and its veterans, as well as on professional research in academia and research centers worldwide.

In IRMI's view, methodology is a critical component of the intelligence practicum, and the convergence between theory and operation is essential for developing knowledge needed for on-going development of the intelligence profession. This is why practitioners are best fit to develop the theory of intelligence whose implementation feeds the development of further relevant knowledge.

The Cognitive Campaign: Strategic and Intelligence Perspectives

Yossi Kuperwasser and David Siman-Tov, Editors

Memorandum No. 197 October 2019

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

The Institute for the Research of the Methodology of Intelligence

המערכה על התודעה: היבטים אסטרטגיים ומודיעיניים

עורכים: יוסי קופרוסר ודודי סימן טוב

Institute for National Security Studies (a public benefit company)
40 Haim Levanon Street
POB 39950
Ramat Aviv
Tel Aviv 6997556 Israel

E-mail: info@inss.org.il
http://www.inss.org.il

Graphic design: Michal Semo Kovetz and Yael Bieber,
TAU Graphic Design Studio
Cover photos:
- Television screens, by Wags05 at English Wikipedia, https://commons.wikimedia.org/w/index.php?curid=43906515
- Courtroom, iStock 876701606
- Mark Zuckerberg at F8, May 1, 2018, by Anthony Quintano, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=72122387
- Nuclear explosion, iStock 955124060
- Tahrir Square, Cairo, February 11, 2011, by Jonathan Rashad, Flickr, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=13535760
- Russian President Vladimir Putin, Shutterstock, ID:10187259g
- Donald Trump presidential inauguration, Washington, January 20, 2107, by White House photographer, Official White House Facebook page, reprinted at https://commons.wikimedia.org/w/index.php?curid=55185771
- Businesspeople: Shutterstock, ID: 409001227

Printing: Digiprint Zahav Ltd., Tel Aviv

© All rights reserved.
October 2019

ISBN: 978-965-92750-3-8

Contents

Preface 7

The Cognitive War as an Element of National Security: Based on Personal Experience 13
Moshe Ya'alon

Part I Theoretical and Conceptual Dimensions

Influencing Public Opinion 25
Haim Assa

Disinformation Campaigns and Influence on Cognition: Implications for State Policy 37
David Siman-Tov

Beyond the Web: Diplomacy, Cognition, and Influence 51
Haim Waxman and Daniel Cohen

Defending against Influence Operations: The Challenges Facing Liberal Democracies 61
Gabi Siboni and Pnina Shuker

Part II Cognitive Warfare: Intelligence and Cyber

Cognitive Intelligence: The Theoretical Aspect 77
Kobi Michael and Yossi Kuperwasser

Subjective Truth as a Challenge for Intelligence in the "Campaign between Wars" 91
Colonel A and Major A

Influence Operations in Cyber: Characteristics and Insights 99
Deganit Paikowsky and Eviatar Matania

Part III Global Dimensions

Russia as an Information Superpower 115
Vera Michlin-Shapir, David Siman-Tov, and Nufar Shaashua

Iran's Information Warfare 135
Itay Haiminis

Part IV Israel and the Cognitive Campaign

Cognition: Combining Soft Power and Hard Power 151
Udi Dekel and Lia Moran-Gilad

When the Intelligence Officer and the Public Diplomat Meet 165
Yarden Vatikay and Colonel O

Consciousness as Leverage: The Israeli Campaign regarding the Iranian Nuclear Program 175
Ronen Dangoor

The Threat of the Delegitimization of the State of Israel: Case Study of the Management of a Cognitive Campaign 199
Shahar Eilam and Shira Patael

Mindset and Social Resilience in Security Emergencies in Israel 213
Meir Elran, Carmit Padan, and Aya Dolev

Preface

In the information era, the cognitive campaign has become a central element of national security in struggles between adversaries. This volume, published jointly by the Institute for the Research of the Methodology of Intelligence (IRMI) at the Israel Intelligence Heritage and Commemoration Center (IICC) and the Institute for National Security Studies (INSS), aims to expand knowledge and understanding of the cognitive campaign, with an emphasis on intelligence methodology in this campaign.

The cognitive campaign is not new, and it is an inseparable aspect of every strategic and military conflict. In recent years, this struggle has played a much more important role than in past conflicts; at times it takes place without a direct military context and is not even led by military bodies. The cognitive campaign is a continuous campaign; thus, its prominence is greater in the period between wars (as a part of the "campaign between wars").

It is important to distinguish between cognition and the cognitive campaign. Cognition is the set of insights that an individual or individuals have regarding the surrounding reality and the way they want to shape it, derived from the set of the values and beliefs through which they examine and interpret their environment and work to confront its inherent challenges, and even to change it. In contrast, the cognitive campaign involves the actions and tools that entities that are part of a certain campaign framework use to influence the cognition of target audiences or to prevent influence on them. The purpose of the cognitive campaign is to cause target audiences to adopt the perception of reality held by the side wielding the effort, so that it can more easily advance the strategic and/or operational objectives that it sees as critical. The cognitive campaign can be negative, that is, prevent the development of undesirable cognitive states, or positive, with an attempt to produce the desired cognition. Along with the use of force, the various tools and methods of operation in the cognitive campaign include designated tools, some of

which are familiar and traditional, such as military psychological warfare (deception, leaflets), spokespeople, diplomacy, and influence via mass media tools (written journalism and television), while others are novel and derive from the digital world, including the social media.

Every use of force in a military context, and likewise every political process, includes a cognitive dimension. Furthermore, the use of force or a political process sometimes takes place in order to achieve an objective in the cognitive campaign, while other times the cognitive component is complementary. Therefore, we must distinguish between actions that aim specifically to influence cognition, and actions that have a different purpose and aim to influence cognition indirectly, and to assess in advance the different kinds of influence in the decision making process. For example, messages relayed through the media aim to influence a certain audience directly. On the other hand, a war that aims to defeat an armed organization that is active in an urban area will also influence the cognition of the population living in that area, even if that is not the war's specific mission.

Many elements take part in the cognitive campaign and operate vis-à-vis a variety of target audiences, while they themselves are subject to influence. As a result, the campaign requires deep familiarity with the basic cognition of the target audiences, which derives from their culture, beliefs, and values, as well as with their situational cognition in relation to concrete events, and with the ways it is possible to help shape the cognition of these target audiences. Establishing this multifaceted familiarity requires a multidisciplinary perspective and professional knowledge from complementary disciplines such as sociology, psychology, anthropology, economics, marketing, and advertising, as well as diverse skills, especially an understanding of the worlds of social media, information, intelligence, and the media.

Intelligence plays a central role in the cognitive campaign. Intelligence agencies must understand and present the basic cognition and the situational cognition of the various target audiences and the ways they are shaped, in order to be able to influence the cognitive efforts of those leading the campaign. Cognitive efforts require various kinds of intelligence, including political, military, social, and cultural intelligence. Intelligence agencies also need to produce content and messages that serve the campaign and to identify opportunities that derive from the information they have and the intelligence knowledge and insights that they produce. Sometimes they

must conduct cognitive operations themselves, based on the knowledge and operational tools they are responsible for, whose scope has increased in the information era. In addition, intelligence agencies must identify the efforts of other parties operating in the campaign, and must sound the alarm and help thwart them, if it becomes clear that they are hostile and covert. The more intelligence for the purposes of the cognitive campaign is integrated with its operational components and within the existing intelligence system, the more effective it may be.

The phenomenon of fake news and the Russian and Iranian intervention in the democratic discourse and in election processes in the West have placed the issue of the cognitive campaign at the top of the global agenda, especially after demonstrating the potential inherent threat to democracy and the difficulty in coping with it while maintaining the commitment to democratic values. This difficulty emerges since preventing external intervention may undermine freedom of expression, especially when it is not clear whether it is hostile intervention, and particularly since in the digital era the division between "internal" and "external" is not as clear as it was in the past. In the case of the internal cognitive campaign, the goal is to counter foreign offensive cognitive efforts without harming the democratic discourse.

The increasing importance and complexity of the cognitive campaign has led to the establishment of designated governmental bodies in the West, including in Israel. However, there is still no overall vision of the campaign that would enable reaching agreement on the different efforts needed to achieve its objectives and create synergy between them. Effectively addressing the challenges of the cognitive campaign requires continuing to develop mechanisms and processes that enable ongoing learning and improvement, both in the offensive context, meaning influencing foreign populations, and in the defensive context, to prevent foreign and hostile influence over the domestic population, while utilizing all of the capabilities and tools at the disposal of those conducting the campaign.

One of the challenges in making the cognitive campaign a central part of the security concept is the difficulty security organizations have operating in a field in which the use of operational forces is not a central component, and in which the mission is to convey messages, sometimes vague, to broad audiences. This is especially prominent in Israel, where the IDF is very

dominant and thus it is difficult to adopt new methods that do not focus on the use of force.

Another challenge is the difficulty in measuring and assessing the effectiveness of cognitive efforts. Some suggest measuring user responses or the message's exposure, but the ability to evaluate effectiveness using only these measures is highly problematic. Another direction for assessing the level of success in changing the discourse is through semantic research. Sometimes there is cognitive influence in the very demonstration of the ability to launch a cognitive effort that penetrates the defenses employed by the defending side. In any case, even when it is possible to analyze influence, it is difficult to separate between the influencing elements that have caused it.

The fast changes in the world of information and the ability to disseminate information quickly enable spreading ideas and rumors at such a fast pace and in such a decentralized way that the ability to understand and control what is happening in this world is very limited. Those who purport to influence cognition must understand this zeitgeist and internalize it.

A significant portion of the centers of control over the global information flow has moved from states to global media companies such as Facebook and Google, which are motivated by commercial considerations. These companies serve as a platform for the transfer of messages and the creation of connections, while also being a player whose policy affects the content on the internet. Civil society likewise plays a dual role in the digital and internet age: it is a central target for influence, but also plays an essential role in the campaign itself, alongside official institutions. The ability of citizens to organize and take action as part of the campaign raises the question: what is the connection between the state and civil society in this context, and what is the role of civilians in the cognitive campaign, in both the defensive and offensive dimensions?

This collection discusses the cognitive campaign from diverse and complementary perspectives, some of them academic and some reflecting the personal experience of the writers, in both state frameworks and in civil society or business frameworks. The articles included in the collection show different approaches to the cognitive campaign, and this diversity illustrates how new, complex, and challenging this field is.

The collection aims to stimulate research and discussion on the diverse fields that make up the world of the cognitive campaign. The need to deepen

the discussion and research stems from the increasing prominence of this field and from its fast development in recent years. Among the topics that require further study are the external and internal threats and the connection between them; the technological developments of the cyber campaign in the context of cognition (which today already enable the creation of false images and in the future will also enable advanced fake videos); and adaptation of the security doctrine to the unique characteristics of the political culture in each democratic society.

This collection includes articles by both researchers and practitioners. We would like to thank the writers – academics, practitioners, and those with the relevant experience who have contributed their time and their knowledge to this collection. Thank you to leading members of the INSS research staff, including Dr. Anat Kurz, Brig. Gen. (ret.) Shlomo Brom, and Dr. Gallia Lindenstrauss, for their important advice and their contributions to the quality of the articles and the collection as a whole.

We would also like to thank the directors and staff of the two organizations: Maj. Gen. (ret.) Amos Yadlin, Executive Director of INSS; Brig. Gen. (res.) Udi Dekel, Managing Director of INSS; Brig. Gen. (ret.) Itai Brun, Deputy Director of INSS; and the leadership of IICC: Brig. Gen. (ret.) Dr. Zvi Shtauber, Chairman of IICC; Brig. Gen. (res.) David Tzur, CEO of IICC; and Hanan Mazor, Deputy CEO of IICC for their contribution to the organizations' efforts toward integration on this project. Thank you also to Moshe Grundman, the Director of Publications at INSS, to English editors Dr. Ela Greenberg, Lisa Perlman, and Dr. Judith Rosen, to graphic designer Michal Semo Kovetz, and to research assistant Shira Cohen.

Yossi Kuperwasser and David Siman-Tov

The Cognitive War as an Element of National Security: Based on Personal Experience

Moshe Ya'alon[1]

I remember the story of the Battle of Kela on the Golan Heights during the Six Day War since my youth. At the decisive moment of the battle, only two functioning tanks remained for conquering the target, commanded by the company commander, Lt. Nati Horowitz (later Brig. Gen. Nati Golan). These two tanks brought about the retreat of a considerably larger Syrian force. The story of the battle was seared in my memory as proof that quantitative advantage and physical superiority are not sufficient – what is necessary, and perhaps even more important, is cognitive superiority.

I have learned from experience that cognitive superiority among forces stems from the morale of the fighters; the fighting spirit; the confidence in commanders, their strength, and their ability; and belief in the justness of the cause. All of these are "soft" elements that are not visible and not calculated with the number of troops or weapons. I have also learned that the importance of cognitive superiority goes beyond the boundaries of the battlefield and applies to the home front as well, as there is enormous importance in the cognitive state of civilians, especially, but not only, when the nation is at war. In the case of civilians too, "soft" elements, such as the population's morale; confidence in the leadership and defense and rescue forces; social solidarity; and belief in the justness of the cause are of the utmost significance before, during, and after the campaign. That is, the cognitive aspect is important both during times of peace and during times of war.

1 Lt. Gen. (ret.) Moshe Ya'alon is a former Director of Military Intelligence, IDF Chief of Staff, and Minister of Defense. At the time of writing this article, he served as a senior researcher at INSS.

It is important to distinguish between several populations in the cognitive campaign:

a. Our forces: It is necessary to distinguish between the political and the military leadership, the fighting forces, and the civilians (families and acquaintances of soldiers, civilians in the areas under attack, and the general public).
b. The enemy: It is necessary to distinguish between the political and military leadership of the enemy, its fighters, and its civilians.
c. The regional and international system, comprising the leaderships of friendly and hostile states, the public in these states, and international institutions.
d. Intermediary bodies that influence public opinion in each of the environments: the media, social networks, and so on.

The many groups and their respective interests have always been a challenge, which is intensified due to the difficulty of separating between the different target audiences. The information age has created new capabilities of division into distinct target audiences and targeted broadcasting of messages to them. At the same time, the messages transmitted to one sector are also received by other target audiences, and each population is able, free, and even expected to interpret the events on the ground, as well as the messages that accompany them, in a way that suits and promotes their perspective and their interests.

Aside from belonging to one group or another, there are several additional factors that influence people's consciousness among each side and their understanding of the campaign forms, including its objectives and achievements. Among them (not necessarily in order of importance):

a. The kinetic-combat activity of both sides and its results.
b. Public diplomacy, propaganda, psychological warfare, and branding by both sides toward the various target audiences, for the purpose of strengthening the spirit of the target audience of one's own forces and undermining the spirit and legitimacy of the other side, both vis-à-vis the other side and in the eyes of the international community.
c. Events in the international arena: the general zeitgeist, along with specific responses by official figures and civilian/private figures in the international community.

Beyond these three factors, which stand out in times of emergency, there are many additional elements that influence a state's national resilience in routine times, and as a result, serve to shape consciousness indirectly. These factors influence both the way the state perceives itself, its capabilities, and the challenges it faces, and the way it is perceived by its adversaries and the entire international community. These factors include the state of the economy, education, quality of life, innovation, and more. Despite the great importance of these variables, the scope of this article allows a focus on the cognitive efforts surrounding the campaign itself, and not the complementary and indirect factors.

The cognitive arena is important in any struggle between states, all the more so in the State of Israel's struggle against terrorist and guerilla organizations, some of which are hybrid (i.e., terrorist organizations with semi-state functions – political, social, and others), such as Hezbollah in Lebanon or Hamas in the Gaza Strip. In this case, the challenge of the cognitive war intensifies and becomes more complex. There are several reasons for this:

a. Acting in accordance with the law: The State of Israel acts in accordance with the law and is subject to both Israeli law and international law, while hybrid terrorist organizations do not see themselves as subject to laws. They make prominent use of intentional attacks against Israeli civilians, while hiding and taking offensive action from within their civilian population centers, which they use as human shields, in violation of international law and norms.
b. Double standard: The State of Israel is challenged in the international arena by figures who ignore its enemies' frequent violations of international law and norms in a way that leaves it alone in the campaign. Those who refrain from assigning sovereign state responsibility, for example to Hamas for the situation in the Gaza Strip, or to Lebanon for Iran and Hezbollah's activity from its territory, fall for intentional cognitive manipulations and tend to believe that these lawbreaking terrorist organizations are the "victim" and Israel is the "victimizer." That is, these same terrorists are presented as "innocent" civilians under "occupation" or "blockade," while Israel is presented as carrying out war crimes regardless of the need to defend itself. Israel's enemies exploit this situation to influence the consciousness of the Israeli public and undermine its belief in the justness of its cause. They understand that when a campaign takes place during a

political argument over its justness, the challenge increases tenfold. This is part of the attrition strategy of Israel's enemies, after understanding that this is the only way they may cause it real damage, in light of their inferiority on the military-kinetic battlefield.

c. The centrality of the home front: Most of the burden in the campaigns that the State of Israel has had to wage falls on the home front, that is, on civilians. Therefore, what is put to the test in these kinds of campaigns is the stamina of society, more than military force. Hence the importance of cognitive superiority, which is expressed in the Israeli public's determination and stamina in light of its belief in the justness of its cause, and in the enemy recognizing these qualities in the Israeli public. The antithesis of this is the way Hezbollah and Hamas treat their civilian home front as human shields.

The Conflict with the Palestinians in the Cognitive Context

In the campaign against Israel that began after the Oslo Accords, Israel suffered over 1,000 deaths in a long series of attacks that were seared into the Israeli consciousness, including suicide attacks. This campaign took place during an internal political debate surrounding the causes and future of the Israeli-Palestinian conflict, as well as Israel's control of Judea, Samaria, and the Gaza Strip.

The Palestinian side presented "the occupation" as the cause of the conflict. It also refrained from stating explicitly that the problem is the "1967 occupation" and never committed to an arrangement whereby an Israeli concession of all of the territories conquered in the Six Day War would constitute "an end to the conflict and end of all claims." Nevertheless, this idea of an end to the conflict upon withdrawal from the 1967 territories took root among many in Israel and worldwide; this false narrative also gained a foothold within Israeli politics and in the international arena, and gave the Palestinians an advantage. They absolved themselves of responsibility and created the impression that the end of the conflict depends on Israel's good will. In presenting "the occupation" as the cause of the conflict, the Palestinian side attained a significant cognitive achievement, which reversed the asymmetry that had characterized the Arab-Israeli conflict from its outset, in which little Israel was analogous to David fighting against Goliath, embodied in a superior coalition of Arab states. The moment "the occupation" was

presented as the cause of the conflict, the Palestinian cognitive effort focused on placing the responsibility for it on Israel alone, while consolidating the image of the Palestinian David and the Israeli Goliath.

From my appointment as Director of Military Intelligence in 1995, at the peak of the implementation of the Oslo Accords, until the end of my term as Chief of Staff in 2005, I saw the Palestinian achievement in the cognitive campaign as a cognitive-leadership challenge for the Israeli political leadership, both internally and externally. It is clear that this reality also made the situation difficult for the tactical echelons. The awareness of this role reversal led me to make operational decisions while seriously considering their cognitive implications. I made efforts to avoid situations that would allow the Palestinian side to exploit them as propaganda, such as pictures of an Israeli tank against a Palestinian youth throwing a stone, or prolonged air strikes (in general, night time strikes were preferred over daytime strikes, and in any case the duration of strikes was kept short).

The many means of photography and communication accessible in the battlefield pose a huge challenge for an army and state that insist on integrity. In operational activity in a civilian environment, every person with a cell phone is a photographer, and photographs can easily be edited in a biased manner. This has placed great importance on the presence of photographers among IDF forces, so that Israel will have visual proof of what actually occurred on the ground. The time it takes for an army and state committed to the authenticity of their reports to verify the facts provides an advantage to terrorists and enables them, their agents, and their supporters to spread their story, which they can photograph, edit, and immediately distribute on the internet and in the international media. By the time the IDF Spokesperson investigates or verifies the facts and then publicizes its credible version, no one is paying attention anymore. The most prominent examples of fabrications and libels produced by the Palestinians that gained momentum before Israel managed to publicize its findings from reliable investigations are the Muhammad al-Dura incident (at the outset of the wave of Palestinian terrorism in 2000) and the so-called Jenin massacre in 2002.

Recognizing Israel's disadvantage in this area led me to work to shorten the duration of inquiries and investigations in order to enable the publication of the Israeli version as quickly as possible. In many cases, Israel has succeeded in shortening the duration of the response after clarifying the matter, while

not compromising on authenticity. Nonetheless, those who do not hesitate to lie will always have the advantage of time.

Along with the obvious adherence to acting within the framework of laws and norms, we took additional steps to address the challenge:

a. Raising the awareness of commanders and soldiers regarding the importance of how their activities appear, and the need to avoid photos taken by the other side, or by members of the media, in a way that could harm Israeli interests. In addition, we introduced the documentation of activity that is important to highlight and publicize.
b. Changing the activity of the IDF Spokesperson's Unit (headed at the time by Brig. Gen. Ruth Yaron) to a unit that operates 24 hours a day, with a war room that receives all of the relevant media information and provides a response as fast as possible in different languages.
c. Training operational documenters from the IDF Spokesperson's Unit who accompany the forces in their activities.
d. Training combat soldiers as documenters.
e. Attaching journalists to forces.
f. Creating reliable and available databases and data centers (in part, both within the IDF Spokesperson's Unit and the Ministry of Foreign Affairs) for those interested in receiving the Israeli version, including volunteers fighting the legitimacy war and struggling against boycott and delegitimization movements (BDS, for example) on social media.
g. Distributing information to governmental bodies, such as the Ministry of Foreign Affairs, the Ministry of Public Diplomacy (if it exists), and the Ministry of Strategic Affairs.
h. Establishing the Center for Cognitive Operations during my time as Chief of Staff, as another way to address the challenge of the cognitive war.

These changes, which were mainly within the IDF, contributed to the State of Israel's improved handling of the cognitive war. I observed this during Operation Cast Lead in the Gaza Strip in 2014 as Minister of Defense: despite the length of the operation, Israel enjoyed both civilian resilience and international sanction to continue its activities, thanks to the understanding and recognition of the operational need for them. However, these processes alone are not sufficient. An integrated effort is required for addressing all of the challenges in the cognitive campaign in the framework of a national public diplomacy and cognition directorate, as will be explained below.

Cognition as an Ongoing Campaign

The cognitive preparation of the fighting force and of civilians does not begin the day the escalation starts. Cognition is formed, influenced, and shaped all the time, and the cognitive state at the time of the outbreak of a campaign is the direct result of the routine that preceded it. The cognitive campaign is never-ending and takes place before, during, and after the campaign on the ground.

Before and during the campaign, there is importance in leadership statements that highlight the justness of the cause and convince both civilians and fighters. Such statements strengthen the belief, fortitude, and resilience of civilians and soldiers in advance of the campaign.

At the outset of the wave of Palestinian terrorism in 2000, when I served as Deputy Chief of Staff, I found myself speaking to the general public, and not just to soldiers, and explaining the essence of the campaign and the challenge Israel was facing. In fact, this is the role of the political leadership and not of army commanders. But in this case, it was politically difficult to admit that a terrorist offensive had been launched against Israel by the chairman of the Palestinian Authority, Yasir Arafat. This created a problem that I saw great importance in clarifying. I decided to prepare the public for the length of the campaign and to make it clear that we must not surrender to terrorism, and that the campaign against it, which will take a long time (even years), is no less important than the War of Independence. I said then, and I still believe, that it is essential that this campaign end in such a way that the Palestinians understand and internalize that terrorism will never be worthwhile for them (the term that I used for this purpose was "seared consciousness"). I expected that these statements would come from the political leadership, but political difficulties prevented this and even led to an argument regarding the nature of the campaign and the right way to respond to the terrorist offensive: to stand strong or to give in.

The cognitive war is also important at the end of the campaign and in its aftermath. Henry Kissinger wrote that in an asymmetric campaign between an army and a guerrilla organization, "The guerrilla wins if it does not lose. The conventional army loses if it does not win."[2] That is, the very survival

2 Henry A. Kissinger, "The Viet Nam Negotiations," *Foreign Affairs* 47, no. 2 (January 1969): 214.

of a guerrilla organization is portrayed as its victory and as a loss for the army that opposed it.

Indeed, it is difficult to explain how at the end of an operation like Protective Edge, Hamas survived a campaign against the IDF that lasted 51 days, while claiming that the IDF won. It is easier to present a victory such as that of the Six Day War, in which it is possible to demonstrate territorial gains and show the flag flying above the Western Wall, at the peak of Mount Hermon, or on the banks of the Suez Canal, or to show pictures of destroyed enemy airfields and the convoys of its destroyed tanks. Do pictures of thousands of destroyed buildings in the Gaza Strip after Operation Protective Edge serve as a victory image?

These two kinds of campaigns raise the question of the essence of "victory" and "defeat." Victory or defeat in a campaign derive from the achievement of the objectives defined for it. My argument is that the defeat of Hamas in Operation Protective Edge was more significant in terms of the period of calm that was achieved than the situation following the brilliant military victory over the Arab armies in the Six Day War. Defeating the enemy means bringing about a situation where it stops wanting to fight against you and accepts a ceasefire according to our conditions. In Protective Edge, Hamas accepted (on the 51st day of the campaign) a ceasefire without any condition and without any achievement on its part, and more importantly – it was deterred. This was reflected in that Hamas did not fire as much as a single bullet into Israeli territory until May 2018 (until the escalation surrounding the Nakba events), and even then, it acted with restraint, due to concern that it would be forced to pay a heavy price for any escalation on its part. Even when southern Israel suffered from the "kite terrorism" in the summer of 2018, the moment the threat to renew the campaign became tangible, it was evident that Hamas acted quickly to restrain events on the ground.

In contrast with Protective Edge, Egypt renewed its fire only three weeks after the end of the Six Day War, and Syria did so three weeks thereafter, in a manner that dragged the State of Israel into the War of Attrition. This does not change the fact that from the cognitive perspective, the victory in the Six Day War was seen as a clear victory, while the achievement of defeating Hamas in Operation Protective Edge was described critically and disparagingly. This illustrates how critical it is that the leadership engage not only in achieving victory on the physical battlefield, but also in the

cognitive battlefield, especially surrounding the results of the campaign, both internally and externally.

After a campaign, the cognitive struggle in the internal arena begins and ends with the expectations that the leadership created regarding the objectives and results of the campaign before beginning the campaign, both among the domestic public and among the enemy. If the feeling that is created among civilians (and also soldiers) is that the objective is the physical elimination of the enemy and complete conquest of the territory (in this case, the elimination of Hamas and the conquest of the Gaza Strip), though at the outset this is not the objective, a gap in expectations is created that generates disappointment, frustration, and even a sense of defeat. Setting expectations and meeting them is a challenge in itself, let alone when politicians exploit the opportunity to foster false expectations, out of an interest in creating a cognitive basis for attacking the current leadership.

It is also important to explain the achievement externally, namely, to those observing the campaign and its results. Hamas understood that it was defeated in Operation Protective Edge, and hence it requested the ceasefire, ceding its initial demands. Despite this, it was important that Israel make clear to those who were not involved in the campaign – civilians in Gaza, other adversaries in the area, such as Hezbollah and Iran, and the world at large – who won and who lost, and at what cost. The cognitive war at the end of the campaign is of great importance, externally for strengthening deterrence and internally for strengthening the confidence and resilience of civilians and soldiers.

The joint appearances of the Prime Minister, Minister of Defense, and Chief of Staff in briefings during Operation Protective Edge and at its conclusion were made out of a recognition of the importance of displaying the cohesion of the political and military leadership, both externally to enemies, and internally to the Israeli public. This recognition became particularly clear against the backdrop of the internal bickering and mutual accusations among the politicians, especially members of the security cabinet.

Creating a Public Diplomacy and Cognition Directorate

Despite the increasing recognition in the State of Israel of the importance of the cognitive campaign, the steps taken so far display a lack of consistency and systematic activity, and range from improvisation stemming from

necessity to ad hoc planning in individual cases. So far, the State of Israel has not built or instituted a national directorate for the cognitive war, as would be appropriate and expected given its experience. In a reality where the decisive importance of the issue is proven time and time again, there should be a national public diplomacy and cognition directorate within the Prime Minister's Office that would operate under the direction of the Prime Minister and coordinate all public diplomacy and cognitive war efforts. The purpose of this directorate is not to create a single message or to impose censorship, but to direct Israel's public diplomacy efforts by clarifying the policy and ensuring consistency and harmony among various efforts. It is recommended that the head of the public diplomacy and consciousness directorate be named as an advisor to the Prime Minister. This would ensure that cognitive considerations are taken into account from the outset in shaping policy.

As part of its role, the directorate would provide direction and define the areas of responsibility and the authorities of the bodies in charge of conveying messages, and ensure that they reflect a clear and organized policy (which should be formulated in advance). In this framework, the authority and the resources for leading the cognitive campaign in the international arena should be returned to the Ministry of Foreign Affairs, preventing division and duplication of efforts, resources, and responsibility in other government ministries, such as the Ministry of Public Diplomacy and the Ministry of Strategic Affairs.

The directorate that would be established in the Prime Minister's Office should lead policies approved by the Prime Minister, translate them into messages, and coordinate the efforts among all relevant government bodies and defense forces, such as the IDF Spokesperson and the intelligence community. In this way, the cognitive war, like any other war, would be carried out in a coherent manner based on the policy dictated and approved by the political leadership, and include every public servant and soldier. Institutionalizing the governmental effort would also enable individual volunteers or organizations in Israel and abroad to receive reliable information and messages and to contribute in their way to the national cognitive effort.

Part I

Theoretical and Conceptual Dimensions

Influencing Public Opinion

Haim Assa[1]

What is Consciousness?

Consciousness is a concept that was developed in the seventeenth century by the philosophers John Locke and René Descartes. It was Descartes who said that the human is a conscious being, meaning that "he knows that he can think." This statement seems simple, but it is not. Over the course of thousands of years of history humans preferred "the thinking of the gods," even if they were small wooden statues or invisible demons. Descartes also said that "I think, therefore I am." These two statements indicate one main premise, according to which human consciousness is equivalent to the very existence of the human being on the one hand, and it includes a subjective – that is, personal – element on the other hand. In other words, the human being is capable of changing his opinions by himself; that is, consciousness is not determined by a divine power, and it changes over the years.

We can refer to the concept of human consciousness as all of a person's knowledge and beliefs, the way and type of thinking, and additional personality components, such as the level of alertness and suspicion toward the environment, comprehension and analytic ability, openness, friendliness, perfectionism, and inclinations, such as racism or humanity (for example), as well as one's sense of class or economic discomfort in small circles (the family circle) or large circles (the political circle).

1 Dr. Haim Assa is the chair and CTO of Saiykan Ltd., which conducts quantitative and semantic analysis of the social networks and the internet.

Essential Layer versus Opinion Layer

When discussing the issue of influencing consciousness, it is customary to refer to two layers of consciousness: a basic essential one that includes "belief in religion" or "affinity for the nation," and a second layer, which is made up of "positions and opinions." Two people who have an identical basic layer of consciousness can have differing opinions on many topics. Thus, for example, a population composed of members of the same religion (Sunni Muslims, for example) can have different political and behavioral opinions.

Changing positions and opinions among individuals or a population with the same essential layer of consciousness is easier than changing the essential layer itself. Change at this level is usually a complex process that we humans do not have control over. It shifts according to long, deep, and complex processes that occur as a result of the large information revolutions, which enable cultural, social, and political upheavals. The concept of "influence" addresses cognitive change, meaning changing attitudes. An example is changing the perspectives of members of the same religious faith who believe in the use of violence to accept other views, such as shifting to political or business activities (with their range of possibilities) as an alternative to violence.

Influencing the Public versus Influencing Individuals

Another distinction lies in the difference between a public's cognitive state and a specific person's consciousness. This article focuses on influencing the broader public, as opposed to influencing an individual. The attempt to influence a specific person depends usually on the ability to understand or estimate formative components of a person's "personality" and the nature of his behavior, as well as "structured" details, such as his place of residence, information about his family members, hobbies, inclinations, and so forth. The opinion of hundreds of thousands or millions of people is harder to estimate and constitutes a technological challenge. The main challenge lies in processing information and turning a large population that contains a mix of people into an "object;" that is, a uniform entity whose opinions on a certain issue we seek to influence. In recent years, "big data" solutions have been created that address this challenge.

Influencing consciousness means attaining cognitive change of defined opinions of a "public," as opposed to changing a basic level of cognition,

which requires significantly larger processes than any intentional attempt at influencing and usually take place over the course of centuries (for example, changing a religious faith or turning a Palestinian nationalist into a Zionist). It should be emphasized that the attempt to convince a person who has a certain religious faith to change elements of his basic faith is usually doomed to failure. However, there are counter-examples, such as the shift in Egyptian public opinion that enabled the peace process with Israel; the transformation in the public consciousness in the Soviet Union that led to its dissolution; or the adoption of Christianity by the Western world in the fourth century of the Common Era.

The process of changing public opinion is not like creating the momentum for an action by a population that already has the desire to act, and all we are trying to do is to cause the public to take action (demonstration, march, signing a petition, and so forth). For example, motivating a public that is angry at a certain regime to take action means influencing it so that it goes to the town square to protest. This is a different kind of process of influence than that discussed in this article.

This article focuses on changing public opinion. For example, if a given public is convinced that only violent means will resolve its problems, the conclusion is that one must try to influence this population and convince it that there is another, alternative position that is preferable in order to achieve its objective. There are, however, situations in which no convincing or relevant "alternative opinion" can be defined. In these cases, it is possible to conduct an influence campaign that is made up of a number of stages: the first stage is an attempt to create "a degree of discomfort" among the target audience by intensively disseminating information (see "information bombardment" below). After a situation assessment that determines whether there are cracks in the opinions of some of the members of this population, it is then possible to move to the stage of influence, which seeks to change existing opinions and to adopt alternative ones.

Influencing Public Opinion

Influence means changing the opinion of a public, which is defined as having a specific position that we seek to change and replace with an alternative one. What characterizes the population as a target audience and as a uniform object is its "basic cognition" (Sunni Muslim or Shiite Muslim in Jordan,

Lebanon, Egypt, or Sweden, or a Jew who is an Israeli Jew or an American Jew or a British Jew) and opinion on a specific issue. An example is the wish to influence those Shiite Muslims who have a violent inclination, desire, or stance. The wish in this case is to remove the violent stance and replace it with an alternative one. This is similar for Jews who believe that violence toward one adversary or another is the right solution and are imbued with the sense that they should engage in violence toward the adversary.

Similarity Groups

A central element in the influence process is the concept of "similarity groups." Research institutes in the United States have found that convincing a group of "similar" people, for example, who have a similar education, locale, or background (military service in the same unit, went through a significant shared experience, and/or are connected in some manner) to change their opinion is many times more effective than attempting to convince a mixed group of subjects/people of the same objective.[2] Media campaigns, such as through television and radio, are, in effect, a process of influencing all segments of the population, and thus have less relevance. As a result, television and radio campaigns have to carry out a long and expensive process of repetition, meaning continually employing components of influence – advertisements – over time in order to convey the message. These messages are usually targeted at the common denominator of the different population segments, necessitating the use of additional avenues of influence in order to fill in the gaps.

This means that the start of any process of influence based on social media is to divide the population into "similarity groups."[3] Here lies the great advantage of an influence campaign on social media: In traditional media, like television and radio, it is not possible to produce "similarity groups," while on social networks it is. When it comes to a population of 50

---

2 P. Karen Murphy and Lucia Mason, "Changing Knowledge and Beliefs," in *Handbook of Educational Psychology*, ed. Patricia A. Alexander and Philip H. Winne (New York: Routledge, 2006).

3 In the construction of "similarity groups," one must take into consideration the premise that these networks are not free from the influences of additional actors, which also include fictitious users, and that the real actors are careful not to share information that reveals their true opinions.

million people, for instance, this must be implemented through an advanced technological system. Such a system enables:

a. Identifying the people with the opinion that one seeks to change, as well as those with the "preferred" opinion (which is usually the opposite of that of the target audience). These people must have a clear opinion on the issue, and their social or professional standing is of great importance when choosing them for the influencing activity. These people will serve as sources of influence within the discourse produced during the campaign (the methodology of the concept of change).
b. Determining the interests and characteristics of both the influencers and those being influenced. Advanced technologies are also required for analyzing connections, texts, and knowing systems such as the Big Five model (see below).
c. Creating "similarity groups" of people. Advanced technological capabilities are required, especially if some members of the group are not connected to one another.
d. Defining the relevant strategy for each group; that is, the process of influence and the alternative viewpoint.

The Alternative Viewpoint: The Methodology of the "Concept Change"

An alternative viewpoint is the one that the side trying to influence seeks to instill in those willing to change their opinions. Choosing the alternative viewpoint is not simple. First of all, it must be convenient for us and preferred by us, with the potential to produce additional benefits. Second, it must be possible to intensify this position should certain events occur (just as miracles serve as a justification for the existence of a god). Note that not all expected events can be realized through networks.

Situation Assessment

Every campaign, whether it involves influence in a military operation or a match of chess or basketball game, requires a situation assessment before any other step. The ability to create a snapshot of hundreds of thousands or tens of millions of people is possible thanks to social media. Without having intended to do so, Twitter and Facebook provide metrics for analyzing the personalities of millions, known as "psychometrics." As early as 2012, it was

possible to analyze the personalities of millions of people just by following the number of posts they "liked" or by the number of followers they had, and whom they followed. Facebook at that time was an open network and each person was able to know how many posts a person "liked" and whose posts they liked.

We can add the smartphones to this new kind of information, as they have the capacity to indicate a person's level of mobility, his response speed to phone calls, and the responses of others. Thus, smartphones serve as a kind of "central station" for the activity of each human being. In the context of social media, we can say that the smartphone is the ultimate analyzer of the personalities of many millions of people without their even being aware of it.

This is the basis, for instance, of the Big Five model.[4] This model, created in 2012, conducts statistical analyses of big data and makes conclusions from them. The model, along with social media and smartphones, enables us to produce insights on the personalities of people who have been active on social media, according to their number of "likes" and whom they follow, based on five characteristics: "openness," or the extent to which it is possible to interest that person in additional topics; "conscientiousness," referring to the person's level of perfectionism; "extroversion," or to what extent the person is outgoing or social attention is important to him; "agreeableness," or how cooperative the person is; and "neuroticism," referring to the extent of the person's inclination toward negative emotions, such as anger and guilt. These five characteristics together are known as OCEAN (Openness, Conscientiousness, Extroversion, Agreeableness, Neuroticism).These characteristics served as the basis for the capabilities that were used by Cambridge Analytica, which later considerably influenced elections worldwide, especially in the United States, where it helped the election campaign of Donald Trump, as well as the Brexit campaign in England. Cambridge Analytica studied the research and products of the group of researchers who created the Big Five model, continued to process them, and succeeded in formulating situation assessments that enabled Trump's campaign to convey the right messages and, ultimately, win the elections.

---

4 Wu Youyou, Michal Kosinski, and David Stillwell, *Computer-Based Personality Judgements More Accurate than Those Made by Humans* (Riverside: University of California, 2015).

In addition, we can add additional technologies that are already active in the field of influencing consciousness, such as extremely advanced text analysis systems, based on deep learning and machine learning; innovative statistical techniques for analyzing topics of discourse, based on enormous amounts of texts; and technologies based on analyzing networks and further research on the ideas of OCEAN. One example is the study conducted by the RAND Corporation in the United States that found a word that characterizes ISIL supporters and another word that characterizes its opponents. This study has enabled researchers to locate supporters and opponents of ISIL in texts that they have written, even if the word "Daesh" (ISIL) itself does not appear and even if the topic of the discourse was not ISIL.[5]

Together, all of these now create the ability to formulate innovative situation assessments that nullify and obviate the traditional public opinion polls, which are based on representative samples (inadequate in their own right) and are quite limited in their ability to identify the personalities, interests, and inclinations of hundreds of millions of people (the new capabilities detailed above enable, for example, the identification of homosexuality).

Influence Campaigns

An influence campaign is a process that takes place over time, meaning that it is not "local" in time but rather is a long and patient process. This campaign is based on a discourse between people with "our" opinion and people with the opinion that we seek to change, and it must include concepts that are characteristic of the influence process (relatively new concepts that are used by the influence campaign). Eventually, these concepts will serve as anchors that will support the ability to estimate the campaign's level of success; that is, they are important in that they have the ability to be tracked, which is a critical component of an influence campaign's success.

A campaign focused on changing positions and opinions requires a monitoring system that periodically or continuously examines whether the relevant people are being influenced and who have been influenced; that is, what type of profile (people's characteristics and interests) has been influenced, what type of profile has not been affected, and who has been

5 Elizabeth Bodine-Baron, Todd C. Helmus, Madeline Magnuson, and Zev Winkelman, *Examining ISIS Support and Opposition Networks on Twitter* (Santa Monica, CA: RAND Corp., 2016).

affected in ways other than expected. This ability to monitor makes it possible to update the campaign according to both periodic tests and alerts that the monitoring system can produce.

Profiles

Profiles of people within the group defined as the "similarity group" must be created in order to identify a common denominator (interests and characteristics) among those people who were not affected by the influence strategy or upon whom it had the opposite effect. These profiles can be produced by the technological monitoring system, which should operate continuously and provide automatic alerts.

The last presidential elections in the United States provides an example of this kind of profile: they are people whose location is North Carolina, are characterized as mine workers, and have either have been fired or still work at mines that have not yet been closed and are about to be fired, as well as their family members. The campaign that targeted these people is different from the campaign that targeted groups of academics and members of the tech industry in San Francisco, suggesting that different cognitive campaigns are needed for various groups. The group composed of the blue-collar workers from North Carolina – who have been fired from mines that closed in recent years, or who are concerned that they will be fired and those dependent upon them – creates a profile of people who are defined as a "similarity group."

This "similarity group" must be provided with relevant messages that can inspire hope among those belonging to it and lead them to change their opinion – from voting for the Democratic Party to the Republican Party, for example. In effect, this was one of the results of Cambridge Analytica in the last US presidential elections, which led to the victory of Donald Trump, among other things. This happened despite the fact that the majority of blue-collar workers traditionally constituted a political force that supported the Democratic Party; however, the party was not able to understand their needs and assumed that they would vote for it in any case, as they had voted over the years. It can be said that these voters changed their traditional political position thanks to the Republic campaign among "disaffected voters."

Influencing the Influencers

In principle, there are two kinds of influencers. The first kind includes those who are able to sway specific populations to change their opinion. These influencers should be activated in the influence campaign, and they are quite effective, especially when they are matched with the discourse groups based on shared characteristics and the level of similarity between them and those targeted. For example, it is likely that the physicist Michio Kaku can be influential among physicists and those interested in physics but would not be influential among soccer players, while Cristiano Ronaldo cannot influence a group of physicists but certainly can sway a group of soccer players and their fans, even if the issue on which he tries to influence them is strategic or political.

The other kind of influencers are "epicenters" for the opinion that we are seeking to change. The concept of "epicenters" in this context means that these people have many connections, followers, and receive numerous reactions (such as "likes," tweets, and so forth) to their statements/opinions. As a result, influencing them is almost impossible, as their status is almost their entire being, and changing opinions or attitudes is equivalent to destruction. In some situations we do not need to change others' opinions but rather convince them to move from an agreed-upon position to a kind of action (demonstration or signing a petition and so forth). In such cases, the influence is not embodied in changing opinions but rather in creating momentum so that the person will quickly carry out an action. In this situation, influential "epicenters" have great value in accelerating the process.

"Dissatisfaction"

Influence, in the sense of changing opinions, needs to focus on groups who are in a state of dissatisfaction. This means groups of people who still have a problematic viewpoint according to those seeking change but who have also expressed a certain dissatisfaction and criticism of some components of the viewpoint that they hold. A group of dissatisfied people is the most convenient platform for influence in the sense of changing opinions. Dissatisfied people can also be identified using the tools described above, including a sophisticated version of the Big Five and text analysis.

"Information Bombardment" as a Means of Influencing

Another method of influence that is intended for very specific situations is creating massive amounts of information that are connected to or perceived as connected to the alternative opinion that we seek to instill, at the expense of an existing opinion that is not advantageous for us. Information bombardment means producing news and presenting data, research, and inferences quickly and at a level that is newsworthy and relevant to the various "similarity groups" (for example, in numbers and graphs for academics and in pictures for truck drivers). This kind of "bombardment" can create cracks in the perspectives of people who are part of our target audience. Sometimes an additional stage is needed, in terms of the conceptual change methodology (CCM), while exploiting the success of the "bombardment" stage in order to expand the cracks and create dissatisfaction among the target audience.

The Synergy between the Different Methods

In order to achieve the desired result, the tools presented above can also be used in parallel and in sequence. The CCM approach, along with information bombardment, creating momentum, and other tools, all serve as means for creating change. Thus, the tools should be used according to a preformulated plan, although any influence campaign can be adjusted and should be dynamic, thanks to the ability to monitor it.

One essential element of an influence campaign, which, in effect, serves as its backbone, is the ability to automatically monitor its results; that is, there must be a system that conducts continuous assessment of the "cognitive status report" of the target audience. Such a monitoring system should also provide alerts about any changes – with the change threshold defined in advance – and produce a periodic "cognitive status report" to be analyzed by those managing the campaign.

Conclusion

This article discusses changing public opinions and offers ways to design an influence campaign for this purpose. This campaign is made up of a number of stages, is synergetic, and includes influencing the influencers and information bombardment.

Influencing consciousness is based, in part, on the Big Five model, which means the ability to collect and process enormous amounts of various

kinds of data and produce insights from it. These are insights about the personalities of people who are active on the internet, according to the number of "likes" attributed to them and whom or what they have "liked." Such an analysis enables the characterizing of people's qualities, such as openness, conscientiousness, extroversion, agreeableness, and neuroticism (the tendency toward negative emotions, such as anger and guilt). Mapping these qualities is necessary for characterizing the population we wish to influence. By characterizing these qualities, we are able to create communities ("similarity groups") and to more easily influence them.

Disinformation Campaigns and Influence on Cognition: Implications for State Policy

David Siman-Tov[1]

The Strategic Problem

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

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

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

---

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

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

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

Threat Reference: Cognitive Subversion

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

The potential threats to Israel include:

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

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

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

Main Concepts

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

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

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

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

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

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

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

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

State Organizations

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

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

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

---

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

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

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

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

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

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

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

---

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

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

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

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

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

Legislation

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

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

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

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

---

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

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

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

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

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

Civil Society and Public Education on Digital Awareness

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

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

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

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

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

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

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

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

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

Cooperation with Existing and New Media Companies

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

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

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

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

---

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

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

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

The Challenge of Foreign Influence on Israel: A Defensive Perspective

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

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

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

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

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

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

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

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

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

---

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

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

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

Recommendations

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

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

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

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

Beyond the Web: Diplomacy, Cognition, and Influence

Haim Waxman and Daniel Cohen[1]

Diplomacy is one of the central tools at the disposal of decision makers for advancing their objectives. To a large extent, it involves the attempt to create influence; that is, to lead other actors at the international level to act in a way that serves the interest of the decision maker. However, powerful global social processes – chiefly the internet and the information revolution – have redistributed power in the international political arena. As a result, any party that is interested in influencing the international system needs to focus not only on leaders but also on various kinds of public opinion leaders ("influencers"), who have the attention of decision makers and who have their own constituencies, including on social media.

The development of technology has created new tools of influence and innovative ways of creating social interactions in the digital era, which have also produced a variety of tools for engaging in diplomacy. Diplomacy has important assets in this new era, but it also poses innovative challenges in the field of cognition, to which it must adapt. This article examines how diplomacy copes with or should cope with these new challenges. To this end, it reviews the transformations that the world of diplomacy has undergone in

1 Haim Waxman is the deputy director of the Center for Policy Research at the Israel Ministry of Foreign Affairs. The views expressed in this article represent his own opinion. Daniel Cohen is the head of Diplomatic Counterterrorism at the Abba Eban Institute for International Diplomacy and a senior researcher at the Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv University. The writers wish to thank the staff of the Ministry of Foreign Affairs who assisted them, and especially Noam Katz, DJ Schneeweiss, Benji Krasna, and Yoav Adler.

the digital era, presents the advantages and disadvantages of diplomacy in the field of cognition and influence efforts, and offers tools for coping with the changes necessary for conducting diplomacy in this era.

Changes in the World of Diplomacy in the Digital Era

While traditional diplomacy was like an exclusive club, the new diplomacy, which has developed during the past few decades, has multiple actors and has a relatively high level of transparency. In the current reality, the standing of professional diplomats – the staff of foreign ministries – is losing ground to new governmental players who have entered the diplomatic arena. It is not only governmental representatives who are active in the modern field of diplomacy; changes in the balance of power have led international companies, businesspeople, members of the media, academics, representatives of non-governmental organizations and international governmental organizations, and in some cases celebrities and even ordinary people to operate in the diplomatic field.[2]

Moreover, diplomacy today deals not only with conflicts between states but also with a wide range of issues, such as health, the environment, climate change, food security, trade, the stability of the international financial system, migration, crime, and human rights. In addition to changes of the actors and the issues, major shifts have occurred in the modes of operation and methods of diplomacy. For example, the field of multimedia diplomacy has greatly developed, with states and various players taking part, including in the framework of international organizations. At the same time, the importance of public diplomacy has increased,[3] especially given the understanding that the modes of operation of traditional diplomacy alone cannot bring about changes in the positions of foreign governments, and it is necessary to try to do this by influencing their publics.

---

2 For more on the topic of changes in the world of diplomacy, see Andrew F. Cooper, Jorge Heine, and Ramesh Thakur, "Introduction: The Challenges of 21st-Century Diplomacy," in *The Oxford Handbook of Modern Diplomacy*, ed. Andrew F. Cooper, Jorge Heine, and Ramesh Thakur (Oxford University Press, 2013), pp. 1-35, https://bit.ly/2IxLsr5.

3 Public diplomacy aims to influence elites and broad populations in order to advance foreign policy objectives.

Diplomacy has always responded to changes in the international environment, including technological changes (for example, the impact of the invention of the telegraph in the nineteenth century). The technological revolution that we have been experiencing in recent decades has also had an extensive impact on values, procedures, and processes in the international arena. While some argue that digital diplomacy is traditional diplomacy with a system of new tools, others argue that the change is much deeper and that the very DNA of diplomacy is shifting.

In particular, social media receives considerable attention in the age of digital diplomacy. In the past, the traditional media had the main function of mediating information between the government and the public, while today, social media is the main platform where citizens receive information on developments in the political arena. Furthermore, digital technologies have intensified the concept characterizing public diplomacy today, in which interactive discourse and dialogue are at its center (as opposed to the one-way broadcasting that was common in the past). The public with whom the dialogue takes places not only consumes but also produces the content in this dialogue. Digital diplomacy has several clear advantages, including effectiveness – meaning the ability to reach relevant actors – and efficiency, referring to the ability to reach many more players with less effort and fewer resources.

The digital era also poses many challenges for diplomacy in a number of aspects:

a. *Speed:* The pace of activity in the world of diplomacy has increased immeasurably.
b. *Transparency:* In the past, diplomacy was largely covert, while today it is mostly overt, public, and open, although it still has a covert dimension.[4]
c. *Tools:* Digital diplomacy makes extensive use of tools such as social media, infographics, algorithms, and artificial intelligence. Diplomacy, which was verbal in the past, has become more visual. The use of big data, for example, allows for monitoring diplomatic developments,

4 For more on the dimension of transparency, see Craig Hayden, "Social Diplomacy, Public Diplomacy and Network Power," in *Diplomacy, Development and Security in the Information Age*, ed. Shanthi Kalathil (Institute for the Study of Diplomacy, Georgetown University, 2013), pp. 17-34, https://bit.ly/2VfejSo.

identifying influential players, distributing focused messages to segmented populations, and monitoring the content of diplomatic events.

d. *The changes to the issues on the agenda:* These include the discourse on "fake news," internet ethics, incitement on the internet, cyber warfare, and so forth.
e. *The mode of operation of diplomacy:* Modern diplomats must become internet "personas" and need to build up status and connections that move between the physical and the digital world, otherwise their means of influence will remain limited. One of the major challenges is the necessity of going "outside the bubble" and overcoming the phenomenon of the "echo chamber,"[5] which existed before the social media era but has intensified greatly due to social media and its influence.

Ways Foreign Ministries Have Addressed the Digital Era

In recent years, leaders and diplomats have made increasing use of digital tools to convey diplomatic messages (US President Donald Trump has brought this approach to new heights in his use of Twitter). In addition, public diplomacy makes use of digital tools that are based on interpersonal social connectivity and algorithms that make use of the social networks' architecture in order to enhance messages and disrupt the messages of adversaries. Furthermore, foreign ministries, corporations, and civil society actors engage in discourse in order to shape the new environment that has been fostered as a result of the technological-social-political developments (for example, cooperation between states and social media corporations on issues of internet regulation).[6]

Foreign ministries around the world are trying to adapt themselves to the digital age, and many of them make use of social media and other digital tools and channels of influence; the level of success, however, of foreign ministries and professional diplomats in adapting to the emerging reality is not uniform.[7] For example, many diplomats use Twitter only in order to

5 The concept of the "echo chamber" represents a space with a closed system of people with similar worldviews, who are exposed to a uniform type of opinions that are identical to their own.

6 Thank you to Noam Katz for his enlightening comments on this issue.

7 Brian Hocking and Jan Melissen, *Diplomacy in the Digital Age* (Clingendael Netherlands Institute of International Relations, July 2015), p. 45.

obtain information and to report about their activities and do not use the platform as a tool of influence by sharing content. The ability of foreign ministries to change depends in part on supportive internal structures and the recruitment and training of effective "digital leaders."[8] There are some foreign ministries that are involved in diplomatic innovation. For example, they hold diplomatic "hackathons," which integrate their own knowledge and skills with those of social entrepreneurs, tech professionals, journalists, academics, and businesspeople, in order to tackle traditional diplomatic problems.

The Israel Ministry of Foreign Affairs, which today is considered one of the leading foreign ministries in the field of digital diplomacy, operates over 850 accounts on different platforms, such as social media, instant messaging apps, and websites, and does so in fifty languages, including Arabic and Persian. The Ministry works to create a "toolbox" for the modern diplomat by using existing tools on the internet and by developing new ones, together with the major tech companies. This is in order to enhance its messages and slow down the flow of damaging and problematic messages disseminated by Israel's adversaries. This activity also provides the Ministry with collaboration opportunities with foreign entities that are likewise trying to develop in these areas.

The use of the internet in order to influence provides an advantage over traditional diplomacy when it comes to the viral distribution of messages. The internet enables exposure to be multiplied while it can impair the opposing narratives by disturbing the adversarial media's image of objectivity and legitimacy, or by upsetting the entire information environment of the target audience.

The Relative Advantages of Foreign Ministries in Creating Influence

Despite the decline in the standing of professional diplomats and foreign ministries, they still have relative advantages when attempting to create diplomatic influence. These advantages depend mainly on the unique assets at the disposal of professional diplomats, namely state authority, the reliance on

8 Tom Fletcher, *The Naked Diplomat: Understanding Power and Politics in the Digital Age* (HarperCollins, 2017).

unique state information, and above all, the network of diplomatic missions. These advantages include:

a. *Direct and legitimate access to decision makers*: Diplomats enjoy personal connections and access to decision makers, which even in the modern world are irreplaceable, as well as connections with actors that can influence public opinion and policy, such as legislators, research institutes, members of the media, senior figures in the private sector, and more.
b. *The development of local knowledge:* Diplomats on the ground have the ability to create "local" knowledge thanks to their familiarity of the place, political culture, decision making processes, trends in public opinion, the zeitgeist, and cultural and interpersonal sensitivities. Local knowledge is vital, because in order to create influence, one must understand the perspectives of the local population, such as the ability to answer the questions of what motivates and frightens it.
c. *Connection between physical communities and virtual communities:* In the age of public diplomacy, being present in a place is still important. Diplomatic missions operate within "physical" communities, which today can also be influenced via the internet. A local physical presence also enables creating new networks in the virtual world, through connections created locally. Diplomatic activity needs to be able to move from one arena to another, for example, by transforming support expressed on social media into being present at demonstrations.
d. *Understanding relationships:* Due to their worldwide deployment, foreign ministries have a better ability of understanding relationships and assessing how activities vis-à-vis one party can cause reactions in another place ("the butterfly effect").
e. *Identifying emerging agendas:* Global deployment enables diplomats to be active in diverse arenas – some that are information crossroads (such as the UN missions) – and to identify new issues that are emerging on the global agenda at an early stage.
f. *Integration:* Expanding diplomacy's areas of activity incorporates various professional figures (such as experts on health and the environment). Diplomats, working in the dimension between the professional sphere and the political-diplomatic one, serve as integrators of the different areas of activity, and thus they have the ability – sometimes unique – to formulate a comprehensive and meaningful picture.

As a rule, the relative advantage of foreign ministries appears to be in creating content on diplomatic issues, forging personal connections for the purpose of influencing the decision making, forming narratives and media strategy, and engaging in public diplomacy. As a result of the broad, worldwide deployment and constant contact with civilian and political figures, foreign ministries have a considerable ability to formulate messages that are tailored to the target audience. One characteristic of the foreign ministries is that the representatives who are stationed in other states are replaced after a while. While this has the advantage of renewal, it also has the disadvantage in that the representative needs to recreate personal connections and refresh digital communities. This situation differs from other civil society actors, who maintain a permanent ongoing presence in their places of residence.

The Challenges of Foreign Ministries in the Field of Influence

While foreign ministries and professional diplomats enjoy unique assets, the changing character of threats has caused challenges and obstacles today that prevent them from fulfilling the potential inherent in the digital world. Noteworthy among these challenges and obstacles are:

a. *Inherent asymmetry:* Today state and non-state adversaries operate in an internet arena and have access to cheap and accessible technological tools with which they can threaten stronger actors and influence the general public. The ability especially of non-state actors to disseminate information via social media, with the intention of waging struggles for diplomatic objectives or recognition of their activities, provides them with greater public exposure than in the past. For example, both state and non-state actors create social media campaigns that disseminate true and/or false information, as well as campaigns on content-sharing sites, in order to influence the cognition of the other side. The current response to this is mainly attempts at getting social media platforms to cooperate and remove content. States are fettered by the extent to which social media corporations will cooperate with them, while the ability to implement state regulation on this issue is meager compared to the scope of the phenomenon.
b. *The characteristics of the internet:* The internet environment enables non-state actors to advance their interests without risk of exposure. This is especially true in cyberspace, in which there are no clear boundaries,

and technological tools can be used to enable anonymity and activity that leaves a small footprint.

c. *The lack of activity of foreign ministries in black and gray areas:* Institutional parties, including foreign ministries, must cope with attempts by undemocratic entities to influence information by using propaganda as well as to undermine international institutions by damaging the effectiveness of laws, inciting terrorism, increasing insecurity, and more. The activity of foreign ministries, which is usually transparent, sometimes makes it difficult for them to respond to actors who operate with a small footprint and on covert levels (for example, by hiding their identity to not reveal who is behind a campaign). One partial response to this challenge exists in the ability of the foreign ministries to cooperate with tech companies, which also have an interest in removing harmful campaigns from the internet. Another obstacle is that some governments prefer to use military force or covert actions instead of public diplomacy, which can be referred to as "smart power."[9] In most cases, there is only partial synergy between foreign ministries and the covert organizations that operate in a parallel realm, and this creates asymmetry, which enables adversaries to use non-military means, without the foreign ministry being able to respond effectively.

d. *The age of false information:* The lack of control of the political-strategic narrative can influence the understanding of events and issues, such as who is responsible for an international crisis or conflict. Therefore, a successful disinformation campaign can convince the public in a certain country that its state is at fault in a crisis, even if the campaign contradicts the facts.[10] Foreign ministries sometimes have difficulty coping with these kinds of campaigns and prefer to focus on promoting the country's narrative.

e. *Technological challenge:* The ability of foreign ministries to cope with technological developments is limited compared to the private sector and the intelligence community. This is partly due to budgetary limitations and because foreign ministries are not considered a natural place for research and development. However, foreign ministries have made achievements

9 Joseph S. Nye, "Get Smart: Combining Hard and Soft Power," *Foreign Affairs* 88, no. 4 (July/August 2009): 160-63.

10 In light of the difficulty in measuring the influence of such campaigns, there are doubts regarding their level of effectiveness in disrupting the political order.

in the field of developing technological tools and even at an advantage in developing tools that the business sector is not interested in, because they are not necessarily profitable.

f. *Human capital:* The diplomatic system today is coping with the modern world of employment and needs to recruit and train personnel with the skills for social media activity.
g. *Slow response capability due to excessive bureaucracy and unwieldiness:* Foreign ministries have difficulty implementing long term systemic initiatives and even short term projects, due to being sometimes overly bureaucratic in making the decisions and providing the necessary approvals. As a result, they have difficulty creating partnerships, and delays even occur in approving work plans and timetables necessary for operating in the internet era.
h. *Limitations on the internet:* One of the main limitations that foreign ministries face is legislation, such as the European Union's General Data Protection Regulation (GDPR), which creates obstacles and restrictions on internet activity and, in effect, prevents foreign ministries from engaging in certain internet activities (for example, impairing their ability to operate vis-à-vis a target audience in a focused manner, by collecting the personal information of social media users).

Conclusion: How Must Diplomacy Change in the Digital Era?

A foreign ministry that aspires to achieve goals and objectives in the field of cognition and to influence its adversaries in the networked digital era must develop qualities that will enable it to be flexible and change quickly, while adapting its messages to the relevant target audience and cooperating with additional parties. In order to meet these objectives, foreign ministries need to develop a range of capabilities, which include developing designated technological means of influence that are adapted to the internet world in general and social media in particular. The desired result can be achieved by:

a. Developing platforms for cooperation that enable a governmental body, such as a foreign ministry, to cooperate with a variety of governmental and private entities, as well as with civil society groups that are involved in diplomacy in a broad sense. Each has relative advantages, such as research, intelligence gathering, operating with a small footprint, technology and cyberspace, activity in traditional and new media, and marketing. It is

important to ensure coordination with these bodies in order to create an effective cognitive campaign vis-à-vis internet challenges, both on the tactical and strategic levels.

b. Coordinating efforts on influence issues vis-à-vis a wide circle of defense and diplomacy organizations improves the state's ability to utilize its smart power. For example, responsibility for coordinating and integrating the efforts in a diplomatic campaign should be placed on foreign ministries, in order to ensure that activities are carried out in an ongoing and synchronized manner. In this respect, it is important to remember that a central advantage of foreign ministries is the legitimacy to pursue opportunities and not just to focus on the world of threats.
c. Preparing for the impact of tools such as artificial intelligence on human-machine relations and other areas that will influence the diplomatic arena.

The ability of foreign ministries today to maximize cooperation both within and outside the system is limited, despite the tools and relative advantages at their disposal for influence efforts. In order to meet objectives, it is necessary to conduct campaigns that integrate proactive activity that is both overt (through foreign ministries and civilian actors) and covert (through defense agencies). The way to achieve this is fostering a range of capabilities, which includes developing designated means of influence that are adapted to the networked world in general and to social media in particular, and operating them through a cooperative integrated mechanism. This should be done through a leading body that serves as a center of knowledge, synchronizes the campaign's tools, and translates systemic goals and vision into measurable and feasible objectives.

Defending against Influence Operations: The Challenges Facing Liberal Democracies

Gabi Siboni and Pnina Shuker[1]

Introduction

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

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

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

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

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

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

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

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

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

Influence Operations

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

The Challenges of Liberal Democracies in Defending against Influence Operations

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

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

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

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

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

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

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

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

---

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

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

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

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

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

Possible Ways of Coping

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

---

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

52 Ibid.

53 Erik Brattberg and Tim Maurer, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks," Carnegie Endowment for International Peace, May 23, 2018.

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

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

Conclusion

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

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

Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, 2018), p. 13.

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

Part II

Cognitive Warfare: Intelligence and Cyber

Cognitive Intelligence: The Theoretical Aspect

Kobi Michael and Yossi Kuperwasser[1]

Introduction

Since the dawn of history, strategic conflicts and wars have had a cognitive dimension. The Cold War is one of the best examples of this. In recent years, it has been understood that intelligence for the purpose of influencing cognition is not just another part of the campaign but a critical component of it. Today, attempts to influence cognition are considered a component of a campaign in the strategic, intelligence, and operative spheres. This is also true of the cognitive intelligence that supports them.

In this article, we will focus on cognitive intelligence as a field in its own right whose importance has increasingly been recognized in recent years, as well as its interfaces with other fields that influence it and are affected by it. The article establishes a conceptual and theoretical foundation and aims to serve as a basis for developing methodologies and operating concepts within the intelligence community in the field of cognition, while relying on existing conceptualizations within the field. The article reveals the scope of the discussion and addresses the open questions, which will expand the knowledge base that the Israeli intelligence community has developed as a result of its practical experience in this field.

In order to properly contend with diverse adversaries in the cognitive campaign – including radical organizations – both integrated national efforts

1 Lt. Col. (res.) Dr. Kobi Michael is a senior research fellow at INSS. Brig. Gen. (res.) Yossi Kuperwasser, former head of the research division at Military Intelligence, is the head of the Institute for the Research of the Methodology of Intelligence at the Israel Intelligence Heritage and Commemoration Center.

and coordinated international efforts are necessary.[2] These efforts need to take place simultaneously in four dimensions: prevention, disruption, response, and proactive designed action. In all four dimensions, the efforts require deep knowledge of the operational arena and of the actors influencing it, including the adversaries and the mechanisms of building cognition and its influences, in addition to a creative approach that goes beyond existing conceptual and operative frameworks. Full synergy must occur between the intelligence system's development and its adaption to the challenge of cognition in order to maximize its potential contribution and the management of operational campaigns.

The use of intelligence for the cognitive campaign, especially in the world of cyber as a relatively new area of operation, requires developing a suitable and revised doctrine that includes the manipulative use of information. At the same time, ethical principles must be maintained when using intelligence,[3] which will ensure the effectiveness by maximizing capabilities and their quick and high quality use, as well as the credibility of messages (both in terms of their authenticity and the way they are perceived by the target audiences) and maintaining the protection of sources and information. This should be done while preventing any possibility of using intelligence for internal political needs that are not related to the objective of the campaign.

Intelligence in Relation to the Essence of Cognition

As with all operations, high quality intelligence is a necessary condition for the success of the cognitive campaign. It must be able to identify the parties that are influencing people's cognition and understand the ways that they affect its development and strength. In the cognitive dimension,

2 "Integrated efforts" refers to joint and synchronized operations based on joint thinking and planning of all state bodies and resources that are relevant to the efforts. "Coordinated" means cooperation and transparency in cognitive efforts against shared adversaries.

3 For more on the issue of ethics in intelligence and in intelligence organizations, see Aryeh Roter, "On the Purpose and Role of the Gatekeepers in Intelligence Organizations: The Case of the Shin Bet," *Hossen*, International Institute for Counter-Terrorism, Interdisciplinary Center Herzliya, https://bit.ly/2GVZmAC [in Hebrew]; Yehoshafat Harkabi, *Intelligence as a State Institution – The Hidden Book* (Tel Aviv: Maarachot and the Israel Intelligence Heritage and Commemoration Center, 2015), pp. 63-64, 71 [in Hebrew].

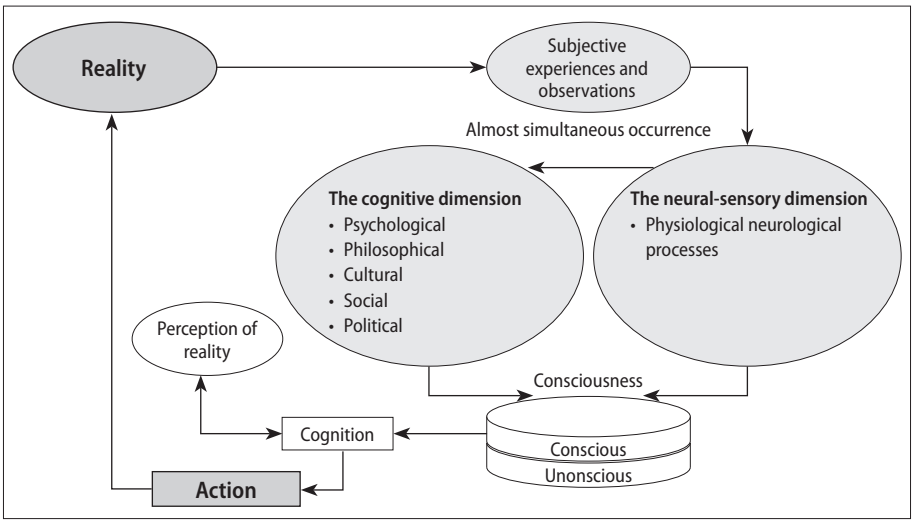


Figure 1: How is Cognition ormed?

this means the philosophical (the worldview of the target audience of the cognitive campaign); the psychological (for example, the way target audiences interpret reality and the question of what is more convincing – intimidation or promises); and the social, cultural, and political aspects. In the physiological-neurological dimension, this refers to how the structure of the brain and nervous system influence the formation of the conscious and unconscious elements of cognition.[4] In addition, intelligence must be able to track the adversary's cognitive activities and produce reliable, timely information in order to influence its efforts and formulate the content of the operations designed to influence cognition.

Figure 1 explains the process of the formation of cognition in an individual. Understanding this process is the core of the intelligence challenge discussed in this article.

Another important issue is the connection between individual consciousness and the collective one. The issue of collective consciousness is complex and difficult to decipher and influence, since the connection between it and that of individuals who make up the collective is not a simple linear sum of all

4 Bernard J. Baars, "Some Essential Differences between Consciousness and Attention, Perception and Working Memory," *Consciousness and Cognition* 6 (1997): 363-71, https://bit.ly/2tvPqpM; "What Is the Difference between Cognition, Consciousness and Perception?" *Quora*, January 25, 2017, https://bit.ly/2IviGHn.

these consciousnesses but rather a unique and complex product influenced by a variety of factors and shaped over time in lengthy, complex processes. One special case is the connection between the leader's consciousness and that of the population. On the one hand, the public influences the leader's consciousness, while on the other hand, the leader has considerable influence over the public's consciousness. The leader's consciousness as an individual with unique responsibility also influences his cognition as a leader and vice versa.

Figure 1 shows how complex and difficult the task of intelligence is within the context of cognition. This is not meant to be discouraging, despite the reasoning behind the critical approach, which warns against investing excessive resources in efforts aimed at addressing this complicated and challenging problem. The need not to give up stems from the fact that the benefits of overcoming these difficulties are significant and could turn out to be a game changer in terms of achieving strategic objectives.

What Is Cognitive Intelligence?

The first distinction that needs to be made in relation to cognitive intelligence is between intelligence about cognition as a phenomenon and an area of activity and influence, and intelligence for cognitive operations.[5] The first category can be defined as foundational and strategic intelligence, while the second can be defined as operative intelligence. The categories overlap and feed off of one another. Operative intelligence is rooted and develops in the logic of foundational and strategic intelligence, while it reveals information and insights that help update and develop strategic intelligence.

In this respect, *situational cognition* and *basic cognition* should be distinguished.[6] Situational cognition refers to specific events/contexts. While it is derived from the basic cognition that relates to a broad and comprehensive perception of the world and reality, it is also influenced by many additional factors, and hence it is easier to influence. The connection between basic cognition and situational cognition in a given context creates

5 This article discusses military intelligence, but it is clear that the intellectual and conceptual discussion of the topic of cognition does not belong only to military intelligence.

6 Zvi Lanir, *The Basic Surprise – Intelligence in Crisis* (Tel Aviv: Hakibbutz Hameuhad Publishing House, Kav Adom, 1983) [in Hebrew].

what we will define as *cumulative cognition*. Understanding the cumulative cognition of target audiences by understanding their basic and situational cognition and the connections between them is the most important task of cognitive intelligence, while cultural intelligence has considerable importance in fulfilling this task.

The Interface between Cognitive Intelligence and Other Areas

Every operative action has significance for cognition. Therefore, in every campaign or operation, even those not defined as cognitive operations – whose main objective is not to influence consciousness – it is necessary to think about the cognitive dimension.

The importance of intelligence in the first stage of campaigns focused on cognitive influence and cognitive operations is partly its involvement in shaping the objectives of the campaign or operation, in order to ensure that they are relevant and achievable. As a rule, the objective is to change the state of mind from situation A to B, or, at least, to prevent a cognitive change in an undesirable direction as a result of the consequences of the operative action. Situation B can be defined as the consciousness that we wish to shape, which is necessarily a derivative of the strategy; that is, what the commanders seek to achieve. This is the reason for the depth of the interface between the cognitive and strategic spheres. The impact of a cognitive operation or campaign explains the connection between the cognitive and the operative spheres.

Cognitive Intelligence and the Cultural and Social Spheres

Cognitive intelligence lays the foundations for understanding the adversary's logic and reveals the agents who influence the adversary and the process. This kind of intelligence helps understand the adversary as well as the cultural foundations of the society in which the adversary operates, and the many similarities and interfaces between them and the world of cultural intelligence.[7]

Israeli intelligence must prepare to contend with a broad and diverse range of cultures in which there are different agents and mechanisms of

7 Kobi Michael and Omer Dostri, "Human Terrain and Cultural Intelligence in the Test of American and Israeli Theaters of Confrontation," *Cyber, Intelligence, and Security* 1, no. 2 (2017): 53-83.

cognitive influence. The challenge in this context is to be able to provide diverse responses, which will help identify the agents of influence who constitute epistemic authorities (those who are seen as agents of truth, who best define the truth, and discourage openness to other information and interpretations)[8] in the various cultures and create mechanisms to influence them in a way that serves the objectives defined.

Intelligence needs to understand the connection between the culture and social structure and the state of mind, both at the basic and situational levels, but it must also understand how this connection develops and the factors influencing it, as well as the practical derivatives of the cognitive influence on the actors. For example, groups with a deep religious consciousness or a strong ideology are expected to behave differently than those with a weak ideology, whose consciousness could be more flexible.

Intelligence for basic cognition and cognitive operations should also relate to the public that is not directly involved in the campaign but influences its results. A certain cognitive operation could have the desired influence on the main target audience but could have a negative influence on secondary target audiences. Therefore, intelligence should be capable of supporting the formulation of cognitive operations whose purpose is to appeal to a limited and defined target (narrowcasting) by conveying focused messages on narrow channels that reach only the defined target audience. Alongside this, general messages should be conveyed on broad and diverse channels (broadcasting) with the intention and understanding that they will reach a variety of target audiences and not just their main target audience. The world of social media – despite its built-in biases – makes it easier to study cognition, makes it accessible, and improves the ability to influence mainly through narrowcasting but also broadcasting. This is partly based on insights related to effective ways to influence cognition; that is, toward whom emotional messages should be directed, toward whom rationalistic or combined messages should be directed, and how.

Cognitive intelligence requires unique access to the social and cultural spaces being researched, an information-gathering methodology, and, in

8 On the significance of the phenomenon of epistemic authority, see Kobi Michael, "The Israel Defense Forces as an Epistemic Authority: An Intellectual Challenge in the Reality of the Israeli-Palestinian Conflict," *Journal of Strategic Studies* 30, no. 3 (2007): 421-46 [in Hebrew].

particular, a suitable research methodology. These should involve skilled and professional personnel from the relevant research fields (anthropology, sociology, psychology, history of the relevant area, political science, social media research, big data, and more). The need for this personnel necessarily influences the selection, recruitment, and training processes of suitable professional staff, while taking into consideration emotional intelligence and cultural intelligence.[9] Creating an intelligence picture of cognition is an ongoing process that also requires information gathering in order to fill in gaps, validate information or assessments, and enlarge the knowledge base, but it also depends largely on overt sources and on tools available in the age of big data.

Unlike intelligence for cognitive operations, intelligence on basic cognition is less limited by place and time, and its work processes and production are characterized as wide-ranging and multidimensional, and it involves a historical and cultural perspective. Intelligence for cognitive operations is much more focused, and its purpose is to advance a specific achievement vis-à-vis a targeted population or adversary, at a given time, and for a defined purpose.

The number of players actively involved in and influencing the cognitive campaign is much greater than the number of players active and influential in the operative one. Therefore, the intelligence challenge is understanding not just the cognition of the adversary and the target audiences but also the methods of action and ways of influencing all the players and connections and the hierarchy of influence in the broad social, cultural, economic, and political contexts, in order to help formulate the most effective and beneficial responses.

The Three Stages in the Process of Producing Cognitive Intelligence

In order to develop intelligence for cognitive operations, a basis of intelligence is needed about the cognition of a target audience in a given arena. Defining the purpose of the cognitive operation by specifying critical intelligence information needed for the operation and engaging in information gathering

9 P. Christopher Earley and Elaine Mosakowski, "Cultural Intelligence," *Harvard Business Review* (October 2004), https://bit.ly/2cChpKL.

and research capabilities enables a more accurate mapping of the existing information gaps that need to be addressed. As for intelligence for cognitive operations, like all operational activity, we must distinguish between three stages: intelligence prior to the operation; intelligence during the operation; and post-operation intelligence (Figure 2).

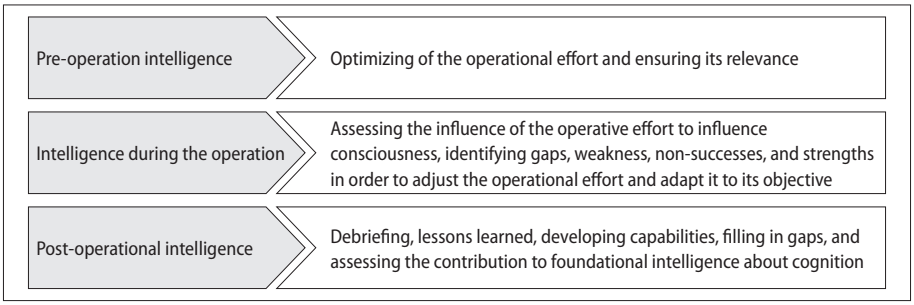


Figure 2: The Three Stages of Operative Intelligence

As with any operation, the intelligence prior to a cognitive operation is necessary in order to optimize the operational effort and ensure its relevance, as well as to prepare the messages and convey them to the target audiences effectively and precisely via their sources of influence. The intelligence during the operation aims to assess the influence of cognitive and operative efforts on cognition in order to locate gaps, weaknesses, and strengths in real time, and to adjust the operational and cognitive efforts so that they achieve their objective, while minimizing unexpected consequences. Post-operation intelligence is required in order to assess the level of compatibility between the result and the desired achievement, and for the purpose of debriefing, lessons learned, developing capabilities, and filling in gaps toward the possibility of another operation to achieve the objective of the original operation, as well as to examine the contribution to foundational cognitive intelligence.

The development of measuring tools and applying them to an operation or campaign are challenging tasks and processes. Along with generic metrics, such as public opinion polls and assessing the overt behavior of target audiences, unique metrics must be developed and defined for each operation or campaign, subject to their specific context.

The Types and Layers of Cognitive Intelligence

Another necessary distinction is between *"preventive" intelligence,* whose purpose is to help thwart the adversary's cognitive efforts by identifying, disrupting, and preventing them, and *"formative" intelligence,* whose purpose is to contribute to efforts to influence the cognition of the adversary and of target audiences in the arena itself or the arena, such as the regional and international ones, which influence the adversary.

In the context of preventive intelligence, it is worth examining the recommendations of Robert Kozlosky, which discuss the need to develop a new intelligence discipline – *public intelligence* (PUBINT) – which requires a new paradigm based on the idea of sharing intelligence information with the public. This contrasts with the traditional paradigm, according to which the public is not a partner in intelligence information and efforts are made even to hide it from the public. The objective of the new discipline is to prevent attempts at subversion by an adversary in the world of modern information warfare, which uses social media and other online means to flood the public with information, some of which is false and biased, in order to influence cognition.[10] Preventive intelligence also requires identifying the adversary's efforts and understanding the logic behind them when trying to influence the consciousness of domestic target audiences, in order to strengthen the adversary's standing, to establish its domestic legitimacy, and to recruit its target audiences for cognitive and operational efforts. In addition, it is important to distinguish between the adversary's actions on *the targeted covert level* (when this aims to serve the efforts on the overt level and complement them, or when it reflects a separate covert effort) and its actions on a more *overt level*, especially in cases where it is necessary to act simultaneously vis-à-vis more than one target audience.

Foundational cognitive intelligence requires methodically tracking the adversary's actions in these contexts and assessing their level of success. In every cognitive intelligence operation, it is also necessary to minimize, disrupt, and prevent the adversary's influence on the consciousness of its domestic and foreign target audiences, in order to weaken it while strengthening the potential influence of countermeasures on the adversary's cognition and

10 Robert Kozlosky, "Modern Information Warfare Requires New Intelligence Discipline," *RealClear Defense*, February 20, 2018, https://bit.ly/2BGIrQ7.

on that of the various target audiences. This is a necessary complement to operative efforts; without it, the effectiveness of the operation will weaken, and its irrelevance possibly will increase.

On the Challenge of Cognitive Intelligence

Cognitive intelligence, including cognitive operations, is different from the operative intelligence that is customary in the military, political, or economic spheres. Unlike intelligence in fairly tangible and defined areas, cognitive intelligence is more amorphous and is difficult to measure and track. Translation into practical terms requires conceptual, linguistic, methodological, organizational, and structural changes. First this requires the establishment of a body that is focused on cognitive intelligence and not just on cognitive operations and then the development of a comprehensive methodology and relevant vocabulary/conceptualizations that provide optimal solutions to all the challenges to which this article refers.

The difficulty and the complexity increase when it comes to defense organizations that are mission-oriented and subject to constant assessment of results or effects in relation to resources and inputs, as well as measuring success and correcting defects. As mentioned previously, it is difficult to measure results and influence in the sphere of cognition. The time required to achieve objectives in the cognitive campaign is significantly longer than in the operative realm. In some cases, a long duration of time is required before identifying the effect or the influence of the cognitive operations, and it is difficult to identify cause-and-effect relations between actions and their results.

Areas of Discussion

The conceptual and theoretical foundations on cognition presented thus far should provide a basis for developing methodologies and operating concepts within the Israeli intelligence community. Now we will present different areas of discussion and open questions that must be addressed so that the relevant body of knowledge will continue to develop, using the knowledge and resources at the disposal of the intelligence community as a result of its practical experience on the issue of cognition.

In the first stage, it is necessary to discuss the question of where cognitive intelligence should be in the order of priorities and which tools and means

(financial and human resources, attention, methodology, organizational changes) should be allocated to this task, given the increasing recognition of cognition's importance in modern conflicts.[11] Until recently, there was a significant gap between the repeated acknowledgment by military researchers and senior defense officials of the importance of cognitive operations and the amount of resources allocated to developing capabilities in this field.[12] In addition, a community-wide authority and organizational structure for coordinating treatment of this topic is clearly lacking. One possible reason is that the topic has not yet been sufficiently regulated on a national level, and that even though the cognitive campaign is defined as a national effort, it is still not being managed as such.[13] Most of the burden is on the IDF, which has succeeded in developing unique and impressive capabilities, but these still do not provide the necessary solutions to the entire scope of the challenge.[14]

In the second stage, it is necessary to analyze the meaning of a rapidly emerging reality that is quickly changing cognition and the way it is shaped. In this context, a number of basic questions arise:

1. How do the characteristics of this reality (volatility, rapid formation, disappearance, and uncertainty)[15] influence cognition and the ability to understand it, and how are the tools that influence cognition changing?

---

11 For example, see the symposium "The Cognitive Campaign: Gaza as a Case Study," held at the Institute for National Security Studies on June 25, 2018, https://www.inss.org.il/event/cognitive-campaign-gaza-case-study/.

12 Kobi Michael and Gabi Siboni, "Preparations for the Nakba March: Hamas's Cognitive Campaign," *INSS Insight* No. 1036, March 20, 2018, https://www.inss.org.il/publication/preparations-nakba-march-hamass-cognitive-campaign/; Gabi Siboni and Gal Perl, "The IDF's Cognitive Effort: Supplementing the Kinetic Effort," *INSS Insight* No. 1028, March 1, 2018, https://www.inss.org.il/publication/the-idfs-cognitive-effort-supplementing-the-kinetic-effort/; Gabi Siboni, "The First Cognitive War," in *Strategic Survey for Israel 2016–2017*, eds. Anat Kurz and Shlomo Brom (Tel Aviv: INSS, 2016), pp. 215-23, https://www.inss.org.il/publication/first-cognitive-war/.

13 See the closing remarks by Brig. Gen. (res.) Udi Dekel, managing director of INSS, at the symposium "The Cognitive Campaign: Gaza as a Case Study."

14 See the statements made by then-IDF Spokesperson Brig. Gen. Ronen Manelis in his lecture at the symposium "The Cognitive Campaign: Gaza as a Case Study."

15 For more on the issue of the challenges of intelligence research in a rapidly changing reality, see Itai Brun, *Intelligence Research – Clarifying the Reality in an Age of*

2. To what extent is this a permanent phenomenon (the meaning of the change)?
3. How can it be measured or assessed (indicators for assessing changes to cognition)?
4. How can the results or impact of efforts to influence cognition be identified in this reality?

Naturally, rapid and volatile changes in reality increase the tension between basic cognition and situational cognition. Generally, changes first influence situational cognition, but they have the potential to penetrate the basic cognition and influence it also. The intelligence challenge in this context is to identify the changes and the potential for change and to identify tools that can influence them, whether by blocking negative influences or enhancing positive ones. Such changes require precise synchronization between cognitive intelligence, which is required for cognitive operations for the purpose of influencing situational cognition, and foundational intelligence, which is required for understanding and influencing basic cognition.

The Connection between Cognitive Intelligence and General Intelligence

Those involved in cognitive intelligence should be in close contact with those who address the comprehensive intelligence picture and should allow synergy between cognitive intelligence and foundational, military, political, and economic intelligence, since understanding the reality requires broad and comprehensive observation of all its components. The connection and the synergy between the areas of intelligence are important because of the input that other areas of intelligence have for understanding cognition and how to influence it, while the synergy should be expressed at both the functional and structural levels of the intelligence community.

The desired synergy should be expressed with a high level of jointness in every operation, especially in intelligence operations.[16] In many cases, cognitive operations are intelligence operations, carried out by intelligence

---

Changes and Transformations (Israeli Intelligence Heritage and Commemoration Center – Institute for the Study of Intelligence and Policy, 2015), pp. 11-12.

16 For more on the topic of jointness in intelligence, see Kobi Michael, David Siman-Tov, and Oren Yoeli, "Jointness in Intelligence Organizations: Theory Put into Practice," *Cyber, Intelligence, and Security* 1, no. 1 (2017): 5-30.

agents; they employ intelligence materials for the purpose of influencing cognition or for gathering information on it. In these operations, even more than in kinetic operations, transparency is necessary between the operative and intelligence dimensions, in order to ensure the relevance of the operative dimension and to identify operational and intelligence risks and opportunities. Every military operation needs to relate to efforts to influence cognition, and full synergy must be ensured between the operative and intelligence aspects and the cognitive ones.

Conclusion

Both cognitive and operational intelligence within the cognitive campaign are relatively new areas of intelligence activity. They support the strategic cognitive campaign (at its center is the political-diplomatic campaign and the use of military force) and more limited operations, some of which are essentially intelligence operations. Cognitive intelligence should be well integrated within every activity in these areas, overlapping with the traditional strategic, operative, and intelligence spheres.

In order to ensure high quality outputs of cognitive intelligence and their optimal integration within diplomatic and military activity, skilled personal is required in the relevant fields, most of which are not part of the classic intelligence professions. In addition, a national directorate on cognition should be established, which could provide a comprehensive perspective on cognitive intelligence issues and all their components, in addition to jointness of the cognitive intelligence with the entire intelligence operations and various operational and strategic aspects.

Subjective Truth as a Challenge for Intelligence in the "Campaign between Wars"

Colonel A and Major A[1]

Background

Intelligence research, which means, among other things, clarifying the strategic and tactical reality, is a complex task that requires fusing considerable information, using "thin paintbrushes" to create a full picture. It also entails formulating a conceptual framework that lacks cultural and personal biases that could influence the observation of reality. Intelligence analysts, as "reality agents," need to use assessment tools to describe a reality that is as accurate, detailed, and complete as possible. Coupled with that, intelligence research requires indicating levels of reliability in the assessment and examination of operative steps that can be based on them, as well as anticipating strategic decisions that the adversary's leaders could make. Beyond this traditional role of military intelligence (MI), in Israel in recent years there has been an increase in MI research on cognitive and influence campaigns as part of what is known as the "campaign between wars," and the IDF's Military Intelligence Directorate has established itself as a force that carries out influence operations.[2]

Increasing friction with the enemy enables continuous study of it and requires, more than in the past, intelligent analysis of the consequences of actions and the use of various tools. Since the "campaign between wars" places the MI officer in the position of a central participant in operational

1 Colonel A and Major A serve in the IDF's Military Intelligence Directorate.

2 Lt. Col. (res.) U. U., "From Intelligence for the Campaign between the Wars to Intelligence in a Reality-Shaping Campaign," Meir Amit Intelligence and Terrorism Information Center, *Intelligence in Theory and in Practice* 2 (2017): 68-71.

activity (beyond his role as a describer of reality), there is of course the danger that his view of reality will be influenced by his involvement in shaping it.

One of the challenges involved in describing reality is the necessity of analyzing it from different angles: "objective" reality (to the extent it is possible to describe it); reality as the enemy sees it in practice; reality as it is perceived by different actors who are relevant to the intelligence question; and of course, reality as it is perceived by decision makers on the analyst's side. Each of these actors makes decisions according to his perception of reality and not according to an "objective" reality that is identical for all, and thus, it is important to analyze the perception of the various types of reality – as it is perceived by the enemy and by the other actors.

A significant marker of the current era is a surge in the "post-truth" phenomenon, in which "objective facts are less influential in shaping public opinion than appeals to emotion and personal belief."[3] This phenomenon was prominent during the last US presidential elections, in 2016, when the internet and social media were flooded with invented facts about the two main candidates, as well as during the referendum held that same year in the UK on the question of whether to withdraw from the European Union (Brexit). It also exists in the Middle East, where the facts have always had different meanings for different actors.[4] The phenomenon is especially evident in situations where there is a lack of clear military victory in wars, and the question of victory remains open to interpretation (for example, the results of the 1973 Yom Kippur War[5] or the Second Lebanon War in 2006[6]). All these instances make it difficult to clarify the reality and develop a clear picture of the situation, but they also provide opportunities to sway

3 *Oxford Dictionary*.

4 Michael Landon-Murray, Edin Mujkic, and Brian Nussbaum, "Disinformation in Contemporary U.S. Foreign Policy: Impacts and Ethics in an Era of Fake News, Social Media, and Artificial Intelligence," *Public Integrity* 21, no. 5 (2019): 512-22.

5 Yemima Rosenthal and Hagay Tzoref, eds., *Haim Herzog, the 6th President of Israel: Selected Documents (1918-1997)* (State Archive of Israel, 2009), p. 240 [in Hebrew]

6 Moshe Arens, "Was the Second Lebanon War a Success or Failure?" *Haaretz*, June 20, 2016, https://www.haaretz.com/opinion/.premium-second-lebanon-war-success-or-failure-1.5397982

the opinions of decision makers and the public, as long as there is sufficient understanding of their views.

The situations described above further intensify the inherent challenge of assessing the intentions of an adversary: in effect, one must not only gauge his intentions, but also to evaluate them in relation to the way he himself views the reality, and today this may be subject to more biases than in the past. The traditional assessment tools that were meant to enable intimate knowledge of the enemy and his methods of making decisions are not sufficient for coping with the new challenge.

Concretely, in the "campaign between wars" in Israel's northern arena, the influences on the adversary's motivation are no less important than physical achievements in the campaign (in this case, preventing Iranian entrenchment in Syria; preventing the buildup of the Shiite axis). The most recent instances of friction in the northern arena have highlighted the intelligence challenge of clarifying the reality, and – even more so – of formulating an assessment of how things will develop.

According to the existing methodology, the analyst must examine the enemy's possible modes of operation in response to a concrete action.[7] However, the methodology does not take into account gaps in the enemy's perception of reality that could cause it to analyze the situation differently, possibly leading it to a different response. These gaps make it difficult to be able to predict the enemy's response and the overall achievements of the action with a high degree of probability.

In this article we aim to point out the main blind spots that directly influence all levels of intelligence research, with an emphasis on the "campaign between wars." We also suggest ways of addressing these points and steps to maximize the impact of operational actions on cognition.

Blind Spots that Influence the Analysis

First, *cultural and geographic gaps* between the researcher and the object of study are significant stumbling blocks in understanding the enemy and

7 Itai Brun, *Intelligence Analysis: Understanding Reality in an Era of Dramatic Changes* (Meir Amit Intelligence and Terrorism Information Center, 2018), p. 37. Brun tries to improve the work of clarifying reality in the Intelligence Corps, even though he does not refer to the reality as understood by the enemy decision makers, which affects their action.

also in understanding the reality in practice. These gaps can lead to a given situation being defined in different ways by different individuals from different societies, and, as a result, a different translation of the reality, leading to different conclusions.[8]

Second, *"everybody lies"* – in the words of Dr. Gregory House, Head of Diagnostic Medicine (played by Hugh Laurie) in the television series bearing his name. Lies often serve as a convenient haven for failures and for idealizing the reality.[9] Some representative examples of this are: a "failed launch" that is reported as a "launch that was intercepted" or a weapons delivery on its way to the enemy that is attacked, and the destroyed contents are subsequently described by the enemy as "non-sensitive goods."

Third, *it is human nature to idealize the result achieved*, as part of the self-efficacy mechanism for dealing with failures.[10] Research subjects often tend to exhibit considerable self-criticism and an expansive sense of national responsibility, but also a complete faith in the rightness of the path they have chosen. This can lead to difficulties in seeing the reality as it is and can make research subjects (as well as intelligence researchers and other actors) perceive it in a way that suits their worldview. This makes us see the reality as it is perceived by the research subjects. Thus, a "failed attack" is actually a "huge success" that the other side has chosen to hide, and an extensive attack on infrastructure is an "attack on abandoned warehouses." This does not tell us about the actual extent of the damage, but only the way the real result is processed by decision makers. Even if the research subjects are aware that the attack on them was serious, their behavior has to reflect the way they would prefer to see the reality, i.e., as an insignificant attack, thereby lessening its significance vis-à-vis the parties responsible.

---

8 Michael Milstein, "'Thou Shalt Never Change… Thou Shalt Change': The Lack of In-Depth Understanding about Objects Researched by the Intelligence Community," Meir Amit Intelligence and Terrorism Information Center, 2017, pp. 12-14.

9 Sandra L. Murray, John G. Holmes, and Dale W. Griffin, "The Benefits of Positive Illusions: Idealization and the Construction of Satisfaction in Close Relationships," *Journal of Personality and Social Psychology*, 70, no. 1 (1996): 79-98, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.584.8875&rep=rep1&type=pdf.

10 A. Bandura, "Self-Efficacy Mechanism in Human Agency," *American Psychologist* 37, no. 2 (1982): 122–47.

A fourth blind spot pertains to *narrative and false information* ("fake news"), that is, made-up information and news that are deliberately propagated in order to be considered real news, but that in fact are fabrications or distractions used as disinformation or propaganda. This is information that supports the worldviews and narrative of the decision maker. In this way, false information receives significant weight, even without being checked. This creates a situation whereby what actually happened does not matter, only how it is reflected and reinforced.

Fifth, *the "game of telephone" phenomenon*: the many ways of reporting, the interests of each of those reporting, and the accessibility that all of them have to what is happening in practice are not unlike the children's game of "telephone" – all these elements make it hard to understand the overall picture and challenge the ability to give a "reliability score" to an individual report and assess how information in the "report tree" (and the biases along the way) flows to decision makers. Even if there is no doubt that those in the field can accurately describe the scene, it is very difficult to estimate what will reach the decision makers at the end of the day.

Sixth: this blind spot is referred to as *"how things look from here."* A good leader adapts his approach to his environment and may even choose his words in a way that contradicts the reality as he himself sees it in order to motivate subordinates or to not be seen as weak. Many leaders express themselves publicly and even privately in a forceful and uncompromising manner, even if they are not interested in a confrontation.

Seventh: *intelligence-gathering biases*. In light of all of the above, access to decision makers whose view of the situation is not accurate (to say the least) "blinds" the researcher, can undermine the real picture of the situation that has been put together through intelligence-gathering efforts, and, as a result, can blur the reality entirely.

Suggested Solutions

Awareness of the different challenges enables us to provide the intelligence community with a set of research and operative tools for coping with the uncertainty and influencing the enemy's perception of reality, and analytical tools for clarifying the picture of reality:

a. *Enhancing the methodology for analyzing possible courses of action*: Along with analyzing the strategic situation according to basic assumptions in

order to reach the possible course of action, the enemy's narrative and its potential developments should be studied; similarly, the situation as it is perceived by the enemy's decision makers should be reviewed, and their expected actions should be derived from these analyses. In other words, it is necessary to consider several possible alternative responses to the response, based on different interpretations and perceptions of reality.

b. *Broad intelligence-gathering*: It is important to attempt to create as diverse an intelligence picture as possible (from tactical agents, civilians, decision makers and junior commanders), even at the expense of the "depth of penetration."
c. It is important to define *hard anchors* in the intelligence picture whose presence is undisputed (locating the "secret" that the enemy cannot deny). For example, the amount of weaponry produced is a hard anchor, even if claims are made that a larger amount has been transferred.
d. *Deeper knowledge of the enemy* and the ability to assess what will be conveyed via the "game of telephone" (that is, the narrative that each subordinate will want to portray to his commander) and how the command will be translated and transferred from the top down according to the interpretations of the various actors.
e. *When evaluating the report* it is important to take into account the proximity of the reporter to the information. For example: is he reporting firsthand or conveying someone else's report? Is he part of the inner circle? What is the report's level of detail?
f. *It is important to clarify the strategic objectives of the Israeli side*, in accordance with the operational logic.
g. It is important to make more frequent use of *control tools* to examine assessments (such as "red team," "contrary analysis," and others).

Analytical Tools for Influencing the Enemy's Consciousness

The ability to influence the enemy's perception of reality (the "narrative") is a much more complex task than analyzing the reality, and it therefore requires a dedicated response. Just as the weapons used for an attack are suited to the nature and essence of the objective, an operation to diminish the enemy's capabilities (such as preventing arms transfers) is not the same as one whose aim is to change the balance of responses, that is, an operation intended to reshape the rules of the game in a campaign. Correspondingly,

the extent of an attack does not necessarily indicate its consequences and impacts, and thus we must not draw conclusions from the demonstration of Israeli operational capabilities regarding their systemic impact on the enemy.

The "campaign between wars" concept has a significant cognitive dimension (influencing the enemy's motivation or its legitimacy to entrench, build up its forces, and use territory or arms). Thus, in a "campaign between wars," the "top down" method should be used: clarify who is meant to be influenced (and how), and derive the physical and psychological actions from this. In addition, it is important to be prepared for cognitive biases of the enemy that could influence the success of the action. In this framework, the following points warrant attention:

a. The level of *publicity* of the operation – is it aimed only at decision makers or also at the general public?
b. Defined *physical objective* of the operation – number of expected casualties, proximity to population centers, and time of the attack.
c. *Limiting the "telephone game"* by helping transmit the details of the operation to the level of the decision makers on the other side, whether by publicizing the operation or by "intervening" in the chain of reports (overt/covert publication in one of the existing tools of consciousness).
d. *Creating points of intervention and transmitting information to the enemy* in a way that reduces its plausible deniability. For example, it is possible to transmit information via message transmission channels in order to explain the objectives of our action; to publicize official statements in the media on the results of the action; or to make use of leaks to a wide variety of sources to portray a clear picture for various actors.

Even operations with only physical objectives (such as preventing the transfer of strategic weapons or reducing intelligence capabilities in the border region) have significant cognition-related aspects. Therefore, even these operations should be leveraged to harm the future motivation of the other side. At the same time, and in light of the increasing use of cognitive and psychological warfare, we should examine military intelligence gathering and research efforts to evaluate consciousness-related achievements (planned versus actual) and to carry out "performance research" on the various tools, so as to achieve their optimal utilization. Such efforts would explore the subjects of influence and the optimal ways of influencing them, assess the expected achievements of the tools versus the tasks required, analyze the

operational expectations of the tools, and recommend military buildup processes for building new cognitive tools. Such efforts should be carried out in a forum that can advantageously utilize the deep knowledge of the research subjects and the ways they are influenced, that is, familiar with the Military Intelligence Directorate's range of systems and all of the activities that take place within them, and where operational opportunities can be identified within that framework.

Conclusion

The attempt to understand the reality and influence the enemy requires understanding and internalizing the "otherness" of the other side and the limitations on our ability to read it. In addition, it is necessary to remember that behind the gleaned information stand people – individuals who have emotions and opinions and face pressures from their personal and professional environment. In-depth study of the enemy's formulations and level of consistency should be conducted; but no less vital is the need to deepen the knowledge of the enemy's life, culture, and aspirations. We must refrain from drawing on the assumptions that characterize our own culture and projecting them onto the conceptions and attitudes of the adversary, but rather search for a flexible response that adapts to emerging processes on the other side.

Influence Operations in Cyber: Characteristics and Insights

Deganit Paikowsky and Eviatar Matania[1]

Introduction

The reports on the attempts to influence the US presidential elections in 2016 through cyber activities bring to the forefront two different phenomena. The first is the expanding circle of targets threatened with cyberattacks: from the computerized systems of critical infrastructure that provide essential and tangible services to infrastructure, processes, and sectors that provide services that are less tangible but still essential to society and the state. For example, there is the possibility to penetrate computerized systems of national elections in order to change the voting results or to affect the concentration of the results, or to access the computerized systems of political parties, the media, polling companies, and even the public itself, in order to impair their functioning.

The second phenomenon is the use of the familiar type of influence operations while taking advantage of the unique characteristics of cyberspace.

1 Dr. Deganit Paikowsky specializes in policy planning and strategy in the fields of science and technology. She lectures at the Security Studies graduate program at Tel Aviv University and previously served in a senior position at the Strategy and Capacity Building Division of the Israel National Cyber Directorate. Prof. Eviatar Matania is the founder and former Director of Israel's National Cyber Directorate. He currently serves as the director of the Security Studies program and a faculty member in the School of Political Science, Government, and International Affairs at Tel Aviv University.
This article does not represent an official opinion or strategy of the State of Israel or of the Israel National Cyber Directorate but is the personal analysis and opinion of the authors.

This is done by influencing, for example, the agenda, the perception of reality, and decision making during an election campaign in order to affect the results (without directly disrupting the elections process) and/or to sow doubt regarding the integrity and credibility of the elections and of the democratic process in general. For example, true, biased, or false information can be publicized with the aim of influencing and shifting public opinion, which is then expressed in voting patterns. Another method is to repeatedly disseminate certain messages on a massive scale via social media in order to shape the discourse in a certain direction.[2] It is important to note that when relevant target audiences (decision makers and/or the public) become aware of damage caused to the functioning of computerized systems, it may influence their cognition.

This article focuses on the overlap between cyberattacks and influence operations, or in other words, cyber actions whose aims are to directly affect cognition. While these influence operations are part of much wider cyber campaigns, they are also a component of the information wars, psychological operations, and attempts to influence decision makers through an entire array of information and narratives. Since the actions described here are located between cyberattacks and cognitive influence, they will be analyzed in parallel from both directions. Thus, a cyberattack that causes physical damage with the intention of paralyzing critical infrastructure, such as electricity or water, is not addressed in this article, even though it could also have cognitive side effects. However, if a cyberattack was carried out with the aim of causing panic or undermining public confidence in the system, then it should be considered having a direct cognitive effect. Similarly, a cyberattack whose goal is to change the election results by altering the data without being noticed is not a cognitive attack.

The phenomenon of cyber influence operations is gradually gaining appeal throughout the world and will likely become more common and elaborate. Therefore, it is necessary to understand the nature of the two phenomena detailed above – of which the cognitive influence via cyber is a part – by emphasizing their shared characteristics, but also, and perhaps especially, their unique features.

---

2 David Siman-Tov, Gabi Siboni, and Gabrielle Arelle, "Cyber Threats to Democratic Processes," *Cyber, Intelligence, and Security* 1, no. 3 (2017): 51-63.

This article discusses the appeal of influence operations specifically in cyberspace and the differences between it and the familiar cyberattack. While the traditional cyberattack or cyber campaign seeks to cause tangible functional damage to the adversary, as its cognitive influence (if it even exists) is indirect, the purpose of influence operations is to harm the adversary by directly affecting cognition. Analyzing these two phenomena is especially critical for democratic states. In order to effectively prepare to defend against them, states must be aware that these are two different phenomena, despite having been placed together on the global agenda. Therefore, each one needs to be addressed differently.

Our main argument is that influence operations in cyberspace and through the use of cyber tools represent significant conceptual changes from the perspective of the cyber campaign; these operations rely on basic premises that differ from those in the familiar cyberattack, designed to impair the proper functioning of computerized systems. Effective defense against the threat of these operations requires an approach that considers the unique characteristics of this threat and its basic premises. Furthermore, it also demands comprehensive national preparedness and cooperation among a variety of bodies, of which cyber defense organizations are only a part.

The first part of the article analyzes the general characteristics of influence operations, including those in cyberspace. It also discusses the human and social characteristics upon which these operations are built. The second part focuses on the specific contribution of social media in making these operations appealing. The third part addresses the expanding targets of the cyber threats and specifically the similarities and differences between cyber actions designed to cause functional damage and those aimed at influencing cognition, which together constitute all cyber threats. The article concludes with initial insights that address the gaps identified in dealing with the challenges of the battle for cognition in cyberspace and the need to develop a comprehensive approach in order to effectively cope with influence operations.

A Strategy of Influencing Cognition

Influencing cognition is the ability to change and/or shape the conceptions of a person or a group of people, and as a result, to disrupt and/or change their behavior, decisions, and capabilities. This occurs by adding or removing topics

within the public agenda and biasing the discourse on them.[3] Influencing cognition is based on a number of social and human characteristics. The first is human difficulty in distinguishing between true and false information, and in reconstructing what was true and false. The second characteristic is the inclination to take shortcuts in assessing the credibility of messages in the context of information overload. A third characteristic is the tendency of people to accept information that suits their worldview, even if it is false, and to accept and believe declarations and claims presumably supported by facts, even if they are false. For example, a display of objectivity strengthens the credibility of a propaganda statement when it is published on a news site.

An influence operation is an old, well-known method that aims to serve various political, military, economic, and social objectives. At the state level, influence operations seek to achieve their objectives by harming personal and economic security, undermining public confidence and support for state institutions, and damaging social solidarity. The means of achieving these objectives include actively intervening systems and processes, or using various kinds of leverage (economic and other) in order to prompt or prevent actions, and acquiring and using information in order to create and disseminate messages and cause them to reverberate so that they achieve the maximum effect. The channels for conveying messages are the traditional media (newspapers, radio, and television) as well as the new media; that is, the internet and its various applications, such as the social networks. Opinion leaders sometimes serve as "unaware agents" for strengthening the credibility of messages and widening their distribution.[4]

A strategy of influence operations is generally part of a holistic approach using multiple channels and means, sometimes referred to as "information warfare." This strategy aims to maneuver actors into behaving in a desired way, sometimes against their interests, in part, by distorting and influencing their picture of reality and exerting various kinds of leverage. These actions

3 Karine Nahon and Shira Rivnai Bahir, "Election Propaganda in the Context of the Internet and Social Media: Background Information for the Beinisch Committee," January 2016 [in Hebrew].

4 Ron Schleifer, "Psychological Warfare in Operation Cast Lead," *Maarachot* 43 (August 2010): 19-20 [in Hebrew].

are carried out toward decision makers and populations of adversaries and allies, during both peace and wartime.[5]

Recently, influence operations have intensified through the use of cyberspace. Cyberspace provides the foundations and the tools – both legitimate and illegitimate – to carry out these operations. To this end, information from computerized systems and databases is being used, even if only partly. According to reports from the US Director of National Intelligence (DNI), which assesses global threats, the United States considers influence operations, especially the cyber ones, to be a significant threat, whose scope, intensity, and importance are increasing.[6]

The Appeal of Influence Operations in Cyberspace and Social Media

The threat of cyber influence operations has intensified and increased as cyberspace, and especially the various social media applications, provide technological platforms and new tools to carry out these operations with unprecedented speed and power. Thanks to cyberspace, various targets for the purpose of gathering and disseminating information have become easily accessible, conveniently available, and fast, all at a relatively low cost.

---

5 Dima Adamsky, "Cyber Operative Art: A Look from the Viewpoint of Strategic Studies and in Comparative Perspective," *Eshtonot* 11 (August 2015): 28-48 [in Hebrew].

6 Daniel R. Coats, Director of National Intelligence, "Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, May 11, 2017; James, R. Clapper, Director of National Intelligence, "Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community," Senate Armed Services Committee, February 9, 2016; James, R. Clapper, Director of National Intelligence, "Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community," Senate Armed Services Committee, February 26, 2015; James, R. Clapper, Director of National Intelligence, "Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, January 29, 2014; James, R. Clapper, Director of National Intelligence, "Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, March 12, 2013; James, R. Clapper, Director of National Intelligence, "Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, February 10, 2011.

From the attacker's perspective, conducting cyber influence operations is appealing because political achievements can be gained effectively and at a significantly lower cost than by using traditional tools (the most extreme being the use of military force). In addition, the ongoing paradigmatic change in how wars have been waged in recent decades has sometimes led to a preference for actions in cyber rather than on other levels, especially in terms of direct military conflict.[7]

Today, social media plays a central role in carrying out influence operations, serving as central "battlefields," as well as effective offensive channels for conducting influence operations.[8] There are several reasons for this. First, the number of people who use social media to consume information and directly interact at any place and time has grown exponentially in recent years.[9] In addition, the dissemination of information on social media occurs quickly within and between groups. Sometimes the spread of information happens so fast that it is difficult – if not impossible – to stop the process, known as the "virality of information flow."[10] The technological architecture of social networks, which aims to manage the flow of information by filtering excess information and exposing users to personalized information, is a significant component of the appeal of social networks as a platform for implementing influence operations.[11] The exposure of social media users only to a small portion of all the information on the internet helps – even if unintentionally – to streamline influence operations, as it magnifies certain content and narrows the focus on them.[12]

Another factor that can work in favor of influence operations is the ability of social media users to create and disseminate information and engage

---

7 For more on these processes, see Ned Lebow, *Why Nations Fight* (New York: Cambridge University Press, 2010).

8 Social media includes platforms such as Facebook, WhatsApp, Instagram, LinkedIn, and Twitter.

9 In 2010, the number of social media users in the world was 0.97 billion, while in 2017 it had already reached 2.62 billion users. See https://bit.ly/2gRTQQk.

10 Karine Nahon and Jeff Hemsley, *Going Viral* (Cambridge: Polity Press, 2013).

11 In order to create a browsing experience that matches the worldview of its users, the platform learns the areas of interest and habits of its users, sometimes interfacing with information from other platforms.

12 Nahon and Rivnai Bahir, "Election Propaganda in the Context of the Internet and Social Media."

in direct, unmediated interactions with others, thus creating an illusion of pluralism, even if the situation is fundamentally different. In influence operations, attackers make use of fake accounts, such as bots or avatars, in order to affect the public agenda and create the impression that public opinion is leaning in a certain direction. The more aware the public becomes of the existence of influence operations on social media, the more critical it will be, thus reducing the effectiveness of these actions.[13]

Cyber Threats of Functional Damage and Cognitive Harm

Although cyber threats that focus on harming functional and cognitive aspects differ from each other, at the same time, both have a number of shared characteristics. Thus, functional damage can cause significant cognitive harm, which, in certain cases, can be greater than the functional damage itself, and therefore can be the main incentive for the attack. For example, a power outage in a large city that lasts a few hours and is discovered by the public to be the result of an intentional attack by an adversary presumably will create panic, fear, uncertainty, and insecurity; that is, the attack will cause much greater cognitive harm than the direct functional damage that occurs due to the lack of electricity for a few hours.

In both threats, the potential circle of people under attack also is increasing. Until recently, cyber campaigns have been characterized as focusing mainly on functional damage to military targets or civilian ones, which constitute the critical infrastructure that enable the society or economy to truly function. Damaging these targets constitutes a severe attack on national security and/or the economic resilience of the side under attack. Meanwhile, in recent years, we have witnessed actions designed to cause functional damage in cyberspace, which is also directed toward social and essential systems and processes, and to a large extent, influence operations are directed toward these systems and processes as well. In other words, the changing battle in cyberspace can be described whereby the entire environment of the side under attack – the physical infrastructure, tangible assets (such as knowledge or secrets), and intangible ones (such as reputation or confidence) – is now the target of the action, whether its objective is functional damage or cognitive influence. In terms of both threats and in the context of attacks on systems

13 Ibid., p. 4.

that are not essential physical infrastructure, it is difficult to estimate the enormity of the threat and to accurately assess the damage and/or to employ the usual measures of economic damage or loss of human life.

Expanding the circle of people who are attacked points to another shared characteristic of both threats, and that is the tension that arises in a situation in which a democratic regime – based on the principles of freedom of expression, a free press, the right to privacy, and the separation of powers – seeks to defend the main institutions and processes of democracy against these threats described above (functional damage or cognitive influence). In order to ensure that the defense mechanisms against these two threats are not abused, democratic regimes must establish a system of checks and balances to reduce the risks to democracy.

The two threats also have several fundamental differences. They have different objectives (expected achievements), although both threats rely on gathering information, disrupting information, or thwarting information.[14] Damage to information is classified according to three main categories (also known as the CIA model): Confidentiality of Data, Integrity of Data, and Availability of Data. Table 1 shows the differences between functional and cognitive attacks in terms of damage to data.

Offensive cyber actions with a functional objective occur with unauthorized penetration of computerized systems by using hostile code. In addition, unauthorized penetration takes place in order to send a message to an adversary or to gather information. In terms of influence operations, manipulation of the adversary's cognition occurs by transmitting, preventing, or disrupting information, for example, by publicizing false information or leaking confidential information, and can be referred to as using hostile content. These actions are sometimes accompanied by unauthorized penetration of computerized systems, but this is not necessary, and many information or influence operations do not require this.

14 For the sake of simplicity, here we are presenting the differences between functional damage and cognitive harm to information only, and ignoring cyberattacks against physical systems that are not information systems, such as generators and electrical systems.

Table 1: Classification of Unauthorized Penetrations of Computer Systems

Types of Damage	The Essence of the Action	
	Functional objective	**Cognitive objective**
Damage to the confidentiality of information	Gathering information to produce military/civilian/ commercial intelligence	Exposing and publicizing confidential information, for example, leaking or threatening to leak embarrassing information
Damage to the integrity of information	Disrupting and changing data in order to cause physical damage or in order to disrupt the situational awareness	Biasing information and/ or planting biased or false information and publicizing it in order to disrupt the situational awareness and sense of reality
Damage to the availability of information	Denial of access to information or disrupting/removing it	Denial of the ability to publicize/disseminate information, for example, blocking platforms where communication and the messages of a political party or candidate are transmitted during an election campaign, in order to prevent the transmission of the messages

Two main types of action make use of hostile content (Table 2). One uses hostile content alone, without malicious penetration of computer systems, for example by leaking information, using avatars in order to place issues on the agenda, slanting the discourse in directions that match the interests of the attacker, inciting terrorism, disseminating rumors, or inciting fear. The other action combines the use of hostile code and hostile content; that is, in order to achieve the objective, unauthorized penetration of information systems occurs, although it is only a means to manipulate the information. Some examples of this include unauthorized penetration of the information systems of polling companies in order to bias the results, thus providing the public with erroneous interpretations of the trends on an issue being polled; stealing information in order to leak it; unauthorized access of mailing lists so that hostile messages can be transmitted; and penetration of mass media systems and/or internet platforms for communicating with the population under attack (website and social media accounts) in order to cause damage, cease activities, disrupt information, and disseminate false information.

Table 2: Influence Using Hostile Code and/or Hostile Content

Damage to computerized infrastructure	**Damage to computerized infrastructure combined with disseminating information**	**Disseminating information in the digital realm; publicizing false information**
• Damage to critical infrastructure • Damage to essential infrastructure • Gathering information in order to carry out operations • "Sending a message" by penetrating systems	• Biasing public opinion polls • Stealing information in order to leak and publicize it • Accessing mailing lists for the purpose of disseminating messages and deception • Penetrating mass media to plant information or disrupt/damage websites	• Leaking information • Using avatars for social media campaigns • Inciting and encouraging terrorism on the internet • Spreading rumors and inciting fear

Hostile code — **Hostile code and hostile content** — **Hostile content**

Another characteristic that partly distinguishes influence operations from that of cyberattacks causing functional damage relates to the level of secrecy. The effectiveness of influence operations increases to the extent that the malicious actions and the existence of a "guiding hand" behind them are unknown. The cost of exposure in such a case can be high, to the effect of harming the purpose of the entire influence operation. Therefore, covert activities that are under the radar, in the form of a "no-logo" strategy, are almost always preferred. Cyberattacks intended to cause functional damage to computer systems or to disrupt information are also sometimes carried out covertly in order not to reveal the way they were implemented or in order to avoid taking public responsibility. But when these cyberattacks damage the functioning of computer systems, they become a known occurrence.

Conclusion: Implications for Democratic States

In this article, we have focused on the distinction between cyberattacks that aim to damage the functioning of computerized systems, which almost always involve unauthorized penetration of these systems, and influence operations, which do not necessarily make use of unauthorized penetration. It is important to note and understand that this distinction is mainly the product of a cultural-democratic approach that accepts the rules of the game of Western democracies, according to which it is wrong and illegal to penetrate computer systems of others (rooted in conceptions, norms, and

legislation). Therefore, this approach sees any action against the functioning of computer systems as an aggressive act that requires defense using various means – legal, police, or military. An output of this democratic approach is the serious concern about intervention in content, narratives, and the media in general given the preference of allowing almost entirely free expression as part of the democratic process. As a result, democratic regimes are quite perplexed regarding the right way to prevent or reduce influence operations and to defend against them, as a result of the concern about government involvement in the media and democratic elections.

Effective defense against cyber influence operations needs to take place vis-à-vis the entire phenomenon of cyberattacks and their threats in the understanding that the attacker does not necessarily distinguish between the two kinds of cyberattacks. As a result, the subjective distinction that exists when looking at this from a democratic perspective poses a serious challenge for the democratic defender: How should a comprehensive, systemic national policy be developed that will consider the various relevant fields for dealing with influence operations and will integrate forces from the various bodies responsible for different aspects of the threats and the responses to them? At the same time, it is necessary to maintain cyberspace as an open space that enables the free flow of knowledge and services and where basic rights are protected, including the rights to freedom of expression and to privacy. These are difficult challenges and dilemmas that democratic states are facing. Non-democratic states, which do not address these issues, find it easier to formulate a systemic defense concept that does not distinguish between actions with a functional objective and those aimed at a cognitive-related objective, either at the conceptual, organizational, or operational levels.

Based on these insights, we believe that from the democratic perspective, a central part of addressing the challenge posed by the phenomenon of cyber influence operations is identifying and mapping all the parties whose involvement is necessary for obtaining effective defense, as well as the interfaces between them. This includes intelligence for identification, prevention, and deterrence; cyber technology for countering actions comprised of unauthorized penetration of computer systems; legislation and enforcement for coping with incitement and the dissemination of hostile content; public diplomacy for neutralizing the influence of hostile content and for raising awareness; and education for a critical perspective toward content on the

internet. It is also worth examining the possibility of utilizing existing knowledge and capabilities in academia and in the private market to this end.

The question of the role of national cyber security agencies in addressing cyber influence operations needs to be asked. In other words, in addition to their responsibility of defending the national or civilian cyberspace against attacks that penetrate computer systems, why not give them the responsibility for defending against cognitive operations? They are seemingly the natural agencies for these activities, since, as emphasized above, attackers do not usually distinguish between penetrating computer systems – an area that cyber security agencies are responsible for defending against – and influence operations. If so, why not expand the responsibility of these defense agencies to include this natural task?

In our view, the answer lies in two fundamental reasons relating to the nature of these security organizations. Firstly, in many countries, the cyber defense agencies are part of the military or the police. Giving them responsibility for defending against hostile content – and not just hostile penetration – contradicts the balances that exist in democratic regimes. It would thus be a mistake to assign them with this responsibility of probing media organizations, taking an interest in their content, and making decisions about it. Secondly, even in countries where cyber defense agencies are not part of the military or the police, such as the Israel National Cyber Directorate, there is a good reason not to connect these two. In countries characterized as democratic, these organizations require that the civilian sectors place great trust in them; only a high level of trust between a government agency and private organizations will enable government security agency to access information, analyze it from a national perspective, and work with the private organizations on their "turf." This trust is a fundamental component of the ability of government security agencies to defend civilian cyberspace. Without it, regardless of the powers the defense agency has, it will not be able to fulfill this responsibility. Achieving such trust is based, first and foremost, on cyber security agencies having a disinterest in content and showing concern only in defending against the penetration of computerized systems. This trust could be severely undermined if security agencies take positions and make decisions regarding content.

These reasons and explanations lead to the conclusion that existing cyber security agencies should not be tasked with handling the defense

against influence operations. Nonetheless, cyber security agencies must not be excluded from the overall national system-wide effort to cope with the threat of such operations.

The tension between the need to defend against influence operations and the need and obligation to maintain basic civil rights highlights the importance of the public discussion on the question of "what are the rules of the game," or in other words, what is prohibited influence and which tools and methods are illegitimate. Thus, an effort should be made to expand the discussion on the issues that will help define the boundaries of legitimacy of influence activities. This includes (but is not limited to):

a. Defining boundaries of the legitimacy of activities aimed at the masses, which seek to create cognitive influence, for example, activities through networks of bots.[15]
b. Defining boundaries of the legitimacy in harming essential and important bodies and processes to society and the state through actions in cyberspace.
c. Defining boundaries regarding the legitimacy of the involvement of defense agencies against actions that combine hostile code and content, including the ability to contend with situations of unauthorized penetration of computerized information systems in essential and important bodies or processes of the state and society. An example is dealing with the abuse of unclassified information attained by unauthorized penetration of computerized information systems.
d. Examining the possibility of developing national and international mechanisms that provide a framework for action and define the responsibility of the companies operating social networks, in the face of threats.[16] This should relate to the architecture of gathering information on users, the flow and filtering of information to them, and the virality in transmitting messages.

Another important issue for effectively coping with influence operations relates to the public's confidence in state institutions. Influence operations

15 For example, in an article published in the *New York Times* on July 15, 2017, under the headline "Please Prove You're not a Robot," researcher Tim Wu from Columbia University suggested defining botnets as "enemies of humanity," similar to pirates.

16 Tim Wu argued in his opinion piece that in the absence of an economic incentive for companies operating social networks, it is difficult to cope with the problem of botnets.

aim in part to harm social stability and undermine public confidence in state institutions and systems. Thus, a high level of public confidence in the party against which hostile content is used is essential to be able to cope with an influence operation effectively.[17] We must invest in finding ways to strengthen and consolidate trust between the public and the various state institutions. From the perspective of the cyber defense organization, one way is to cultivate a continuous and direct connection with the public and to promise that in times of crisis the reliability of computerized systems and their information will be quickly verified, and this will be shared with the public.[18]

In conclusion, the phenomenon of influence operations has become a common pattern of action and significantly threatens the ability of states to make decisions independently. Defense preparations as part of the cyber campaign have so far focused mainly on defending against functional damage. The intensified use of influence operations requires that the unique characteristics of this type of activity is addressed, while ensuring the openness and freedom of cyberspace and the upholding of basic civil rights.

17 For example, Ron Schleifer argues that "an effective medium that Hamas used in Operation Cast Lead was spreading rumors. Among others, it spread rumors regarding the number of IDF casualties, but since the IDF Spokesperson enjoys a high level of credibility, these false rumors did not cause damage." See Schleifer, "Psychological Warfare in Operation Cast Lead," p. 22.

18 Rand Waltzman, "The Weaponization of Information – The Need for Cognitive Security," Testimony presented before the Senate Armed Services Committee, Subcommittee on Cybersecurity, Rand Corporation, April 27, 2017, p. 6.

Part III

Global Dimensions

Russia as an Information Superpower

Vera Michlin-Shapir, David Siman-Tov, and Nufar Shaashua[1]

In recent years, there has been much research and political attention directed to the campaign to influence cognition through the manipulation of content, especially in light of the accelerated development of information technologies.[2] This article looks at Russia, which has drawn considerable attention as a case study of political media influence operations. The article reviews conceptual, organizational, and operational aspects (principles, methods, tools, and modus operandi), while emphasizing the element of content. In addition, it explores several recent proven instances that included Russian influence efforts, and draws patterns that characterize Russia's action in this field.

Literature Review

Since 2008, the Russian regime has invested considerable efforts in rebuilding Russia's military capabilities.[3] However, aware of the ongoing

1 Dr. Vera Michlin-Shapir is a researcher on Russia at INSS, David Siman-Tov is a researcher on intelligence, cyber challenges, and cognitive warfare at INSS, and Nufar Shaashua is a former intern at INSS.

2 See the INSS publications on this topic: Zvi Magen, "The Battle over Consciousness," in *The Delegitimization Phenomenon: Challenges and Responses*, eds. Einav Yogev and Gallia Lindenstrauss, Memorandum No. 164 (Tel Aviv: Institute for National Security Studies, 2017), pp. 93-98; Yotam Rosner and David Siman-Tov, "Russian Intervention in the US Presidential Elections: The New Threat of Cognitive Subversion," *INSS Insight* No. 1031, March 8, 2018; Gabi Siboni and Gal Perl Finkel, "The IDF's Cognitive Effort: Supplementing the Kinetic Effort," *INSS Insight* No. 1028, March 1, 2018.

3 Scott Boston, Michael Johnson, Nathan Beauchamp-Mustafaga, and Yvonne K. Crane, *Assessing the Conventional Force Imbalance in Europe: Implications for*

gap between Russia's conventional capabilities and those of the "collective West" (NATO in general and the United States in particular), it invests considerable resources in an attempt to develop tools and methods that offset its inferiority. These include asymmetric measures, including a doctrine on the use of non-military means. In effect, this is a doctrine based on the indirect warfare approach, which has existed since the days of the Soviet Union.[4] According to this doctrine, one must consistently look for the enemy's weak points and attack them by means of fast, constant maneuvering, in order to surprise the enemy. Against this background, the Kremlin has exploited the sense of crisis in the West, the increasing opposition to globalization, and the rise of nationalism, populism, and ultra-nationalism, and looked for weak links, in the hope of identifying tensions between Western countries and rifts within the respective societies. Attacking these tensions and rifts is meant to undermine intergovernmental organizations, such as NATO and the European Union, which are seen by Russia as a threat, as well as the institutions and societies of specific countries, such as Ukraine or Germany.

Russia has adapted its traditional approaches to the current era, which is shaped heavily by economic, geopolitical, and technological processes of globalization that blur international borders, both physically (the movement of goods, capital, and people) and technologically (the flow of information and knowledge). Within this framework, Russia has also adapted its historic Soviet doctrine of indirect warfare to the information age, and plays with new tools and according to new rules of the game, in order to fulfill both novel and traditional objectives.

According to published Russian doctrines, activity in the information realm is an integral part of regular governmental activity.[5] The "information struggle" is defined in Russian Defense Ministry documents in the following manner:

> A struggle between two or more countries in the information realm with the aim of damaging information systems, processes,

---

Countering Russian Local Superiority (Santa Monica, CA: RAND Corp., 2018), http://bit.ly/2U6AFoY.

4 Ulrik Franke, *War by Non-Military Means, Understanding Russian Information Warfare* (Stockholm: Totalförsvarets Forskningsinstitut – FOI, 2015).

5 Ibid.

> or resources, critical or other infrastructure, in order to undermine political, economic, and social systems, undermine the society and state by massive psychological influence of the public, and place pressure on the [attacked] state to make decisions that suit the interests of the attacker…it shall be used before using other means in order to achieve the state's objectives without the use of kinetic force, and in order to positively influence the reaction of the international system if and when the struggle becomes conventional.[6]

Sergey Chekinov and Sergey Bogdanov, former senior officers in the Russian army, note that one of the main advantages of activity in this realm of warfare is the ability to deny it, thanks to the nature of the technological and communications network, in which one can operate covertly and with a small footprint, and the relative difficulty of proving the identity of the attacker, unless he/it chooses to reveal himself.[7]

The strategic and academic discourse in the West refers extensively to Russian activity in the information realm, including political influence operations. Many researchers connect Russian activity in the field of cognition with what is called the "hybrid warfare doctrine" or "new generation warfare." Their studies often refer in part to a speech by General Valery Gerasimov, Chief of the General Staff of the Armed Forces of Russia, who in 2013 referred to the "new kind of warfare" as warfare based on the understanding that in the age of digital communication, the human brain increasingly becomes the battlefield of the future. As a result, he believes that the focus should be on human cognition, making the use of kinetic means only one part of the overall struggle.[8]

The "hybrid warfare doctrine," as it is described in the West, includes a combination of psychological measures and electronic and cyber warfare in a comprehensive systemic attempt that becomes a force multiplier to ensure

---

6 "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space," Ministry of Defense of the Russian Federation, 2011 [in Russian].

7 Sergey G. Chekinov and Sergey A. Bogdanov, "The Nature and Content of a New-Generation War," *Military Thought* 4 (2013): 12-23.

8 V. Gerasimov, "The Value of Science in Forecasting," V*oenno Promyshlennyi Kur'e*r 8, no. 476 (2013) [in Russian].

victory in a future war. The information struggle takes place in wartime, during phases of conflict escalation, and during times of peace, and continues regardless of the nature of the relations between the countries.[9]

Researcher Mark Galeotti noted that researchers in the West need to rethink whether the Russian information warfare in reality bears the characteristics of a formal doctrine.[10] Another researcher, Keir Giles, claims that the current Russian approach to information warfare is not new, but is based on Russian military thinking since the Second World War and the Cold War. In his opinion, this is an adaptation of traditional Soviet doctrines of warfare and political subversion (known as active measures) to the current era. Giles claims that the Kremlin sees information simultaneously as a tool, a means, a goal, and a theater of operation, and thus its activity in this sphere relates both to processing digital information and to processing information in the human brain.[11]

We agree with Galeotti and Giles and believe that Russia's activity is not necessarily part of a formal doctrine, but rather an adaptation of traditional methods of action to the era of digital communication and information. In our opinion, this approach allows for better understanding of Russian modus operandi in the field of cognition and national security.

Russia's Cognitive Operations in Various Arenas

There are several geographical arenas in which Russia conducts campaigns to influence political cognition: the internal Russian arena, the arena of the Commonwealth of Independent States, the Western arena (which also includes the East European countries that have joined the European Union and NATO), and the arena of the Middle East and Africa (not addressed in this article).[12] As a rule, in these arenas Russia works to achieve several overarching objectives in the field of cognition: maintaining its own regime

9 Keir Giles, *Handbook of Russian Information Warfare* (NATO Defense College, Research Division, 2016).

10 Mark Galeotti, "I'm Sorry for Creating the 'Gerasimov Doctrine,'" *Foreign Policy*, March 5, 2018.

11 Giles, *Handbook of Russian Information Warfare*.

12 The RAND Corporation made a similar division into arenas: Todd C. Helmus, Elizabeth Bodine-Baron, and Andrew Radin, *Russian Social Media Influence* (Santa Monica, CA: RAND Corp., 2018), http://bit.ly/2SWcw7S.

stability; influencing the policies of foreign governments in ways that benefit Russian interests as they are perceived by the Kremlin; and undermining citizens' trust and confidence in government leaders and institutions in target countries, in order to harm the legitimacy of liberal democracy and disrupt relations between target countries and third countries.[13] The Russian regime conducts cognitive campaigns with different messages and tools that are tailored to each arena.

Early in the 21st century, the regime decided to manage Russia's domestic political arena as a cognition theater, and has continued this approach ever since. In this framework, the Kremlin retook control of Russian media networks that were privatized and those established in the 1990s, and began to use them to convey self-serving political messages. There are three significant interests that the regime seeks to advance and thereby also advance its interests in other arenas: maintaining Putin's rule; strengthening the state's control over internal affairs, dubbed "sovereign democracy" (or as it is called in the West, an "illiberal democracy"); and demonstrating its great power status in the external arena. This is often achieved by weakening and denigrating (by disseminating negative, embarrassing, or false information, often known in Russian as *kompromat*) opposition figures who advance liberal ideas or other notions that challenge the regime (e.g., nationalist extremists).[14]

Russia's main interest regarding the former Soviet Union is to maintain the Russian sphere of political and economic influence and retain the rule of pro-Russian elites who do not challenge the Russian form of government. The Color Revolutions in Georgia (2003) and Ukraine (2004) challenged the Russian regime with the loss of political-economic influence, the penetration of liberal ideas into the post-Soviet political sphere, and the possibility of undermining the "sovereign democracy"; they were also a military threat vis-à-vis the expansion of NATO. In these countries, the Kremlin fosters relations with Russian-speaking communities, which are considered supportive of Russia. Sometimes, cognitive influence over these groups occurs in part

13 Pynnöniemi Patri and András Rácz, "Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine," FIIA Report 45 (2016).

14 For further reading on the topic of the use of denigration measures in the Russian arena, which is considered a very common tool and not only by the regime, see Alina V. Ledeneva, *How Russia Really Works? The Informal Practices that Shaped Post-Soviet Politics and Business* (Ithaca: Cornell University Press, 2006).

by fanning the flames of tensions between Russian speakers and the general population, which is considered more critical of Russia.[15] Other times, this occurs by weakening confidence in government institutions and leaders in those countries in order to cast doubt on democratization processes underway and liberal ideology in general, and to undermine the relations between these countries and Western countries and intergovernmental organizations.

The Kremlin has three main interests in relation to the West. First, it seeks to demonstrate Russia's strength as a great power in the ongoing power struggle with the West in general and with the United States in particular. In other words, Russia seeks parity with the West and resists what is seen by the Kremlin as American subversion in Russia's internal arena aimed at toppling the regime. Second, it seeks to undermine the foundations of the European Union and weaken the NATO alliance, whose spread eastward is seen by Russia as a military threat; and third, it aims to erode democratic institutions and mechanisms in the West by exploiting the structural weaknesses of capitalism and democracy.[16] In these countries, Russia fosters relations with political groups that challenge liberal-democratic regimes (such as extreme right wing groups, religious groups, or even extreme leftist groups) and uses their assistance to change the public's cognition and undermine citizens' confidence in state institutions and in the democratic system. In addition, Russia attempts to undermine the relations between NATO and European Union states and Western intergovernmental institutions.

The Russian "Information Community"

The cognitive campaign that Russia wages internally and externally includes overt and covert efforts in the traditional and new media (social media); they involve content attacks, as well as technological attacks. Russia's activity in these spheres is carried out by a variety of official, semi-official, and unofficial actors, which side by side make up the "information community." This community can be divided into two main spheres: the military sphere (including Military Intelligence – GRU, the Federal Security Service – FSB,

15 Helmus, Bodine-Baron, and Radin, *Russian Social Media Influence*.

16 William C. Wohlforth and Vladislav M. Zubok, "An Abiding Antagonism: Realism, Idealism, and the Mirage of Western-Russian Partnership after the Cold War," *International Politics* (2017): 1-15.

and the Foreign Intelligence Service – SVR), and the governmental-civilian sphere.

The Military Sphere

In 2012, the Russian Ministry of Defense published its "Cybernetic Strategy."[17] The new strategy, which was approved by President Putin, expands the powers of Russia's security and intelligence organizations in cyberspace. In 2008, after the war with Georgia, Russia's military intelligence became the last of the organizations to join the Russian information community. At that time, as part of changes to Russian operational doctrines, the Russian Defense Minister made initial attempts to integrate the field of information warfare within military activity and to create military departments that would carry out attacks to accompany military actions.

In 2013, the Russian government announced the establishment of information units in the Russian army, which would include hackers, journalists, media strategists, psychological operations experts, and linguists. The emphasis was placed on language skills, to create the ability to communicate with large and diverse target audiences.[18] These units seem to have begun operating between 2013 and 2017. In February 2017, Russian Defense Minister Sergey Shoygu announced that a propaganda department had been established within the army, which would join the information operations division.[19]

The organizations that make up the "military sphere" use diverse media to achieve cognition-related objectives. The most basic tool is the human communication group in Russia and in the target countries. This group includes ordinary people, "concerned citizens," experts, statesmen, and celebrities, who are interviewed and refute Western messages or, alternatively, support Russian narratives. This framework likewise activates pro-Russian organizations, pro-Russian parties, activists, and lobbyists. When the Russians

---

17 "Conceptual Outlooks on the Activity of the Armed Forces of the Russian Federation in the Information Sphere," Ministersvo Oborony Rossiyskoy Federatsii, 2011 [in Russian]; Oren Dotan, "Cyber Bullying: How Russia Uses Hackers and Broadcasts Global Cyberattacks," *Walla*, July 21, 2016, http://bit.ly/2TdF6kB [in Hebrew].

18 Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare* (Arlington: Center for Naval Analyses, 2017).

19 Demian Sharkov, "Russia Announces 'Information Operations' Troops with 'Counter-Propaganda' Remit," *Newsweek*, February 22, 2017, http://bit.ly/2GXQpXM.

operate in countries that are home to communities of Russian immigrants (for example, Germany), they try to galvanize these communities as part of the information struggle, and do so by spreading rumors in the local community.

Social media has also become a very important tool in the hands of the military sphere of Russia's information community. At a relatively early stage, Russia adopted advanced technological tools toward these objectives, and unlike most Western countries, which are cautious about using such tools − as their activity could be seen as undemocratic and because their impact is unclear − has learned through trial and error how to use them and utilize them extensively against strategic targets.[20] Keir Giles estimates that inter alia the Russian army's propaganda unit carries out psychological and influence operations in traditional and new and online media – social networks, the press, and other media.[21]

Reports by many security companies in the world point to signs on the internet starting in 2013, that indicate the activity of a unit identified as belonging to GRU, known in the West as APT28 (Advanced Persistent Threat) or "Fancy Bear." According to these reports, APT28 focuses on foreign security agencies and government ministries.[22] For example, it attacked the Georgian Foreign Ministry and its footprint was clearly identified.

During the US presidential election race in 2016, American researchers identified another group also belonging to Russian military intelligence – APT29 – which is known as "Cozy Bear."[23] The indictment by special prosecutor Robert Mueller, who was appointed to investigate Russia's intervention in the US presidential elections, revealed that these groups belong to units 26165 (the cyberwarfare unit) and 74455 of GRU, and described in detail their practices and their synergetic use of three spheres

---

20 Timothy Thomas, "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?" *Journal of Slavic Military Studies* 27, no. 1 (2014): 101-30; Giles, *Handbook of Russian Information Warfare*.

21 Keir Giles, *Russia's 'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power* (Chatham House, Russia and Eurasia Programme, 2016).

22 "APT28: A Window into Russia's Cyber Espionage Operations?" *FireEye, Inc*., 2014; Eric Lipton, David Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *New York Times*, December 13, 2016.

23 Connell and Vogler, *Russia's Approach to Cyber Warfare*.

– technological (hacking), psychological (exposing information via third party sites and fictional identities), and espionage-related (collecting sensitive information on official figures).[24]

It was reported recently that GRU (together with FSB), funds and operates "cadet classes" at public schools in Moscow, whose purpose is to foster and improve the mathematical and technological skills of potential recruits.[25] Within this framework, unit 25165, mentioned in Mueller's indictment, developed a curriculum at several public schools over the past few years. In addition, it was revealed that there are a number of leading organizations that operate under unit 54777, responsible for psychological warfare in the Russian army, that are officially funded by government grants, but covertly run by the GRU. Two of the most important organizations that operate under this unit are the InfoRos news agency and the Russian Diaspora Institute.

The Governmental Sphere and the Civilian Sphere

The governmental sphere of the Russian information community consists of governmental bodies and private companies that are recruited both overtly and covertly by the government and security organizations. Actors are mainly active in the cognitive-psychological sphere (cognitive operations), and sometimes also in the technological sphere (cyberattacks). The private companies that are part of this sphere include the Internet Research Agency, which is connected to the regime but is not part of the chain of command of military and governmental bodies. According to the US Justice Department indictments and a detailed report submitted to the Senate, this company conducted an extensive cognitive operation to influence internal politics in the United States.[26]

---

24 United States of America v. Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin and co., Criminal No. (18 U.S.C. §§ 2, 371, 1030, 1028A, 1956, and 3551 et seq.), July 13, 2018, US Department of Justice Website, http://bit.ly/2XjTtmJ.

25 A. Troianovski and E. Nakashima, "How Russia's Military Intelligence Agency Became the Covert Muscle in Putin's Duels with the West, *Washington Post*, December 28, 2018.

26 United States of America v. Internet Research Agency LLC and Co., Criminal No. (18 U.S.C. §§ 2, 371, 1349, 1028A), February 16, 2018, US Department of Justice Website, http://bit.ly/2NoIL9M; Philip N. Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François, *The IRA, Social Media, and Political Polarization*

In addition, "hacktivists" work within Russia's governmental and civilian sphere – hackers who carry out relatively complex offensive actions, along with patriotic pro-Russian civilians, who volunteer to advance Russia's national interests when the goal of the activity is compatible with their worldview. It is not clear to what extent the hacktivists can be effective in influence operations without assistance from the state. For example, the attack on the internet in Estonia (2007), which occurred during a diplomatic and cognitive struggle that Russia conducted against the intention of the Estonian authorities to remove the "bronze soldier" statue in memory of the Soviet soldiers during the Second World War, was attributed at a certain stage to "activists" from the Nashi (Ours!) youth movement, who claimed responsibility for the event. The Estonian government did not accept this version and claimed that the attack was complex and carried out by the Russian government, and that the involvement of the hacktivists in it was apparently marginal.[27]

These actors also used online and new media, and the Justice Department indictments identified the Internet Research Agency's use of trolls and bots.[28] "Bots" are artificial digital entities that collect information and carry out activities on the internet by imitating human users. The use of bots on the internet takes place in social media, blogs, forums, and internet communities. "Trolls" are people who operate and manage fake profiles on the internet (also via blogs, social media, forums, and so on). Each troll can maintain several profiles and several digital identities. The trolls that the Russians operate write comments on anti-Russian news sites and articles, maintain pro-Russian blogs, report on anti-Russian statuses and videos on YouTube and social networks, flood these networks with posts supportive of Russia, and in addition respond to anti-Russian posts in order to shift the discussion to one that suits the Russian narrative. The purpose of the use of bots is to

---

in the United States, 2012-2018 (University of Oxford, Project on Computational Propaganda, 2018); "The Disinformation Report," New Knowledge, December 17, 2018, http://bit.ly/2E6pIgk.

27 Joshua Keating, "Who Was behind the Estonia Cyber Attacks?" *Foreign Policy*, December 7, 2010, http://bit.ly/2U5d33V.

28 United States of America v. Internet Research Agency LLC and Co., Criminal No. (18 U.S.C. §§ 2, 371, 1349, 1028A).

"strengthen" the posts uploaded by trolls (with "likes," shares, and built-in responses).[29]

In addition, there have been reports of the use of fake news sites and landing pages,[30] and fictitious users, both journalists and news sites, have disseminated misinformation and received extensive publicity.[31] Russia uses mechanisms to distribute messages that are customized to various targets. This involves the distribution of paid advertisements or information on social media, based on algorithms of big data analysis that studies the characteristics of specific targets and sends them messages with the goal of capitalizing on their personal weak points that are recognized by the systems and motivating them to act. The distribution of messages takes place through text messages sent to personal cell phones, emails, and personal messages on social media.[32]

Likewise acting in the Russian governmental-civilian sphere are federal media bodies and agencies that constitute an important part of Russia's information struggle. These agencies and bodies operate openly and disseminate information that serves the Kremlin through articles, television coverage, citation of sources, and the creation of "external" content, such as movies and TV series that convey particular messages. Russian federal TV stations broadcast on cable and satellite networks to countries around the world and relay messages that suit Kremlin ideology to Russian-speaking populations in those countries. Russia also operates the broadcasting corporation Rossiya Segodnya (Russia Today) for its purposes, which includes Radio Sputnik and the news agency RIA Novosti, which broadcast in a large number of languages throughout the world. In addition, the government media network RT broadcasts in five languages, and two different content networks broadcast in English (one is aimed at the UK, and the other at the United States).

---

29 Keir Giles, "Putin's Troll Factories," *World Today* 71 (Chatham House, 2015).

30 A "landing page" is a dedicated web page that looks like part of a site, but is in fact a single page but sometimes looks like part of a well-known site, even though they are not connected. Phony news sites are similar to leading global news sites, with a similar domain name and almost identical appearance to the original site.

31 Boris Toucas, "Exploring the Information-Laundering Ecosystem: The Russian Case," CSIS, 2017.

32 Giles, "Putin's Troll Factories."

The traditional institutional media group disseminates information that is convenient for Russia in the form of news reports, talk shows, movies, TV series, documents and "special reports," newsletters, and printed materials. All are distributed in a variety of ways, or posted on bulletin boards. The media networks that are under the control of the Russian administration (RT and Sputnik) disseminate the initial information, repeating it, simplifying it, and framing it as part of events taking place around the world in a manner that is convenient for Russia. In addition, these networks have disseminated information that was stolen through hacking carried out by the Russian military sphere. In doing so, the networks have caused the foreign media to take an interest in the information and repeat it in their reports, contributing to the propagation of the Russian narrative. Figure 1 charts the structure of the Russian information community.

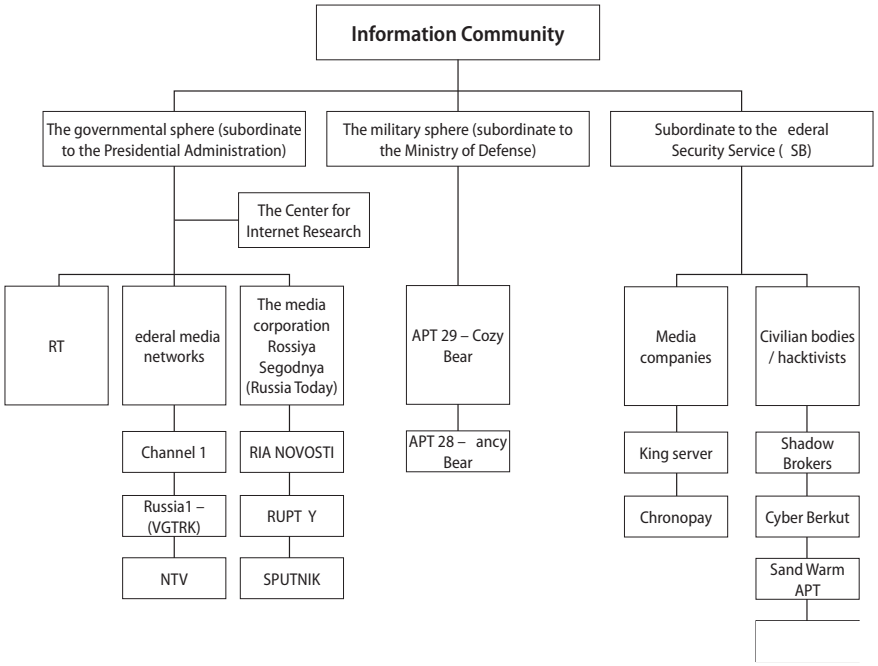


Figure 1: The Russian Information Community[33]

33 The diagram does not include all of the bodies that belong to the Russian information community, but maps its general architecture.

Two clear interests drive the Russian approach behind the decision to activate actors from the governmental and civilian sectors, and they are compatible with Russia's attempts to adapt its traditional methods of indirect warfare to the era of digital media and information: first, the desire to maintain ambiguity and plausible deniability regarding the Kremlin's direct involvement in the Russian cognitive campaign; and second, the relatively cheap cost of these means of warfare.

The Use of Force: Primary Modus Operandi

An analysis of political influence operations attributed to Russia shows the modus operandi of the Russian information community as it utilizes its cognition capabilities and the new tools at its disposal. The analysis indicates a number of patterns: appealing to emotions and sowing doubt among the target audience; aiming at a diverse target audience using diverse messages, and constantly looking for the adversary's social weaknesses. Often, several types of activity can be seen in a single influence operation. Indeed, in the Russian influence operations that we are aware of, a mix of several types has been identified.

The Emotional Element and Undermining Confidence

One of the most prominent characteristics of the Russian activity is the appeal to emotions. The purpose is to influence the cognition of the other side, from the most senior statesman to the citizens of the target country.[34] The appeal to emotion influences decision making, whether it is deciding whom to vote for or a strategic-diplomatic decision by a certain senior official. The feelings sparked are often meant to create doubts and sow confusion, with the aim of influencing an individual to take a certain action or to refrain from a different one.[35] The emotional effort includes attempts to instill the sense that news organizations in the world are not credible, and therefore one must doubt every figure or piece of information they present.

---

34 Michael Kofman, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer, *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Monica, CA: RAND Corp., 2017).

35 Nigel Inkster, "Information Warfare and the US Presidential Election," *Survival* 58, no. 5 (2016): 23-32.

This perspective can also be seen in the motto of the Russian governmental media network RT – "question more."

Reports by Ukrainian civilians describe how the information that Russia disseminated during the occupation of the Crimean Peninsula undermined their certainty of an objective truth.[36] Indeed, the Russian method of operation in annexing the Peninsula in March 2014 created a sense of confusion and raised doubts about whether Russia was even involved in the critical hours at the outset of the operation, as for many hours people wearing unidentified uniforms, later nicknamed "little green men," took action on the ground. The Russian media coverage of the annexation aimed to evoke positive emotions toward Russia's actions and to cause viewers to doubt claims by the West of its illegality.

At home Russian media networks are active not only in the effort to glorify the regime's achievements, but work to undermine the public's confidence in its political competitors. In Russian international coverage they too aim not necessarily to promote the Russian narrative, but to offer an alternative and cover the information from a different angle, ostensibly in order to present "the full picture." Underlying this aim is the assumption that doing so can undermine the truths told from a liberal perspective that the public is exposed to on Western international news networks. Creating doubt is based on the assumption that Western governments lack the means to systematically refute the coverage on Russian networks, and on the assessment that the moment doubt is introduced, it is hard to convince the target audience of factual truths, and these doubts compose another possible version of reality. In this way, Russian influence operations erode the hegemony of Western-liberal news coverage and challenge the West on its home turf – international satellite and internet media.

One example of this is the documentary film by RT on the downing of Malaysian Airlines Flight 17 over eastern Ukraine in July 2014.[37] En route from Amsterdam to Kuala Lumpur with 298 passengers and crew on board, many of them Dutch citizens, the plane was downed over a region in which pro-Russian separatists were active, and led to negative coverage of Russia in

36 Peter Pomerantsev, "Inside the Kremlin's Hall of Mirrors," *The Guardian*, April 5, 2015, http://bit.ly/2BNNWvm.

37 RT Documentary, "MH-17: The Untold Story. Exploring Possible Causes of the Tragedy," *YouTube*, October 22, 2014, http://bit.ly/2tA8T8U.

the Western media. Blame was directed at Russia for supporting the separatist groups in Ukraine and providing them with advanced weapon systems. The RT network chose a media approach that encouraged doubting the Western version, which held that the Buk air defense system, given by Russia to the Ukrainian separatists, is what shot down the Malaysian plane. Not only did the Russian network undermine the factual basis of the accusations against Russia; it also created a parallel narrative whereby there was Ukrainian Air Force military activity over Ukraine at the time of the incident, which could have caused the plane's fall. RT did not try to refute the claims against Russia or to substantiate its claims regarding Ukrainian responsibility for the tragedy. RT did not strive to create its own narrative of the events, but to present another possibility, and focused on gaps in the Western version, in order to cast doubt on Russia being at fault for the event. In later coverage of the same event, RT focused on the version whereby the investigation into the incident is not conclusive, thus attempting to exonerate Russia due to the existence of reasonable doubt.

Target Audiences and Social Weaknesses

Aiming at a diverse variety of groups shows that the Russian information community undertakes in-depth social research on target populations. In addition to the civilian population, Russian information operatives direct their messages at leaders and public opinion shapers, and in military campaigns, also at commanders and soldiers. Russia's political influence operations are customized to the various targets, with the message itself directed at a weakness that characterizes each of the target populations. In order to succeed in customizing the attacks to these weaknesses at the right times, intelligence work is required, and this takes place constantly in order to identify the particular weaknesses to be targeted by the attack.

A clear example of the approach of aiming at a variety of target audiences can be seen in the number of political influence operations that the Russians have carried out over the past few years in various places, including Germany. Russia has recognized Germany's importance in intergovernmental European mechanisms, especially in the European Union. Russia also seems to have recognized that Chancellor Angela Merkel's policy regarding the refugees has agitated much of the German population, and saw this as an opportunity. Even before the decision to operate in Germany, Russia worked to consolidate its

relations with pro-Russian elements and candidates for the German political and establishment sphere, in order to expand its influence and its power, and in order to improve its information-gathering in the internal arena.[38]

An example of exploiting the weakness of public opinion in Germany was the way Russia likely used the events surrounding a Russian-speaking girl who lived in Germany, 13-year-old Liza, whose parents reported to the Berlin police that she was missing. She returned home 30 hours later and told her parents that she was kidnapped and raped by three immigrants, but it quickly became clear that this was not the case. Nonetheless, Russian federal television networks began intensive broadcasts on YouTube and on social media in order to spread the girl's initial version, while casting doubt on the credibility of the response by German authorities (who ostensibly silenced the story) and blaming Chancellor Merkel's immigration policy. Following this, demonstrations were organized in Germany, building on the local Russian-speaking community, joined by additional social groups. The demonstrations received media coverage, and the girl's story went viral and flooded the German media. Russia continued to claim that the police version that was publicized, including evidence that contradicts the girl's version, aimed to cover up Germany's inability to cope with the refugee problem – an issue that Russia recognized as a political vulnerability of the German government. In the end, the girl's story became a central issue in the discourse in Germany and caused considerable tensions within the German government, and undermined public confidence in the Merkel government.[39]

Diversity and the Distribution of Content

As a direct continuation of the ongoing search for social weaknesses among the public, the Kremlin sees great importance in the scope and diversity of the content distributed, as well as the continuity of activity. A study conducted by NATO claims that Russia aspires to flood the internet with information relating to the narrative that it wants to instill, including unnecessary and irrelevant information, in order to maximize its distribution. In addition, it has an interest in blurring the relevant facts and replacing them with

38 Stefan Meister, "The Lisa Case: Germany as a Target for Russian Disinformation," *NATO Review*, 2016.

39 Jim Rutenberg, "RT, Sputnik and Russia's New Theory of War," *New York Times*, September 13, 2017.

"alternative facts."[40] In effect, Russia optimally adapts its types of activity for the era of online communication.

Historian Yuval Noah Harari emphasizes that in the world of internet communication and the information technology revolution, the most effective way to impose censorship is to flood the information arena – "today, censorship works not by blocking access to information, but by concealing it in enormous amounts of irrelevant information."[41] Proof of this type of activity can be seen in the testimony of two former employees at the Russian troll organization.[42] The two related how each day they received a new list of tasks, which was updated according to events and included detailed explanations of possible responses and links to designated content. The goal was to create new content each day that would be distributed on the internet and serve the Russian narrative.

Russia ensures that each campaign includes the use of several parallel channels to distribute messages, including official media, informal media, and social media. These are sometimes operated simultaneously by actors from both the military sphere and the governmental-civilian sphere. An example of the variety of sources distributing the content and the continuity of activity can be seen in the Russian intervention in the US presidential elections in 2016, when Russia used tools from all three of the groups. Each day additional information was disseminated, some of new information and some information that was already available on the internet.

The US Department of Justice stated that Russian intelligence operated the Guccifer 2.0 Twitter account, which posted content that came from hacking the Democratic Party headquarters. The account shared tweets by other users, among them those issued by trolls operated by Russia, including manipulated content on events in the United States surrounding the elections. It also responded to accusations against it and created an ongoing, lively

40 "Russian Information Campaign against Ukrainian State and Defense Forces," NATO Strategic Communications Centre of Excellence, 2017.

41 Yuval Noah Harari, "In a World Deluged by Irrelevant Information, Clarity is Power," Penguin Books, August 20, 2018, http://bit.ly/2IxxWUm.

42 Shaun Walker, "Salutin' Putin: Inside a Russian Troll House," *The Guardian*, April 2, 2015.

discourse supportive of Donald Trump, and came out against Democratic candidate Hillary Clinton.[43]

The US presidential elections also revealed the variety of platforms that Russia used: manipulated content was distributed on Twitter, Facebook, written media, live YouTube videos, and Russian-funded television networks. Later, after the information received attention, it appeared in all foreign media networks, including American networks. British media researcher Stephen Hutchings recognized this Russian pattern of activity, but also noted that the Russian system of message creation, which is meant to influence political consciousness, is highly decentralized and does not necessarily convey a coordinated, coherent doctrine.[44]

Conclusion

This article presents Russia's political-cognitive efforts, and surveys the Russian information community that operates in military, governmental, and civilian spheres. Russia's information community is a diverse professional community that enables sophisticated activities in all geographical arenas of activity that are relevant to Russia, using a variety of technological spheres of activity. The information tools that Russia uses rely both on online media and on traditional and human communication, via military and governmental-civilian actors. The efforts that Russia invests in the realm of influencing cognition, through the information community and with the help of new information technology tools, have increased its confidence in its ability to operate in this sphere around the world.

In this way, Russia attempts to overcome what it sees as its structural inferiority in the conventional and economic spheres, compared to other superpowers. Thus, it situates itself as an information superpower that aspires to control the new tools of warfare offered in the knowledge and information era. This is multi-dimensional control, from the ability to disrupt the functioning of communications systems and computers, to advanced espionage capabilities and the manipulation of content. The control of

---

43 "Kremlin Troll Tells All About Influencing U.S. Elections," *Moscow Times*, October 16, 2017, http://bit.ly/2VkxWbT.

44 Stephen Hutchings, "We must Rethink Russia's Propaganda Machine in Order to Reset the Dynamic that Drives It," London School of Economics blog, April 4, 2018, http://bit.ly/2SjhMgN.

information could provide an answer to the question: what is a superpower in the era of knowledge and information? Russia's activities in the realm of information are in effect an expression of the new superpower status that it has helped create.

Yet Russia's efforts to become an information superpower indicate a mixed balance sheet. In effect, there is no unequivocal proof of the effectiveness of the use of information as a strategic tool. This is a tool that poses two main problems for its users: difficulty measuring success (it is more than likely that some activity has only limited influence); even when an influence operation seemingly succeeds, the level of success in achieving strategic objectives is still in doubt. Russia's intervention in the US presidential elections illustrates this problem. For example, even if we assume that it is true that Russia conducted a large scale influence operation with the goal of helping Donald Trump's election as president, and that this operation did indeed play a significant role in his election as president, it is still an open question whether Russia achieved its objectives in this way. In effect, its increased intervention in the American information arena exposed President Trump to unprecedented criticism and pushed him into a political situation that does not enable him to improve relations between the United States and Russia – which was a prominent campaign promise.

Thus at least for now, information warfare is a new tool that creates opportunities in the international arena, but its level of effectiveness and its ability to achieve political objectives are still in doubt. The Russian case should also warn us against any exclusive overreliance on information warfare as a tool in international relations, as long as its level of credibility and the consequences of its use have not yet been fully clarified.

Iran's Information Warfare

Itay Haiminis[1]

Iran is an active player in the arena of information warfare at the regional and global levels, alongside Russia and China.[2] This article analyzes and assesses Iran's information warfare capabilities and activities, and demonstrates how it serves Iran's diplomatic and military objectives, including strengthening the regime's image and standing, and undermining the internal resilience of its adversaries.

---

1 Itay Haiminis is a Neubauer research associate at INSS.

2 The identification of Iran as an important player in the arena of information warfare is expressed in the words of a number of senior American officials. Former US National Security Advisor John Bolton said in August 2018: "I can say definitively that it's a sufficient national security concern about Chinese meddling, Iranian meddling and North Korean meddling that we're taking steps to try and prevent it," Caroline Kelley, "Bolton: Chinese, Iranian, North Korean Election Meddling 'a Sufficient National Security Concern,'" *CNN*, August 19, 2018, https://cnn.it/2E4i4mI. In this context, in September 2017, the American CENTCOM Commander said: "One of the key things that we see here is their [Iran's] use of cyber capabilities to manipulate the information environment. This is where you see the most significant influence of these actors in this particular space. Their ability to use cyberspace to manipulate information, propagate a message is a key aspect of what we see," Patrick Tucker, "US Military Leaders Worry About Iran's Media Operations," *Defense One*, September 15, 2017, http://bit.ly/2NmxqXS; Michael Moss, Deputy Director of the Cyber Threat Intelligence Integration Center, said in August 2018: "Russia, China, Iran, and North Korea will pose the greatest cyber threats to the U.S. during the next year," "Statement for the Record Mr. Michael Moss Deputy Director of the Cyber Threat Intelligence Hearing on Cyber Threats to our Nation's Critical Infrastructure," Cyber Threat Intelligence Integration Center, August 21, 2018, http://bit.ly/2TdJ3Wt.

The Characteristics of Iranian Information Warfare

Iran, similar to other countries, sees information warfare as a tool that helps it achieve its diplomatic and military objectives, alongside other non-military tools (such as financial aid). Iran's information warfare includes public diplomacy, cyber influence operations, and strategic communication, and is a central element in a cohesive and well-established doctrine that prioritizes non-military warfare. This is due to Iran's military and conventional inferiority in relation to its enemies, and its concerns regarding the dangers of a military confrontation with them.

Iranian information warfare is part of a broad, coherent doctrine of political warfare. According to the RAND Corporation, political warfare is the "intentional use of one or more of the implements of power (diplomatic, information, military, and economic) to affect the political composition or decision making within a state. Political warfare is often – but not necessarily – carried out covertly, but it must be undertaken outside the context of conventional war."[3] Information warfare holds special importance as part of political warfare: "The information arena is an increasingly important battleground where perceptions of success can be determinative. Information warfare works in various ways by amplifying, obfuscating, and, at times, persuading."[4]

Information warfare, as part of the cognitive campaign, is, as noted, an element in the array of efforts used by Iran to achieve its objectives, including expanding its base of influence in the Middle East; undermining the internal resilience of its adversaries, including the Gulf States; strengthening the impact of its military efforts (for example, by exaggerating their successes); and improving its own image and that of its regional policies. In addition, Iran's information warfare supports and supplements its ability to export its ideological, religious, and cultural principles, including combating the West and supporting the "resistance."

---

3 Linda Robinson, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson and Katya Migacheva, *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND Corp., 2018), http://bit.ly/2SmhNAz.

4 Ibid, p. xix.

Iranian information warfare incorporates a very wide variety of tools. Iran uses public diplomacy[5] and strategic communication[6] in the form of public statements, publications in the "traditional" media, pop culture products (movies, books, songs, etc.), and the internet, with all of the possibilities that it offers – from social media to news websites. The content is diverse and changes according to context and concrete need, and, in addition, is quickly adjusted and adapted in a way that is relevant to Iran's changing environment and to the challenges it is grappling with.

From a historical perspective, Iran's use of information warfare, such as posters, recordings, and propaganda pamphlets, was common even during the times of the Shah, when his opponents made extensive use of these tools as part of their struggle against him. After the 1979 revolution, the Ayatollah regime adopted these methods to safeguard its survival and to propagate its principles, even outside Iran's borders.[7] Like other authoritarian regimes, the Iranian regime has a long-held belief that the primary threat from its enemies is not only a conventional military one, but also cultural and philosophical, extending to the struggle over the character of Iranian society. This view was well illustrated during the 2009 demonstrations in Iran. These events were declared by Iranian decision makers to be a direct

---

5 "A government's process of communicating with foreign publics in an attempt to bring about understanding for its nation's ideas and ideals, its institutions and culture, as well as its national goals and policies." Available at Jan Melissen, ed., *The New Public Diplomacy: Soft Power in International Relations* (New York: Palgrave Macmillan, 2005), http://bit.ly/2SmhPbF. For discussion of the term "public diplomacy" in different cultural contexts, see Dov Shinar et al., *Public Diplomacy in Israel* (Shmuel Neeman Institute, Technion, and the Ministry of Foreign Affairs, March 2009), http://bit.ly/2IAv2hw [in Hebrew].

6 There are various definitions for the term "strategic communication," most of which focus on harnessing all forms of communication available to an organization in order to promote its goals. There are a number of relevant sources, such as Kirk Hallahan et al., "Defining Strategic Communication," *International Journal of Strategic Communication* 1, no. 1 (2007): 3-35, http://bit.ly/2TcLWH4; and Kjirsten Thorson, "Strategic Communication," in *Communication* (2013), http://bit.ly/2GV6ldg; for discussion of the term "strategic communication" in the context of military operations, see Richard Halloran, "Strategic Communication," *Parameters* (2007): 3-14, http://bit.ly/2E4SSML.

7 Ariane M. Tabatabai, "A Brief History of Iranian Fake News," *Foreign Affairs*, August 24, 2018, https://fam.ag/2E8F6bU.

continuation of extensive efforts by the country's enemies – chief among them the United States – to incite internal Iranian public opinion against the regime with the goal of instigating a revolution. From Iran's perspective, cultural, ideological, and philosophical aspects that threaten the hearts and minds of Iran's citizens require information warfare counter-efforts, in order to preserve the character of the Islamic Republic.[8]

Current Expressions of Iran's Information Warfare

Today, Iranian use of information warfare (alongside other tools) is seen in part in its regional intervention.[9] A brief look at its efforts in this area demonstrate that despite the varying and diverse methods employed, Iran's information warfare is usually just one component that complements other Iranian efforts – political or military. Thus, Iran's main achievements in the region in recent years were gained by applying conventional military power or granting military and financial aid to its allies, or via diplomacy.

Strategic Communication and Public Diplomacy

Strategic communication in the Iranian context is the utilization, both public and clandestine, of all of the tools available to the regime in order to convey messages. Iran makes use of public diplomacy in various ways to create direct dialogue with a range of populations. Its use of strategic communication and public diplomacy, as part of its information warfare, rests on a sound understanding of the target audiences that it wishes to influence, as well as an ability to fine-tune public messages (verbal or otherwise) in

8 For example, Iran's Supreme Leader warned in 2015 that "economic and security infiltration [of the West against Iran] is not as important as intellectual, cultural and political infiltration," "Enemy Infiltration Major Threat: Leader," *Press TV*, September 16, 2015," http://bit.ly/2GDD7jT; motifs of victimhood, lack of security, and lack of trust in its neighbors, as well as the West due to a history of conflicts along its borders and foreign intervention in its internal affairs, are also expressed in Iranian information warfare. The content that characterizes Iranian information warfare in this context often demonstrates ongoing deep suspicion and fears of foreign aggression, with conspiracy theories about threats that Iran is facing.

9 Raz Zimmt, "Iranian Soft Power in the Middle East," Forum for Regional Thinking, November 10, 2017, https://bit.ly/2k5D2vs [in Hebrew]; more evidence of Iranian success at information warfare in the Middle East can be found in the words of the US CENTCOM Commander, cited above in note 2.

order to achieve goals. For example, Iran uses the media for deterrence by intensifying the "price tag" that its enemies will pay if they cross "red lines." It does this both through demonstrations of advanced weapons and with threatening public statements.

Detailed below are various Iranian influence efforts, not all of which were successful. To be sure, it is difficult to measure success in information warfare, and many initiatives in this area fall into the category of "help others today and one day they will help you." Nevertheless, in public diplomacy, the target audience also plays a role. In the case of Iran, the closer the beliefs and perceptions of the target audience to those of Iran, the higher the chance of success.

One example of Iran's use of strategic communication against the United States was in November 2018, against the backdrop of the American announcement of renewed sanctions against Tehran. In response to American messages on this topic, Iran's official spokespeople declared that the US actions effectively constituted a declaration of war, and that Iran reserves the right to respond to them. The Chairman of the Iranian Parliament (Majlis), Ali Larijani, asserted at the time that "for 80 years, the US has interfered in the internal affairs of Iran and committed crimes against it." Minister of Defense Amir Hatami added that "the President of the United States, Donald Trump, and Secretary of Defense Mike Pompeo are lying in order to undermine the Iranian nation's unity." The acting Commander-in-Chief of the Islamic Revolutionary Guard Corps, Hossein Salami, said that "Iran is willing to control the presence of the US in the Middle East," and the Commander-in-Chief of the Islamic Revolutionary Guard Corps, Mohammad Ali Jafari, declared that "the US' power is fading and Iran is not afraid of it." These emphatic and hostile statements were backed up by a well-publicized military drill (Velayat 97) of Iran's advanced air defense systems.[10]

Iran's use of strategic communication against the US increased after Donald Trump began his term as president. In September 2017, after Trump accused Iran of violating the nuclear deal, Iran revealed a new ballistic missile named Khorramshahr, during a military parade marking the 37th anniversary of the Iran-Iraq War. The unveilingof the missile was accompanied by a

10 "As US Sanctions Resume, Iran Starts Annual Air Defense Drill," *Business Insider*, November 5, 2018, https://read.bi/2Es9kbr.

belligerent message from Iranian President Rouhani, pronouncing that Iran intended to continue to shore up its military capabilities.[11] In August 2018, the Iranian Secretary of Defense presented another new ballistic missile.[12] The well-publicized presentations of the weapons were intended, in part, to signal to the Trump administration that its policies had the potential for damage, and could lead to a military confrontation between the two sides.

Alongside its official spokespeople, Iranian strategic communications also enjoys support and assistance from influential figures inside the US, including Seyed Hossein Mousavian of Princeton University and Trita Parsi, the head of the American-Iranian Council. These individuals were prominent supporters of the regime prior to the signing of the nuclear agreement with Iran and during the negotiations, and voiced opinions that were aligned with Tehran's.[13] Mousavian and Parsi attacked Trump and expressed opinions that support Iranian policies, particularly regarding American policy towards Iran. Though these people are not regime officials, their stances mirror Iran's outlook, and therefore their statements validate and bolster the legitimacy of Iran's positions.

Iran also makes extensive use of public diplomacy, with its senior representatives working to convince target audiences of the justness of its worldview and interests. In Iran's primary arenas of combat in the Middle East – Syria and Iraq – public diplomacy is particularly prominent; in these countries, alongside additional military and political tools, it serves strategic purposes such as supporting powerful actors allied with the Iranian regime, most prominently the Assad regime in Damascus, strengthening the Iranian-Shiite circle of influence, and fending off competing influences (American, Turkish, Gulf States, Russian, or Chinese – and even Israeli).[14]

---

11 Roi Kais, "Response to Trump: Iran Reveals New Ballistic Missile," *Ynet*, September 22, 2017, http://bit.ly/2XkU3At [in Hebrew].

12 "Iran Presents: New Medium Range Ballistic Missile," *Ynet*, August 13, 2018, http://bit.ly/2GCDVoU [in Hebrew].

13 Seyed Hossein Mousavian, "The Strategic Disaster of Leaving the Iran Deal," *Foreign Affairs*, May 10, 2018, https://fam.ag/2XjctBL.

14 Raz Zimmt, "Iran in the Post-ISIS Era," Israeli Intelligence Heritage and Commemoration Center, November 23, 2017, https://www.terrorism-info.org.il/app/uploads/2017/08/E_172_17.pdf [in Hebrew].

However, Iranian public diplomacy was only partially successful in Syria, where it was forced to rely more on conventional military fighting. The reasons for this were the limited number of Shiites in the country and the sectarian tensions there (as in Yemen and Bahrain), which limit Iran's ideological, cultural, and religious powers of persuasion.[15] Noteworthy in this context are Iranian efforts in the media to emphasize its role as the protector of the Shiite population and its holy places, such as the Sayyidah Zaynab tomb in Damascus, or encouraging the Shiization of the public sphere via the media.[16]

In Iraq, Iran succeeded in limiting American influence and winning military and political loyalty to it there, while weakening the central and nationalist Iraqi government and challenging the local religious establishment. A prominent example of Iran's public diplomacy occurred in 2014 and 2015, when Qasem Soleimani, the commander of the Quds Force, went on a well-publicized journey with his fighters in Syria and Iraq, meant to highlight Iran's military leadership and its integral role in the local fight against extremist Sunni Islam. Since then, Iran has made sure to highlight in its media the important stabilizing role that it plays in the region, including its military achievements against ISIS.

It is difficult to precisely estimate the impact of Iran's information warfare compared to its other efforts that are made simultaneously. However, it is reasonable to assume that in the countries where the sectarian and religious make-up allow for it (i.e., those with a Shiite or pro-Iranian population), there are advantages to the "soft" realm of information warfare.

In Lebanon, Iran's public diplomacy is expressed in its attempt to be seen as an alternative to Saudi Arabia as the financial and military benefactor of the Lebanese army. Iranian efforts in this area are supported by official public statements, official visits by high-ranking figures, and media coverage of the Iranian position on pro-Iranian media outlets in Lebanon. The goal of these efforts is not only to improve its image and boost its standing, but also to goad Saudi Arabia, to drive a wedge between Saudi Arabia and its allies in Lebanon, and to signal to the US Iran's weight in the region. At the same time, Iranian influence efforts in Lebanon benefit from the dominance

15 Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses*.

16 MEMRI, "The Shi'ization of Syria: In Damascus, Unprecedentedly Extensive Observance of the 'Ashura,'" November 16, 2014, https://bit.ly/2kudtoc.

of Hezbollah there, and especially from its total hegemony among the local Shiite community.

Meanwhile, Iran's strategic communication vis-à-vis Israel is part of a wider mission dictated by the Iranian regime's ultimate objectives,[17] chief among them weakening the State of Israel to the point of destroying it, and blocking Israeli actions against Iran.[18] Iranian officials use threatening rhetoric against Israel, which is sometimes backed up by displays of military strength (such as military drills or parades) aimed at conveying messages of deterrence and reflecting Iran's aspirations to sow panic in the Israeli public.

A significant component of Iranian strategic communication against Israel is Hezbollah. Hezbollah enjoys control of various and diverse media outlets in Lebanon, which help the organization convey messages to decision makers in Israel and to the Israeli public. In addition, its leader, Hassan Nasrallah, makes public televised speeches on a regular basis, in which he integrates messages on both internal and foreign policy. These communiqués serve the Iranian agenda and incorporate messages of deterrence against Israel as well as maligning its image and portraying Israel as working to undermine regional stability and as serving American interests.

Cyber Influence Operations[19]

The technological tools made available by the internet clearly play a more central role than in the past, and this is seen in the Iran case too. Iran uses

17 Another important element in Iran's information warfare efforts against Israel is the anti-Israel propaganda on popular media and cultural outlets. This includes content such as criticism of Israel's regional policies, specifically vis-à-vis the Palestinians, Holocaust denial, and exaggerating Israel's supposed threat against the security and stability of the Middle East. An example of an organization that works to distribute anti-Israel propaganda is the Owj Arts and Media Organization, which is connected to the Iranian Revolutionary Guard Corps. See https://bit.ly/2m1mju4.

18 Meir Litvak, "Iran and Israel: The Ideological Enmity and Its Roots," *Issues in the Revival of Israel* 14 (2004): 367-92, http://bit.ly/2XlZlfo [in Hebrew].

19 Cyber influence efforts are those with the purpose of changing the opinions, decisions, and/or behavior of the target audience. See the FireEye report: "Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in US, UK, Latin America, Middle East," *FireEye Intelligence*, August 21, 2018, http://bit.ly/2SVxwMc.

cyber information warfare to demonstrate to its enemies that it can harm their "underbellies," meaning the fabric of civilian life in their countries.

Like other types of information warfare, it is difficult to claim or prove success in the cyber realm as well, especially when discussing a brief time period, and therefore we simply outline here Iranian efforts in this area that have recently been uncovered. At the same time, we can reasonably assume that Iran has also undertaken some covert actions that have not yet been discovered.

Via the internet, Iran exploited Western and internal criticism of Crown Prince Mohammed bin Salman's regional policy by spreading false rumors of his death and efforts to replace him as part of its struggle against Saudi Arabia, its main adversary in the Middle East. In addition, following the murder of Saudi journalist Jamal Khashoggi in the Saudi consulate in Turkey in October 2018,[20] Iran created bots, fake news sites, and fake Twitter profiles to spread false information and to increase public pressure on Saudi Arabia, as well as to undermine the Kingdom's relationship with the United States.[21]

An additional recent example of Iran's internet activities to influence consciousness, this time directed at the Israeli population, is the website Tel Aviv Times, which was exposed by the Israeli security company ClearSky.[22] The site included current news content, mostly copied from Israeli news sources, which was doctored to reflect the reported events and their contexts according to Iranian policy goals regarding Israel. The website was intended to achieve several grandiose goals for Iran, though it is very doubtful that that was the result. These goals included achieving a "foothold" in the Israeli public discourse, disrupting daily life in the country, and undermining public confidence in the Israeli media. Prominent examples of the website's attempts to influence the consciousness of the Israeli population include describing Hezbollah as an "organization" instead of a "Shiite terror organization," exaggerating the Assad regime's military achievements in Syria, and describing

---

20 "Jamal Khashoggi: All You Need to Know about Saudi Journalist's Death," *BBC News,* December 11, 2018, https://bbc.in/2BOJXyC.

21 Jack Stubbs, Katie Paul, and Tuqa Khalid, "Fake News Network vs Bots: The Online War around Khashoggi Killing," *Reuters*, November 1, 2018, https://reut.rs/2GHv4Cj.

22 Sagi Cohen, "It's Not an Israeli Site, it's Iranian Propaganda," *Ynet*, September 6, 2018, http://bit.ly/2SX1pMc [in Hebrew].

the IDF as "concerned" about Iran's response, against the backdrop of the conflict between Israel and Iran in Syria.

Iran operates several cyber organizations against Israel through its security and intelligence wings, as well as through subsidiaries with connections to the Iranian regime. These organizations conduct influence operations during times of regional tension or on symbolic dates, such as the Iranian Jerusalem Day, which include hacking Israeli websites.

Iran also regularly targets the US through fake news websites and social media profiles. Over recent years, information security and technology companies have exposed extensive cognitive operations by Iran, aimed primarily at influencing the American public. These activities included a large number of fake news websites, over a million Tweets created by fake accounts, and dozens of fake Facebook profiles. Iran's goals are to exacerbate American internal polarization between different social groups (liberals-conservatives, blacks-whites, Trump supporters-opponents) and to improve the Iranian regime's image and the legitimacy of its policies in American public opinion, as well as to attempt to establish its presence on the web, to be utilized by Iran in the future. The exposed content covered issues at the center of the American agenda, ranging from articles about publicly sensitive and loaded topics, such as racism, controversial policies of President Trump, police violence, and more. The texts were adapted to the target audiences of different platforms and seem to have been intended to agitate, radicalize, and provoke heated discourse. The content about the Middle East included piercing criticism of American, Israeli, and Saudi Arabian policies alongside positive coverage, from Iran's perspective, about events in Yemen, Lebanon, Syria, and Iraq.[23]

The exposure of these operations led to considerable negative media discourse against Iran, which forced the spokesperson of the Iranian UN delegation to deny the claims against it and counterattack these accusations by claiming that they are an additional expression of American attempts to bring about regime change in Iran.[24] A similar message was repeatedly

23 Daphne Ringuet, "Iran Has Its Own Fake News Farms, But They're Complete Amateurs," *Wired*, October 25, 2018, http://bit.ly/2SZJEM7.

24 Jason Rezaian, "Iran Is Spreading Lies on Social Media. There's an Easy Way to Stop Them," *Washington Post*, August 23, 2018, https://wapo.st/2GlK48j. These statements join claims by additional official Iranian regime spokespeople who

expressed by official regime spokespeople in late 2018, against the backdrop of the internal protests in Iran.[25]

While recently-exposed Iranian cyber influence operations indicated Israel's and the US' vulnerability to Iran's attempts to contaminate the public discourse, they also highlighted the limited effectiveness of their efforts to change public opinion, not to mention to bring about pro-Iranian political activity.

A few weeks before the April 2019 Israeli elections, Israeli media reported that the cell phone belonging to Blue and White party leader Benny Gantz was hacked by Iran, and that Iran had the phone's contents in its possession. Despite the fact that Iran did not release the information that it had acquired, and even denied that this happened, Gantz's political rivals used the alleged hack to undermine his image, claiming that he was unfit to serve as prime minister because he would be vulnerable to Iranian blackmail.[26]

While the media and public discourse in Israel discussed the consequences of the hack on Gantz's candidacy, nobody asked whether this was an Iranian

---

accuse the US and Saudi Arabia of inciting ethnic minorities in the country and supplying them with financial aid in an attempt to undermine the regime's stability. See James M. Dorsey, "Amid Ethnic Protests, Iran Warns of Foreign Meddling," *BESA Perspective Papers* No. 931, August 26, 2018, http://bit.ly/2GWeCxu.

25 The 2018 protests in Iran were also a catalyst for the escalation of the cognitive struggle between the regime and its domestic opponents. While Iran makes extensive use of social media and internet tools in general to amplify its official messages, it has also in recent months been restricting the ability of its citizens to use the internet to make their voices heard (such as blocking Telegram and slowing internet speeds). These restrictions, which drew sanctions from the United States, are an example of the regime's growing attempts to deal with internal protests by shaping content, communications, and the framework of public discourse. These include arresting Iranian citizens who are active on social media and efforts by regime organizations to compete with them. The Iranian regime's efforts to influence consciousness in the internal arena include not only fighting its adversaries, but also a more significant element of preserving and strengthening the legitimacy of the regime and justifying its regional intervention – an element whose importance grows as Iran increases its intervention in the region.

26 Uri Berkovitz, "Cyber Experts: Concern that False Information Could Be Disseminated, Supposedly Like that which Appeared on Gantz's Phone, to Influence the Elections," *Globes*, March 16, 2019 https://www.globes.co.il/news/articleaspx?did=1001278223 [in Hebrew].

influence operation meant to influence the Israeli elections. Iranian cyber activities aimed at influencing the Israeli public were detected long before the elections. Despite the fact that Iran has an interest in undermining the integrity of the elections and in contaminating the Israeli political discourse, no unusual Iranian activity was identified during the elections. The characteristics of the discourse on social media after the hack became known did not change, and certainly did not resemble the discourse on American social media following Russian intervention. Therefore, there remains a possibility that Iranian involvement for the purpose of espionage generated – with the help of internal forces – influence on the elections even without Iran intending to do so.

Conclusion

This article presents the ways in which Iran uses information warfare as an important tool to achieve its objectives in the Middle East. It did not examine here the level of success of these efforts, but rather emphasized the goals behind them and the methods used by Iran to promote them.

Firmly held perceptions and experiences in Iran, such as fear of another conflict similar to the Iran-Iraq War and fear of foreign intervention, have over the years established information warfare as a central arena for Iranian activity. From this perspective, cyberspace holds vast potential, both in light of its characteristics that suit Iran's preferred types of activity (such as secrecy and indirect conflict) and also because Iran's adversaries are still having difficulty developing the concepts and capabilities to defend against these types of actions in the realm of consciousness. At the same time, as observed in this article, Iranian information warfare is currently limited in its ability to serve Iran's objectives. Iran must continue to rely on "traditional" military and diplomatic tools. Its uniqueness in the field of information warfare and influence campaigns is that it behaves like a world power though it is only a regional power, and it demonstrates the audacity to operate against great powers, such as the United States, through the extensive use of social media.

Israel is not at the center of Iran's agenda. Still, it would be prudent for Israel to not only be aware of its existence, but also to work to thwart activities stemming from that agenda, or at the very least to acknowledge the level of danger inherent in it. Any Israeli effort to decrease Iran's regional influence must include both offensive and defensive aspects that can cope with the

Iranian information warfare threat, also in light of the great importance that Iran places on such threats as part of its pursuits in the region. Such aspects could include, for example, operations against the publication of false Iranian content (exposing platforms or content, blocking TV broadcasts, etc.), while promoting anti-Iranian content to establish a counter-narrative. In addition, it is possible and worthwhile to exploit Iranian consciousness efforts to strengthen the legitimacy of Israeli actions against Iran by presenting them as additional expressions of Iran's destructive activities in the region.

Part IV

Israel and the Cognitive Campaign

Cognition: Combining Soft Power and Hard Power

Udi Dekel and ia Moran-Gilad[1]

The cognitive effort is woven into all stages of military and political activity. At the outset of an action, it prepares the groundwork and creates the legitimacy for exerting hard or soft power. During the action, the cognitive effort enables the ongoing exertion of various powers, provides the logic of their integration, and establishes the foundations for the political resolution and the shaping of a stable improved military and political situation. At the end of the action, the cognitive effort emphasizes the achievement attained as a result of the powers utilized, and works to maintain it over time and prevent cognitive achievements by the adversary.

This article examines the hypothesis that cognition involves a conceptual framework that connects all efforts, "hard" and "soft," aimed to achieve defined political and military objectives. The article first examines theoretical aspects of power and consciousness and cognitive effort as a central element in the approach of the political-military campaign ("translating" the achievements of the efforts exerted). Afterwards, the article presents two case studies in the Israeli context, and examines the hypothesis that cognition connects all of the efforts that aim to achieve political and military objectives. The article concludes by offering key insights and recommendations.

1 Brig. Gen. (res.) Udi Dekel is the Managing Director of the Institute for National Security Studies. Dr. Lia Moran-Gilad holds a doctorate in International Relations from Ben-Gurion University.

Hard Power and Soft Power

The complex concept of "power" is of major centrality in the domain of international relations. Its complexity is expressed in being multi-dimensional and having a dynamic structure. For example, power can change its scope, the area in which it is exerted, its level of intensity, its cost (the price paid by the actor exerting the power, and the price paid by the actor upon whom power is exerted), and its means. Another dimension of power that is sometimes hidden is the dimension of intent. Cases in which one actor overtly influences another actor are easier to identify, whereas cases in which one actor influences another actor without overt or intentional activity or by means of covert activity are harder to identify.

The centrality of the concept "power" in international relations is evident in a large variety of approaches that define it and the way it is expressed. One general distinction indicates the difference between "behavioral power" – the ability to attain the results in the international arena sought by the actor exerting it – and "resource power" – the resources that the actor has that enable it to attain its desired results. Behavioral power is manifested in two principal means: "hard power" and "soft power."

Hard power is applied when Actor A exerts coercive or conditional (deterrent) measures on Actor B, thus causing it to act in a way that is in the interest of Actor A, which Actor B would not have done without this coercion or condition. In contrast, soft power is expressed when Actor A succeeds in causing Actor B to act in accordance with Actor A's wishes without exerting coercive or conditional measures to this end, but through persuasion or through norms and values.[2] It follows from this that hard power and soft power, while connected, are not the same, and sometimes complement one another.

An actor's power is a tool for exerting efforts to promote its interests, in accordance with the strategic objective that directs both hard and soft efforts toward achieving political objectives. Therefore, the strategic objective is a compass for directing and synchronizing all efforts, including cognitive efforts. Cognitive efforts are integrated in soft power and hard power and

2 Joseph Nye, "Soft Power," *Foreign Policy* 80 (1990): 153-71; Joseph Nye, *Soft Power: The Means to Success in World Politics* (New York: Public Affairs, 2004).

aim to influence the adversary's cognition by manipulating information and enhancing the effect of hard power.

Cognition as a Central Element in the Political-Military Campaign

The information revolution and the technological leaps of the past few years that have made information more accessible through many advanced platforms have led to the element of cognition assuming diverse layers. Cognition has also received greater weight in advancing the policy and objectives of various actors in the international system, both in conflict situations and in routine times.

Attaining a cognitive effect requires a series of actions aimed at shaping the approaches to the reality of different target populations, including the enemy, the domestic public (the internal arena), the enemy's domestic public, the regional environment, and the international community. The goal is to achieve the defined strategic objective. Cognition is always subjective and adapted to the culture and to the religious, political, and social views of the different populations, and to their expectations. Cognition is sometimes shaped over time, but there are cases in which a single picture can change the perception of reality. We suggest also seeing cognition as a conceptual framework that connects all efforts, hard and soft.

The shaping of cognition during a conflict between adversarial actors includes several stages: formulating the narrative of the conflict by describing the reality that prevailed before; the need and the legitimacy to change the situation or to maintain it, due to an assessment that the possible end states are inferior to the current situation; the reasons for defining the political-military objectives; and the principles for conducting the campaign such that it will influence the consciousness of the various target audiences in a way that serves the strategic objective.

The various measures and powers exerted need to match the "story" that the actor wishes to convey to the designated target audiences. This is so that the construction of cognition is effective and strengthens the legitimacy of exerting hard power, especially military power; so that the achievements of exerting hard or soft power are translated into political and international achievements; so that is possible to shape an image of victory that illustrates the achievement of the political-military objectives, or offsets

the achievements of the adversary; and in order to establish an improved political-military reality over time.

Cognitive influence efforts create an ongoing process of providing meaning to events as part of the attempts to instill these meanings in target audiences. The primary and direct circle of cognition is the way adversarial sides who are involved in a conflict assess their achievements by examining the extent to which achievements in practice match declared objectives. At the same time, in secondary circles, cognitive efforts are directed toward external populations that are not directly involved but have the ability to influence the image of the achievement. The conclusion of an event in which one actor exerts power over another actor will be examined by each of the actors as it forms a sense of the achievement. This includes physical achievements (maintained territory, destruction, neutralized capabilities, and prevention) and cognitive achievements (recognition, formulated understandings, achievement of a settlement, adoption of international norms, and accepted rules of the game). This examination occurs by interpreting the situation as it is seen by the different populations and actors in local and international arenas. This interpretation has considerable implications for the level of legitimacy to continue to manage the incident or conclude it through deterrence, impose a situation, or reach a settlement. Hence cognitive failure can uproot physical achievements, while cognitive success can leverage them toward political achievements, but also compensate for the limitations of achievements on the battlefield or in the political campaign.

The central objectives of cognitive efforts include, therefore, leveraging the achievements of hard power, and as defined above, cognitive efforts are interwoven in all stages of military and political activity. At the beginning, they create the legitimacy for exerting hard or soft power. During the action, they enable the continuous exertion of various powers and provide the logic of their integration; the use of hard power thus places a cognitive emphasis on increasing the estimated cost of defeat for the adversary if it continues the conflict. At the end of the action, the cognitive effort emphasizes the achievement attained as a result of the use of the powers exerted, offsets the adversary's achievements, and works to maintain the achievement attained over time and to prevent later cognitive achievements by the adversary.

Israel, as a state actor that accepts international rules and standards, is also expected to cognitively emphasize humanitarian efforts, the importance

of international norms, compliance with international law, and integration of non-governmental organizations and civil society organizations in the processes of regulating and shaping the new reality.

Israel: Case Studies on Integrating Cognitive Efforts within Military Campaigns

In the current era, in which the international system has multiple actors of different kinds propelled by different logics, states are not necessarily the most influential actors in the arena. The international system is no longer solely examined in terms of the sizes of forces and the military capabilities at the disposal of states, or their economic, scientific, and cultural capabilities; this is a system in which cognition may be shaped by non-state actors (that can be directed by state actors), which do not act in accordance with the traditional and familiar rules of the game in the international arena. This reality, which is known as "asymmetric conflict," creates a situation of an almost built-in lack of symmetry in the struggle on cognition, and poses a number of questions related to cognitive efforts as an element that connects between hard power and soft power.

From Israel's standpoint, cognitive efforts aim to leverage achievements of the battlefield, translate them into political achievements, and create a stable security regime over time. There are a number of basic elements for managing a successful cognitive campaign:

a. International and internal conviction regarding Israel's legitimacy to operate in the designated arena.
b. Clear achievements on the battlefield, portrayed through documentation and facts, along with strategic communication that clarifies the purpose of military activity and the expected cost to the other side of continued fighting.
c. Imposition of Israel's conditions for a ceasefire on the enemy, subsequently followed by imposition of the principles of the settlement.
d. Complete coordination with the United States regarding the goals of the war and how to achieve them, while taking American interests into consideration.
e. Upholding of the laws of war, including by minimizing collateral damage and harm to non-combatants.

f. A social media campaign vis-à-vis designated target audiences in order to advance the Israeli narrative and shape the image of victory.
g. Counter cognitive efforts of the other side, such as false and unsubstantiated information (fake news).

A central challenge is the ability to leverage a military achievement for a political achievement through cognitive efforts. We will illustrate this through two case studies that represent two different archetypes: one can be defined as an "ongoing" event, while the other is an event that has clear start and end points.

Along the Gaza Border since the Spring of 2018

The so-called Marches of Return encouraged thousands of Gaza residents to march toward the border fence in order to penetrate Israeli territory. These developed into violent conflicts between the IDF and Hamas and other terrorist groups, which included the dispatch of incendiary kites and balloons, and rockets and mortar shells launched into Israeli territory; in response, Israel carried out air strikes on Hamas targets.

The Israeli military achievement, which prevented the penetration of terrorists and rioters into its territory and enabled the interception of rockets and mortars and sharply reduced damage, was significantly offset in the cognitive dimension following public diplomacy and public relations achievements by Hamas in the international arena (with the assistance of foreign media networks critical and even hostile toward Israel) and in the internal Palestinian arena (by convincing the Gaza public of the justness of the cause and recruiting it for the ongoing campaign against the "blockade" of the Gaza Strip). The ongoing cognitive campaign has had a number of peaks, such as the split television screen broadcast on May 14, 2018, with the harsh scenes from the clashes on the border of the Gaza Strip on one side, and the ceremony inaugurating the American embassy in Jerusalem on the other side, as if it were a different universe.[3] The ongoing conflict enabled seeing how both sides achieve cognitive successes: Hamas sought to revive the world's interest in the Gaza problem, while Israel sought to

3 Nevo Brand, Pnina Shuker, and David Siman-Tov, "'The March of Return' – Operative Achievement and Strategic Failure: A Test Case for Cognitive Warfare," *INSS Insight* No. 1063, May 30, 2018.

send a clear message to the Gaza population and to Hamas that crossing the fence is not possible.

At the same time, there were prominent cognitive gaps in that same conflict: Israel saw great importance in the knowledge that the majority of those killed were Hamas members, while the international mindset did not attribute great importance to this fact. The reason for this is the cognitive "proximity" between the Hamas movement and the residents of the Gaza Strip, who are seen as motivated by the hardship for which they blame Israel. The picture brimming with contrasts that was broadcast on television from Jerusalem and from the Gaza Strip undermined Israel's operative achievement, having taken action in order to maintain its security and its sovereignty. The large number of casualties on the Palestinian side strengthened the image of Israel's disproportionate use of force against civilians that demonstrated against it.

The picture described above illustrates a situation in which Israel did not properly prepare for the cognitive campaign in accordance with its basic components: it did not create the preliminary, accompanying, and subsequent account of the events in advance; did not sufficiently clarify Hamas's objectives; relied on its sense of the justice and legitimacy of its actions in defending its sovereignty; and did not manage to assess the negative possible consequences of the asymmetric confrontation in Gaza, especially against the backdrop of the celebratory and disconnected pictures from Jerusalem. Israel responded somewhat late, with a meager stock of pictures, videos, and facts to support its version that it made cautious and restrained use of force in order to maintain its sovereignty.

The incongruence between Israel's military activity and its cognitive activity led to ongoing instability in Israel's Gaza border region, and increased Hamas's motivation to continue to challenge Israel and exploit the momentum in order to improve its standing in the Palestinian arena and with respect to the international community. The negative consequences for Israel from the sequence of events on the border with Gaza were extensive: the Palestinian issue was restored to the center of the international stage; Hamas's legitimacy and the "path of resistance" were revived in the eyes of the Gaza public; international decisions against Israel were facilitated; and full responsibility for events in the Gaza Strip was ascribed to Israel.

Another round of escalation occurred in November 2018, when Hamas and other organizations fired some 500 rockets into Israeli territory. This time, the Israeli response was expressed in extensive air strikes on Hamas targets in the Gaza Strip, while minimizing harm to civilians and acceding to Hamas's request for a ceasefire. Israel thereby made clear that from the cognitive perspective it does not have an effective response to the problem of the Gaza Strip, and the event ended with a "victory image" for Hamas – the resignation of Defense Minister Avigdor Liberman.

The Cognitive Failure of the Second Lebanon War (2006)

The Second Lebanon War ended with a highly negative feeling among the Israeli public, which felt that operationally it was a missed opportunity or even a loss to Hezbollah, despite a series of clear operational achievements by the IDF. The achievements included: destroying Hezbollah's strategic array of surface-to-surface missiles; destroying the organization's nerve center in the Dahiya quarter of Beirut; intercepting rocket and missiles launchers; and translating the military achievement into a political achievement in Security Council Resolution 1701, which led to a change in the overt reality in southern Lebanon, the transfer of responsibility there from Hezbollah to the Lebanese government and army, and the deployment of an expanded peacekeeping force (UNIFIL) in the theater.[4]

From the cognitive perspective, here too Israel did not manage a cohesive cognitive campaign according to the basic elements described above. Internally, Israel was perceived as having lost: it did not succeed in returning the soldiers who were taken captive by Hezbollah – an event that in part constituted the grounds for going to war; it did not decisively defeat a sub-state actor with inferior military capabilities and powers; extensive faults were discovered in the ground forces' preparedness for an emergency; and the campaign continued far longer than planned, without ending the launch of rockets from Lebanon toward Israeli population centers. The most prominent expression of the cognitive failure was the widespread

4 Zipi Israeli, "'Did We Win or Lose?': Media Discourse in Israel about the Second Lebanon War, 2006-2016," in *The Quiet Decade: In the Aftermath of the Second Lebanon War, 2006-2016*, eds. Udi Dekel, Gabi Siboni, and Omer Einav, Memorandum No. 167 (Tel Aviv: Institute for National Security Studies, 2017), pp. 71-82.

demand in Israel to establish a commission of inquiry to assess the war.[5] In retrospect, impressive achievements following that war are evident, chief among them consolidating Israeli deterrence and establishing a stable border regime between Israel and Lebanon for the first time since the beginning of the 1970s.

Where does this gap come from? In this case too, the cognitive aspect was not managed properly: at the outset, the Israeli government presented overambitious war aims, considering the limitations that it imposed upon itself in the use of force, such as rejecting and delaying ground maneuvers and not damaging Lebanese infrastructure. The story of the war was woven only afterwards, such that there was no central idea directing cognitive efforts and spokespersons during the war; the military successes were downplayed and the failures emphasized, including on the part of the media and Israeli politicians. It is very difficult to achieve decisive victory in conflicts that are asymmetrical in capabilities and objectives; hence the results are not unequivocal, which led to an image of failure with respect to public expectations. Furthermore, the facts on the ground in Lebanon were discovered late, mainly for the Lebanese side, which while deterring it from another escalation against Israel for more than thirteen years (to date), did not change the negative image of the war among most of the Israeli public, even years later.

Israel did not manage to focus its cognitive efforts on its military achievements (eliminating Hezbollah's strategic array of surface-to-surface missiles; destroying the organization's operations center; destroying every launcher that launched medium range missiles, and more) and on providing its citizens with a sense of security in these achievements. Therefore, despite the strategic objective defined for the war – changing the security reality in southern Lebanon, distancing Hezbollah from the border, and severely harming the organization's strategic capabilities – a gap arose between the expectations of Israeli society and the results in practice.

Since it is difficult to judge the achievements of a war while it is raging, the prevailing sense among decision makers is often that fighting should continue in order to deepen military achievements and leverage them for

5 Udi Dekel, "The Second Lebanon War: The Limits of Strategic Thinking," in *The Quiet Decade: In the Aftermath of the Second Lebanon War, 2006-2016*, pp. 27-37.

political achievements. So it was during the Second Lebanon War: Hezbollah's condition was not properly assessed and the enormous damage done to the organization was not cognitively leveraged at the end of the first week of the war, when Israel could have ended the fighting, with Hezbollah surprised by the scope and intensity of the Israeli operation. Similarly, Operation Protective Edge against Hamas in the Gaza Strip in the summer of 2014, though it lasted 51 days, did not bring about a substantial change in the strategic situation.

Israel's delayed action and the lack of an effective cognitive campaign directed at increasing Hezbollah's and Hamas's concerns regarding Israel's unexpected leeway enabled these organizations to overcome the initial shock (which stemmed from the Israeli response that they did not expect) and adjust to the IDF's mode of action. This is supported by the words of Hezbollah Secretary-General Hassan Nasrallah, that had he known in advance that this would be Israel's response, he would not have approved the abduction of the Israeli soldiers. Hamas also admitted this regarding the damage to its strategic asset – the tunnels. Lacking a clear image of victory for Israel, Hezbollah's leader was able to declare victory despite having regretted abducting the soldiers, and the leaders of Hamas did likewise. In contrast, Israel immersed itself in internal criticism and commissions of inquiry into the failures. The sense of failure and/or success in past wars influences the motivation of the government, as well as the operative planning of the next war.

In conflicts such as those presented in the case studies described above – between a state and sub-state terrorist organizations, e.g., Hezbollah and Hamas – the asymmetry is a given dynamic. On the one hand, terrorist organizations are free of state responsibility, willing to hide among the civilian population and use it as a human shield, and direct their operations toward harming civilians on the other side. On the other hand, the state, in this case Israel, instilled in the Lebanese population, as well as the international community, the understanding that since Hezbollah turned the Lebanese villages and urban centers into launchpads for missiles and rockets, this made them military targets that would be hit hard in any war. Developing this understanding creates the legitimate foundation for Israel's use of hard power, if it becomes necessary. The message enters people's consciousness, serves Israel's deterrent image, and is included in Hezbollah's cost-benefit calculation when considering whether to escalate the situation. With respect

to the Gaza Strip, in contrast, Israel sends the message that there is no point in conquering it or even causing heavy damage there, which is interpreted by Hamas as providing it with flexibility and preventing the concern that its actions will bring about the toppling of its rule.

An asymmetric conflict is expressed not only in the way force is exerted, but also in the objectives of the war. For the sub-state enemy, its continued survival and the fact that it has not been defeated by a state and standing army is considered a victory (in the cases of Hezbollah and Hamas, this is also expressed in the continued launching of rockets at the Israeli civilian home front). In contrast, the IDF must create clear facts on the ground that cannot be manipulated by the enemy. The way to create these facts is to cause very heavy physical damage, potentially including ground maneuvers deep into enemy territory. Nonetheless, in order to stop the other side or convince it that continued fighting is not worthwhile, it is not sufficient to assess the balance of achievements and failures at the end of the war; cognitive manipulation must also be carried out on the organization's leaders and on the population that supports it to clarify the enormous extent of the damage that they can expect from continued fighting or from violating the ceasefire.

Conclusion

In the past, Israel was forced to take part in conventional wars, in which victory on the battlefield influenced their cognitive implications. This was the case during the War of Independence, the Six Day War, and the Yom Kippur War. As a result, in Israel there is a tendency to prefer the military option, which relies on the conception that the region in which we live only understands "the language of force" and is influenced more by the ability to cause damage to adversaries than by the use of tools of persuasion. This is a somewhat limited worldview. Today Israel needs a broader, more complex, and more sophisticated approach in which the cognitive aspect is of central importance in combining and synchronizing between the use of hard and soft power. If in the past cognitive efforts aimed mainly to enhance the effectiveness of the military act, today military force is exerted in part as a tool to create the desired cognitive effect.

The changing battlefield and the decline in the relevance and frequency of large scale military conflicts between standing armies, along with the increasing number of actors influencing the situation and the dynamic rules

of the game, have diminished the relative importance of military efforts and increased the importance of soft and semi-soft efforts accordingly, including cognitive efforts. Cognitive efforts are another dimension of the campaign to fulfill national security objectives, and aim to shape the perception of reality of different target audiences by combining subjective aspects with created facts on the ground.

The change in the nature of conflicts has led Israel to develop the conception of the "between wars campaign," or the "ongoing campaign," whose purpose is to maintain power and deter enemies while controlling the levels of escalation, in order to avoid crossing the intensity threshold to a state of war. The campaign between wars contains a toolbox that aims to strengthen and maintain Israeli deterrence over time, in a controlled and planned manner. This toolbox is made up of three levels that serve the objective: disrupting enemies' military buildup efforts; demonstrating Israel's growing capabilities through diverse, covert, and surprise operations; and developing the cognitive foundations among the adversary that deter it from the damage it can expect from escalating into war, along with mentally preparing the Israeli home front for behavior that will significantly reduce effective harm against it. In order to advance the aims of the campaign between wars and achieve effective influence on target audiences in the internal and external environments, the narrative (or stories) that we wish to instill in the target audiences need to match the actions directed toward shaping the reality. This is the purpose of the cognitive campaign.

Cognitive efforts towards the adversary's population and leadership, as well as the international arena, aim to create a narrative and achieve influence, which in Israel's case are translated into consolidating its standing in the local, regional, and international arenas, and removing possible barriers, limitations, sanctions, and damage to its legitimacy, especially when the use of power will be required in order to fulfill and/or defend interests. There are several examples from the current decade.

This article examines the hypothesis that cognition is a conceptual framework that connects hard and soft efforts that aim to achieve defined political and military objectives, through a number of examples. Additional measures that can cultivate cognitive efforts in order to achieve the objectives include:

a. Utilizing direct access to the adversarial population, whether through public diplomacy and social media or by providing humanitarian aid up to the level of local communities. An example of this is the Operation Good Neighbor project that Israel conducted on the Golan Heights, which aimed to demonstrate to the Syrian population that Israel is not a threat to it, but rather contributes and provides assistance.
b. Employing soft measures, such as economic leverage, water and energy arrangements, security and technological assistance, and initiatives for the private and civilian market in neighboring states. This can increase dependence on Israel and influence the cost-benefit calculations of regional actors in scenarios of military escalation.
c. Multi-dimensional cooperation with actors that have interests that are close to or overlap with those of Israel. The most prominent shared interest of Israel and the pragmatic Sunni states today is the concern about Iran's increasing negative influence in the Middle East, along with the need to neutralize the threat of Islamist jihadist terrorism. This is also the basis for Israel's cooperation with Jordan and Egypt and even with the Palestinian Authority's security forces. Cognitive efforts aim to strengthen the recognition of shared interests, as well as demonstrate Israel's unique contribution to the advance of these interests among potential partners.
d. Cyber warfare is also of great importance. While this is focused on neutralizing enemy capabilities, it also has a cognitive element – creating influence by assisting with cyber defense, as well as using it as a central platform to convey messages and illustrate the situation. A necessary condition for this is the use of new media, as well as traditional media, in order to achieve influence on social media discourse, both among the adversary's population and among the domestic public.
e. Domestically, Israel must cultivate the cognition of its citizens as a democratic and liberal society, based on hard power and soft power. In this case, government transparency is important, as is informing the public of strategic objectives and political and military goals, in order to set expectations and reinforce national resilience. In this way, the public will feel that it is a partner in these objectives and goals.

When the Intelligence Officer and the Public Diplomat Meet

Yarden Vatikay and Colonel O[1]

Background

On April 30, 2018 at 8:10 PM, Prime Minister Benjamin Netanyahu took the stage in VIP Hall 3 at the Kirya (IDF headquarters) in Tel Aviv, and before dozens of Israeli and international journalists dramatically unveiled materials from the Iranian nuclear archive, seized not long before by Mossad agents from the heart of Tehran. The press conference was broadcast live on television in Israel and worldwide, on websites and social media, providing exposure to millions of viewers.[2] The event was also mentioned in a speech by US President Donald Trump the following week (on May 8) as part of the motives leading to his decision to withdraw from the nuclear deal with Iran (JCPOA).

The press conference concluded almost two months of preparatory work following the clandestine raid conducted by a small group of intelligence, communications, and political officials. The preparatory work was characterized by constant tension between public diplomacy versus intelligence considerations. Many questions were discussed, such as: what is the purpose of the exposure and who are its target audiences? Which materials displayed will achieve the greatest effect? What kind of intelligence materials will best support the political messages? How should these materials be made

1 Yarden Vatikay until recently was the Director of the National Information Directorate in the Prime Minister's Office. Colonel O served until recently as the intelligence assistant to the Prime Minister's Military Secretary.

2 The picture and text of his speech appear on the website of the Ministry of Foreign Affairs at https://bit.ly/2kkNcIG.

Prime Minister Netanyahu at the UN General Assembly, September 27, 2018. Photo appears in the video of the Prime Minister's address on the Ministry of oreign Affairs website.

suitable for media display, and how might complex materials be simplified in order to be presented in a clear and accessible manner that could be grasped by the general public and target audiences? Which materials should not be revealed? What needed to be concealed? How would the exposure be perceived by the various target audiences, including in Iran? How could all this be done without jeopardizing intelligence sources and modus operandi?

This event serves as an instructive example of the importance of the close connection and fruitful dialogue between intelligence organizations and communications experts engaged in "influence" campaigns aimed at advancing national security objectives. One possible and significant conclusion to be drawn from the event is that a combined diplomatic-communications-intelligence effort is capable of leading to significant achievements in the political arena serving the most critical national interests.

Another example that illustrates the issue was provided in the Prime Minister's speech at the UN General Assembly on September 27, 2018. In this speech, Benjamin Netanyahu revealed two additional Israeli discoveries: a secret warehouse in Tehran in which the Iranians were concealing equipment used for their nuclear program, including nuclear materials, and three Hezbollah sites located next to Beirut's international airport that were used for the

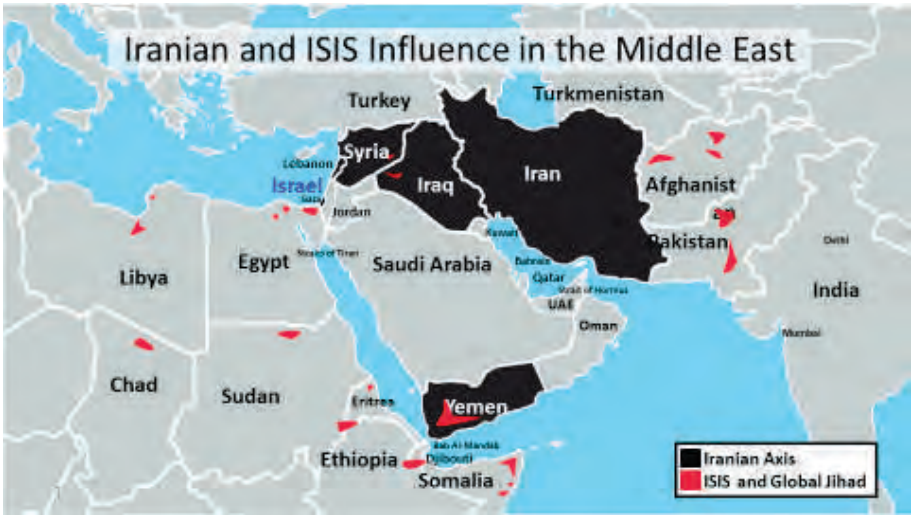
Iranian nuclear warehouse, Turquzabad, Tehran, displayed by Prime Minister Netanyahu at the UN General Assembly, September 27, 2018. See video of the address on the Ministry of oreign Affairs website.

development and production of precision guided missiles. The Prime Minister also added a specific deterrent message to these revelations: "Israel knows what you're doing, and Israel knows where you are doing it. Israel will never let a regime that calls for our destruction to develop nuclear weapons. Not now, not in 10 years, not ever."[3]

It was clear that these discoveries caused embarrassment in Iran and Lebanon and troubled their leaderships. Three days after the Prime Minister's speech, the Lebanese Foreign Minister led a tour for journalists to the sites in Beirut that Israel had exposed in order to refute the allegations and supposedly prove that no covert missile-production activity was taking place there. The IDF Spokesperson responded quickly, posting a short and humorous video that ridiculed these actions, showing how much can be done in three days, including removing missiles from the sites.

A third example of fruitful cooperation between the intelligence apparatus and public diplomacy officials is a slideshow prepared by the National Information Directorate for the Prime Minister, to help illustrate Israel's central interests and arguments. The presentation is used during all the

3 For a transcript and video of the speech on the Ministry of Foreign Affairs website, see https://bit.ly/2m28ZoW.



rom a slideshow prepared by the National Information Directorate

Prime Minister's meetings with heads of state and other senior officials. And indeed, at almost every diplomatic meeting with world leaders, whether in Israel or abroad, Prime Minister Netanyahu illustrates his remarks on the various issues with these slides. They include Iran's entrenchment in Syria, the Iranian influence and the presence of the Islamic State in the Middle East, the ranges of long range missiles that Iran is developing, attempts to execute terrorist attacks around the world that were foiled thanks to intelligence provided by Israel, Hezbollah's activity in southern Lebanon, Hamas's army of terror, and more. The military and intelligence components of the slideshow, which are updated daily, are based on high quality intelligence material. At the same time, the presentation is characterized by the simplicity of its messages and the effectiveness of the depicted images. The process of designing the slideshow is made possible through an ongoing dialogue between public diplomacy and intelligence officials at the Prime Minister's Office, and between them and the Prime Minister. The process involves a number of challenges: first, selecting a topic that needs to be added to the presentation; second, determining the information and data that can be used; and third, designing each relevant slide.

The graphic design process of the slideshow is by no means technical. Its importance is no less than the previous stages; the design stage is essential for achieving public diplomacy objectives. The central goal is to achieve

maximum simplicity and clarity of the message contained in each slide, such that will be instantly understood by the viewer. The result is a very visual slideshow, with minimal text and few figures, focusing on the core points (each slide relays only one message) and without burdening the viewer with too much information. Our experience in hundreds of meetings indicates that the slideshow is effective and enhances the messages conveyed by the Prime Minister in his diplomatic meetings.

Intelligence as a Central Tool for Public Diplomacy

The examples provided above illustrate the importance of intelligence information as a central tool for public diplomacy, emphasizing the need to make optimal use of intelligence material for the needs of "influence campaigns." Effective use of intelligence is relevant and meaningful at all levels and organizations in Israel that are engaged in influence/public diplomacy campaigns. For example:

a. The ability of the IDF Spokesperson to refute false information, which can become a negative smear story at a dizzying speed, depends to a large extent on his ability to receive intelligence information in real time and reveal it to the media.
b. The ability of the Prime Minister's Office and the Ministry of Foreign Affairs to cope with "public diplomacy/political attacks" in the international arena depends to a large extent on relevant intelligence information.
c. The ability of the Ministry of Strategic Affairs to cope with delegitimization attacks against Israel can be fortified by the prudent use of intelligence.

Maximum utilization of intelligence for the use of public diplomacy is based on a series of principles, some of which are also challenges. The main ones include: simplifying the message that arises from the intelligence material; deciding whether or not there is a need to "blanch" intelligence materials; and adhering to professional ethics.

Simplifying the Message and the Intelligence Material

Public diplomacy messages directed at target audiences like world leaders, or the international press, face two main challenges. The first is the lack of familiarity of these audiences with the issues discussed, for example, the complex Middle East reality or technological issues. These audiences will have difficulty coping with a complex message that requires prior or

deep knowledge and understanding. The second pertains to leaders and populations that have a personal or historical set of beliefs and conceptions that are inconsistent with reality, sometimes contradicting simple facts and information. In this case, the messages conveyed to them need to be sharp, clear, and fact-based enough to penetrate that layer of existing beliefs and opinions.

Simplicity seems to be an obvious principle: the simpler the message, the better it will be received. However, experience shows that the conventional wisdom regarding this notion does not accord with the powerful "punch" that may be needed to achieve the desired result – namely a catchy understandable message that sticks in one's mind. This is especially true with respect to the conveying of complex messages from the political-military world, which are also based on intelligence materials.

In order to formulate a brief and clear message, it is necessary to take the initial concept and the existing intelligence materials and information on the given issue and put them through a process of reduction, simplification, and refinement, until the message and the way it is presented can pass the test of the "quick look" or first hearing. The intention is to reach a situation in which listening to the message once or taking a quick look at a visual representation of it are enough to be understood and consequently convinced. To a certain extent, the reduction process contradicts the existing approach in the intelligence community toward the use of information. Due to the nature of their work, intelligence experts tend to maintain the complexity of each phenomenon, the different angles that exist for understanding it, and the subtleties that it contains. However, maintaining such complexity and nuances can sometimes "kill the message."

Another common tendency of many intelligence officials is to present a wide range of details to explain a phenomenon. This tendency is based on the premise that adding details strengthens the validity and credibility of the statement. However, the overabundance of details seriously harms the effectiveness of the message, at least when it is directed to the general public. For example, a few years ago, one of the intelligence organizations prepared a special presentation for public diplomacy purposes following a military operation as part of the efforts to counter delegitimization of Israel. Preparation of this presentation lasted weeks, with hundreds of work hours invested in it. But when it was presented to public diplomacy officials, their

immediate response was that it was overloaded with details, thus blurring the message (in addition to the fact that it was submitted too late for effective use in the media), and the whole effort was shelved.

The conclusion is that the message must be brief and focused. A brief message has few words, and if expressed, it must appear in one display (picture, map, or other visual image). A focused message is one that minimizes complexity and ambiguity. In addition, it is important to consider how suitable the message is to its specific target audience. For example, an infographic that presents ranges and distances of enemy missiles should be prepared in a number of versions that use different measuring systems (km, miles), making it readily suited to the measuring system found in each country. Another example: if we want to address Iran's terrorist activity around the world, it is best to prepare versions that provide incidents from different international locations, so that in each country the incidents that occurred within or near its territory can be highlighted.

Getting the target audience to identify with the message can be better achieved by adapting it to the culture and internal worldview of that audience. Prominent examples can be seen in the video clips that Prime Minister Netanyahu posts occasionally in a direct appeal to the Iranian public and highlight Iran's extreme leadership. These clips include references to events that take place in Iran and are recognizable to the average citizen there. They might include mentioning streets and places in Iran or real problems that are of local concern, such as air pollution and water shortage. Many Iranian citizens respond to these videos favorably and even emotionally, because the sense of familiarity with Iranian culture, and even the effort to get to know them, makes them feel respected.

"Blanching the Secret": The Use of Classified Information in Public Diplomacy Campaigns

Public diplomacy pertaining to issues of policy and national security sometimes involves presenting the negative actions and intentions of enemies and adversaries. Thus, it must sometimes make use of classified information and intelligence materials in order to expose enemy plans and actions of which the target audiences are not aware. This raises questions and creates tensions relating to the diplomatic and political benefits of exposing such

information versus the risks to intelligence sources and the possible harm to operational methods.

The exposure of the nuclear sites in Iran and the missile production sites in Lebanon are prominent and current cases that underline this tension. But they are not precedents. One major example that received publicity was revealed on June 6, 1967, the second day of the Six Day War, when the political leadership in Israel decided to publicize a classified conversation between Egyptian President Gamal Abdal Nasser and King Hussein of Jordan that was recorded by Israeli military intelligence. In the conversation, the Egyptian President offered to declare that the United States and Great Britain participated in the attack on the airfields in Egypt. The following day, the Arab media did indeed begin to broadcast this message, which led to an uproar in the Arab world and to political pressure on the US. After deliberation, the Israeli political leadership decided to release the recorded conversation, anticipating that Egypt might try to drag the Soviet Union into the war, based on their bilateral defense treaty, which was followed by the USSR's intention to support Egypt in case the US were to do so on Israel's behalf.

In such cases, the best way to choose between public political needs and the risk to intelligence sources is to have a joint consultation between the political leadership and the intelligence community on the nature of the material and the method and degree of its exposure. The political echelon retains the right to make use of intelligence information even if the professional echelon opposes its exposure. This was the case in the Nasser-Hussein phone call, despite the opposition of then-Director of Military Intelligence Aharon Yariv.

More recently, Prime Minister Netanyahu has articulated this approach, stating that "we are a country that has intelligence, not intelligence that has a country." However, the country's leadership should prefer a shared dialogue with the heads of the intelligence community, so that any final decision will be based on an understanding of all the considerations, including the perspective of maintaining intelligence assets. This has in fact been done in practice, in the past and the present.

Along with these momentous exposure events, there is less dramatic and much more frequent and daily use of intelligence materials for the purpose of public diplomacy. Intelligence materials are used in the ongoing activity of the political leadership, in its public statements, in diplomatic meetings,

and are released to the media. Coordination regarding the level and form of exposure of sensitive information occurs daily in the professional echelons between intelligence, communications, and diplomatic officials.

In general, the need for simple messages in public diplomacy considerably helps reduce potential harm to sources. The process of simplifying the message leads to "rounding numbers" and to schematic presentation of visual information, thus creating some distance from the specifics found in intelligence material and the sources on which it is based.

Intelligence at the Service of Policy

Public diplomacy officials are committed first and foremost to supporting policy, and so tend to leave content that does not serve that purpose "outside the editing room." Public messages will not, of course, include falsehoods, but neither must they necessarily present the entire picture with all of its angles. Intelligence people, on the contrary, have more comprehensive knowledge of the picture, and their professional ethics require adhering to that aspect. Therefore, the work of preparing public tools, items, and content needs to unfold as a dialogue between the two, with the public diplomat attempting to mold content in a way that best serves policy and effectively conveys the message, and the intelligence official assisting him in his work, while ensuring that the final product remains true to reality as the intelligence community understands it. This inherent tension, along with the work of simplifying and refining the message ("keep it simple") and illustrating it in a visual and catchy manner, leads to the best end products that serve the national interests of the state.

Conclusion

Colossal attempts are made in world politics in order to shape the narrative and influence public opinion. This is done through the press, on social media, in WhatsApp groups, and in cyber operations, sometimes mixing facts and rumors, truths and lies. Israel's many challenges in this arena require it, more than other states, to invest in effective public diplomacy efforts to maintain its freedom of operation and promote its national objectives and interests.

At the same time, Israel's intelligence prowess offers important capabilities and opportunities that can be tapped for the purpose of political-public diplomacy efforts. Furthermore, the controlled exposure of intelligence

materials can help not only with the general dissemination of public messages among broad target audiences, but also serve as an actual operative tool, that can help develop legitimacy for conducting kinetic military operations, or even replace them.

The utilization of intelligence for purposes of public diplomacy and efforts to influence should be expanded. Possible directions include augmented cooperation between intelligence agencies and those involved in public diplomacy; development of the intelligence community's knowledge of the public diplomacy echelon and objectives and the ability to contribute to it; and the development and acquisition of technologies that support and advance these national goals. Public diplomacy is and should be perceived even more than before as a national effort that needs to be supported by any resource available, especially by the intelligence community.

Consciousness as Leverage: The Israeli Campaign regarding the Iranian Nuclear Program

Ronen Dangoor[1]

Background

Iran's nuclear program has constituted a central security issue for Israel over the past two decades. Against this backdrop, Israel has conducted a multifaceted drive to block it, in part through a complex cognitive campaign that extended from the summer of 2002 – when the Iranian nuclear program was revealed – to July 2015, when the agreement between Iran and the world powers on restricting the nuclear program was signed.

This article discusses the central characteristics of the cognitive campaign, which included four main components and motifs: the first and most basic, which was a constant for the entire period, was exposing and raising awareness of the dangers of the Iranian nuclear project; the second emphasized the other threats that the Iranian regime poses, chief among them its aggressive policy, which includes involvement in terrorism and extensive activity to develop long range missiles; the third component was the threat of a possible Israeli military attack on Iran's nuclear facilities, which was prominent as a central narrative mainly during the years 2010-2012; and the fourth component, which dominated from 2013, dealt with the negotiations between the world powers and Iran and with the nuclear deal that was reached between them. The struggle against the agreement has intensified in recent months against the backdrop of the United States' withdrawal from it, but that development is not addressed here due to the lack of sufficient perspective.

1 Ronen Dangoor is a former Deputy Director of the Research Department at the Prime Minister's Office.

The article focuses on a number of basic questions: what were Israel's main positions on the question of the Iranian nuclear program and, in this context, what were the main goals of the cognitive campaign? What tools did Israel make use of in the campaign? At which target audiences was it directed? And which of the narratives in the campaign were enduring and which changed over time? Finally, the article will attempt to assess the campaign's level of success, whether a connection can be found between the cognitive activities and the actual results, and what general conclusions can be drawn regarding long term cognitive campaigns.

Iran's Nuclear Program: Israeli Assessments, Interests, and Positions

The official Israeli positions regarding Iran's nuclear program remained consistent and stable throughout the campaign – that Iran's aim is to achieve an arsenal of nuclear weapons. All of the Iranian delays over the years were presented as tactical and temporary, and as resulting from deception, technical difficulties, or diplomatic considerations. According to the Israeli position, Iran has been deceiving the international community and concealing its capabilities and its true intentions. Moreover, Iran employs an aggressive strategy that includes the development of missiles, support for terrorist organizations, and intervention in neighboring countries.

The Israeli interests included, as a top priority, halting the nuclear program, and only afterwards restricting Iran's regional power and stopping its support for terrorist organizations. Unlike other threats, the Iranian nuclear capability is seen in Israel as an existential threat. According to the Israeli narrative, Iran's ambition to achieve military nuclear capability reflects its basic ideology and is part of the objective of destroying the State of Israel. The combination of these intentions and achievement of the capability to use nuclear weapons is seen by Israel as an intolerable potential danger. In addition, Israel fears that Iranian possession of nuclear weapons will lead to a regional nuclear arms race in which Saudi Arabia, Turkey, and Egypt might participate. Nuclear arms in the hands of Iran would also, in Israel's assessment, lead to the strengthening of Iran's regional standing and serve one of its main goals – situating itself as a hegemonic regional power.

Israel's actions in its struggle against Iran's nuclear program followed the Begin Doctrine, according to which it must prevent enemy states, such

as Iran, from acquiring nuclear weapons, even if this requires the use of military force. Israel's red line regarding Iran's nuclear efforts was to prevent it from enriching uranium at high levels or from producing plutonium, and Israel's overall ambition was to deprive Iran of its enrichment capabilities. The premise was that the production of fissile material is a critical component of the Iranian nuclear project.

The Cognitive Campaign

The main goal of the campaign was to cause the international community, and especially the United States, to take action to stop the Iranian nuclear program, as Israel cannot do so alone. The prevailing assumption was that the means at Israel's disposal, including a military attack, would not stop or eliminate the Iranian program, but only delay it, as confirmed by former Defense Minister Ehud Barak.[2] Basing the campaign on international assistance also stemmed from the norms that have taken shape in the international system against the proliferation of nuclear weapons, and from the American view that saw Iran as a threat to regional stability and to American interests. While the campaign involved expressing Israeli positions and assessments, this was intended not only for the purpose of public diplomacy, but also to explain the need for determined international action, and especially as leverage for putting international pressure on Iran.

Intelligence Assessments as a Basis of the Campaign

The cognitive campaign was based on professional assessments by the Israeli intelligence agencies. The political leadership relied on this information and on statements by senior intelligence officials, which were meant to lend the campaign validity and credibility. At the same time, the political leadership at times interpreted some of the data differently and emphasized aspects other than those highlighted by the intelligence community.[3] For example,

---

2 For example, when Barak was asked in a press interview about the option of attacking Iran, he answered: "We are not deluding ourselves. Our goal is not to eliminate the Iranian nuclear program…if we succeed in delaying the program by a few years, there is a good chance that the regime will not survive…so the goal is to delay." See Ari Shavit, *Haaretz*, August 10, 2012, https://bit.ly/2ViD1RZ [in Hebrew].

3 On the intelligence work on the Iranian nuclear issue, see Sima Shine, "The Intelligence Challenges of the Iranian Nuclear Issue," in Shmuel Even and David Siman-Tov, *The*

occasionally, relatively moderate declarations by senior officials from the Israeli intelligence community were published[4] that contradicted the leading narrative of the political leadership,[5] including assessments that Iran had not yet decided whether to develop nuclear weapons.[6] Some of the intelligence assessments were close to those of foreign intelligence officials on certain points. Despite these gaps, the messages of the political leadership and the military leadership in Israel regarding the danger of an Iranian military nuclear program and Iran's regional and terrorist activity usually concurred.

The Distribution Channels and Target Audiences of the Messages

The Israeli campaign in its entirety was led by Prime Ministers Ariel Sharon, Ehud Olmert, and Benjamin Netanyahu, as well as by their defense ministers, especially Ehud Barak. There were several reasons for it being led by the highest echelons: this is a strategic issue that Israel sees as being of supreme importance; the campaign was intended to influence other leaders in the international arena; and handling the issue required close relations with the US administration.

The campaign was directed at five main target audiences: the American administration, whose decisions with respect to the Iranian nuclear program are decisive; the Iranian regime, which Israel sought to deter; other world governments, in Europe and Asia, and specifically China and Russia; at American and world public opinion, hoping it would lead to further pressure on decision makers; and, finally, at the Israeli public, in order to recruit its support for the government's policy.

The two main channels of dissemination were state diplomacy and public diplomacy. For the latter, relatively little use was made of the official agencies, such as the Government Press Office. Even the IDF Spokesperson

---

Challenges of the Israeli Intelligence Community (Tel Aviv: Institute for National Security Studies, 2017) [in Hebrew].

4 Yoav Zeitun, "Director of Military Intelligence: Calls in Iran to Reconsider the Nuclear Program," *Ynet*, March 14, 2013, https://bit.ly/2VhMysu [in Hebrew].

5 "Mossad, CIA Agree Iran Has Yet to Decide to Build Nuclear Weapon," *Haaretz*, March 18, 2012, https://bit.ly/2SVQOBf [in Hebrew].

6 "Director of Military Intelligence: 'Iran Has Not Yet Decided Whether to Develop Nuclear Weapons,'" *Walla News*, February 2, 2012, https://bit.ly/2U5hpbg [in Hebrew].

was barely involved in the campaign. A significant portion of the public messages were conveyed in speeches, declarations, interviews, and briefings by the political leadership for the media in Israel and worldwide. During the period under discussion, there was almost no use of social media for conveying these messages. Prime Minister Netanyahu's Facebook account was used for redistributing his statements and speeches, and in effect served as another medium of communication.[7] Reports by the International Atomic Energy Agency and by research institutes were promoted and publicized, especially when they strengthened Israeli messages. The public diplomacy was intended for all of the target audiences, while the diplomatic efforts were aimed primarily at the level of decision makers within the American administration, and subsequently at other world leaders. In addition, information and messages were communicated to professionals, such as intelligence agents and academics.

Main Messages and Rhetoric

The majority of Israeli spokespeople described the Iranian nuclear project in the most severe terms. The agreed-upon definition from an early stage was that if Iran achieves nuclear capability, this could create an "existential threat" towards Israel.[8] The impression was that Iran was relentlessly progressing towards developing nuclear weapons,[9] and the intelligence assessments supported the political leadership's position that the sense of urgency on preventing this development should be emphasized, e.g., the statement attributed to the director of Military Intelligence, claiming that

7 Benjamin Netanyahu's Facebook account: https://bit.ly/2VhMCIK.

8 In an article published in *Yediot Ahronot* in February 1993 titled "The Great Danger," Netanyahu claimed that nuclear weapons in the hands of Iran would constitute an existential threat toward Israel. He wrote that Iran could achieve this in 1999, and the entire world should rally to stop it: https://bit.ly/2Iwszoj; see also Prime Minister Ehud Olmert's speech at the US Congress: https://bit.ly/2Veu1Nt. Later statements by Netanyahu, this time as Prime Minister, continued to claim that nuclear weapons in the hands of Iran would threaten Israel's existence. See, for example, a television interview with Ilana Dayan on *Uvda* in November 2012: https://bit.ly/2GIHpGo [in Hebrew].

9 Maya Bengal, "Military Intelligence: Iran Stampeding toward Nuclear Weapons," *nrg*, September 21, 2008, https://bit.ly/2GZ3P5N [in Hebrew].

"the nuclear hourglass" is running out.[10] According to the Israeli campaign, the time when the threat was liable to be realized was always "in three to five years."[11]

The rhetoric and the terms used by the media to describe Iran's nuclear efforts were influenced by military slang. Iran was described as "stampeding" towards nuclear weapons,[12] as waiting for the right time "to storm towards the bomb," as being liable to "enter the immunity zone," or as already having reached "the point of no return."[13] As a result, Israel was described as having "a sword upon its neck" and as facing, each year anew, "a decisive year."[14] Starting in 2010, Israeli messages stated that Iran had already "crossed the technological threshold."[15] In order to intensify the sense of emergency and to pressure the Iranians, a seemingly dichotomous choice was publicly presented between two possibilities: "bomb or bombing."[16] A third possibility, employing economic pressure and the diplomatic path, did not usually receive

10 Anshel Pfeffer, "Director of Military Intelligence: The Nuclear Technology Clock in Iran has Almost Completed its Rotation," *Haaretz*, December 14, 2009, https://bit.ly/2SmXKlw [in Hebrew].

11 See, for instance, statements by officials from the early 2000s onwards, e.g., Gad Lior, "Defense Minister Binyamin Ben-Eliezer: 'Within 4 Years Iran Will Threaten Israel with Nuclear Weapons,'" *Yediot Ahronot*, July 10, 2001 [in Hebrew]; Ronen Bergman, "Last Stop on the Way to the Bomb," *Yediot Ahronot*, July 8, 2005 [in Hebrew]; Orly Azoulay, "Prime Minister Olmert: Within a Few Months, Iran Will Be Able to Put Together a Nuclear Bomb," *Yediot Ahronot,* June 22, 2006 [in Hebrew].

12 For example, the Director of the Military Intelligence Directorate's Research Department, Yossi Baidatz, in an overview for the government on September 21, 2008: Barak Ravid, "Iran Stampeding towards Nuclear Bomb," *Haaretz*, September 22, 2008, https://bit.ly/2T7wD2v [in Hebrew].

13 Former Director of Military Intelligence Amos Yadlin in an interview with Ben Caspit: "Iran Passed the Point of No Return a Long Time Ago," *nrg*, January 21, 2012, https://bit.ly/2U4gnMW [in Hebrew].

14 For example, the Director of Military Intelligence Aharon Ze'evi-Farkash claimed in August 2004 that "in 2005 it will become clear whether Iran will succeed in producing nuclear weapons," and warned that "in 2005 we are going from the year of shock to the decisive year": *Ynet*, August 30, 20014, https://bit.ly/2SUyF6S.

15 "Director of Military Intelligence to Government: Iran Has Crossed the Nuclear Threshold," *Ynet*, March 8, 2009, https://bit.ly/2BP8XWR [in Hebrew].

16 Former Defense Minister Barak explained the dilemma well in an interview with Gidi Weitz: *Haaretz*, January 14, 2015, https://bit.ly/2Ep2bsf [in Hebrew].

credibility.[17] Even after the strictest sanctions were imposed on Iran during the years 2011-2012, the Israeli leaders publicly doubted their ability to change the Iranian policy and stop Iran's nuclear program, and emphasized the need for a credible and explicit military threat.[18]

Over the years, relatively moderate statements met with criticism, in part because they undermined the narrative of an immediate Iranian threat. An example of this is the responses to the declaration by then-Mossad Director Meir Dagan, who predicted early in 2011 that Iran would not achieve nuclear weapons before 2015.[19] Former National Security Advisor Giora Eiland, for example, countered that such statements are problematic, since they "may cause the world to relax" and reduce the pressure on Iran.[20]

Differing Interpretations regarding "Nuclear Capability" and the Status of the "Nuclear Threshold"

Part of Israel's difficulty in stressing the severity of the Iranian nuclear threat stemmed from the conceptual and interpretation gap between it and the United States and European countries. The Israeli approach to assessing how long before Iran might develop nuclear weapons was based on the "worst case scenario," while the US and Europe referred to "the most likely timeframe." Furthermore, a central component of the Israeli assessment was the buildup of Iranian capabilities, with an emphasis on the ability to enrich uranium, while the US and the other world powers also related to the weapons development path and the intentions of the Iranian leadership, especially the question of whether a decision had already been made to renew efforts to develop nuclear weapons.[21]

---

17 Gideon Alon, "Director of Military Intelligence: After March 2006 there Will be No More Point in a Diplomatic Effort regarding the Iranian Nuclear Program," *Haaretz*, December 1, 2005 [in Hebrew].

18 Netanyahu also repeated this message in his speech to the UN in September 2013, and even warned that Israel was willing to take independent action against Iran. "Israel 'is Prepared to Act Alone against Iran,' Netanyahu Says," *The National*, October 1, 2013, https://bit.ly/2ErAXBq.

19 "Meir Dagan: Iran Will Not Attain a Nuclear Weapon until 2015," *Maariv*, January 6, 2011 [in Hebrew].

20 Sara Leibowitz-Dar, "Like Her Scream?" *Maariv*, January 14, 2011 [in Hebrew].

21 Yossi Melman, "Between Two Nuclear Clocks," *Haaretz*, March 19, 2009, https://bit.ly/2STAL6O [in Hebrew].

In November 2007, a National Intelligence Estimate (NIE) was published, stating that Iran had stopped its project to produce nuclear weapons in 2003, and since then had not yet made a decision to renew it.[22] This assessment was rejected by Israel, and at the time also angered US President George Bush, who later recalled in his memoirs that the NIE undermined the diplomatic efforts to create a unified front against Iran.[23] In November 2011, an International Atomic Energy Agency (IAEA) report confirmed the American intelligence estimate from 2007. The report noted that until 2003, a project to develop nuclear weapons existed in Iran, that Iran lied about it and hid information related to it, and that a few areas of nuclear research continued until 2009.[24] The IAEA's final report, which was published in 2015 and summarized the agency's efforts regarding the issue of possible military dimensions (PMD) of the Iranian nuclear program also came to the same conclusions.[25]

The Non-Nuclear Iranian Threat

The cognitive campaign that Israel conducted focused on the Iranian nuclear threat, but in order to strengthen it and undermine Iran's standing, there was a constant effort to tarnish Iran's image and position it in the world's consciousness as "the regional source of evil." Among other things, these efforts emphasized the Iranian regime's ambition to destroy Israel, its aggressive behavior in the region, its intention to control the Middle East by creating a "Shiite crescent," and its worldwide terrorist activity. The Iranian missile program was highlighted as a central threat in two ways: both as

22 See the non-classified portion of the report: https://bit.ly/2Dd0JXW; Amir Oren, "American Intelligence: Iran Can Develop Nuclear Weapons but Has Not Yet Decided to Do So," *Haaretz*, February 3, 2010 [in Hebrew].

23 George W. Bush, *Decision Points* (New York: Crown Publishing, 2010), pp. 418-19. Bush writes: "I do not know what motivated the intelligence agents to write such a report… maybe they were influenced by their failure in the Iraq War. In any case, from that moment I didn't have the practical option of putting a military option on the table… and our diplomacy was undermined."

24 "Implementation of the NPT Safeguards Agreement and Relevant Provisions of Security Council Resolutions in the Islamic Republic of Iran," Board of Governors (GOV/2011/65), November 18, 2011, https://bit.ly/1Nsifrx.

25 "Final Assessment on Past and Present Outstanding Issues regarding Iran's Nuclear Program," Board of Governors (GOV/2015/68), December 15, 2015, https://bit.ly/2w3Bpno.

an inseparable part of its buildup of military nuclear capability and as the conventional offensive capability that in its own right threatens Israel, the Gulf States, and American bases in the region.

Much publicity was given to Iranian military maneuvers and to Iranian technological developments, as well as to missile test launches.[26] Later, Israeli leaders attempted to highlight Iran's intention to develop intercontinental missiles,[27] in order to emphasize its potential direct military threat towards European countries and the US.

An Israeli attempt was also made to strengthen the jihadist-terrorist image of Iran's leadership and to compare it to al-Qaeda and ISIL.[28] The Israeli political leadership presented the thesis that the extremist global Muslim "terrorism monster" in effect has two branches, similar in their goals and methods: one extremist Sunni (al-Qaeda and later ISIL) and the other extremist Shiite (Iran and Hezbollah).[29]

Along with all these, emotional aspects and historical analogies were emphasized so as to establish the legitimacy of the Israeli sense of emergency and the need to halt Iran's nuclear program. Prime Minister Netanyahu and other Israeli spokespeople made considerable use of Holocaust analogies: the Iranian regime was compared to the Nazi regime;[30] Iranian President Mahmoud Ahmadinejad (2005-2013) was compared to Adolf Hitler; the Iranian nuclear facilities were presented as analogous to the extermination camps in Poland;[31] and later the nuclear deal between the world powers and Iran in 2015 was even compared to the Munich Agreement.[32]

---

26 Ephraim Kam, *From Terrorism to NuclearBombs: The Significance of the Iranian Threat* (Tel Aviv: Ministry of Defense Publishing House, 2004) [in Hebrew].

27 Netanyahu's speech at the AIPAC convention, March 6, 2012, *Wikisource*, https://bit.ly/2HZzVjV.

28 Netanyahu: "ISIL Burns People and in Iran They Hang Them," *Channel 10 News,* February 4, 2015, https://bit.ly/2GUXSqu.

29 Public diplomacy video of the Prime Minister's Office, July 1, 2015, https://bit.ly/2GGT9JK.

30 Peter Hirschberg, "Netanyahu: The Year is 1936 and Iran is Germany," *Haaretz*, November 14, 2006 [in Hebrew].

31 For example, Aluf Benn, "Netanyahu Nearing War with Iran," *Haaretz*, March 6, 2012 [in Hebrew]. Shmuel Rosner, "Playing the Holocaust Card," *New York Times*, April 25, 2012.

32 "Ministry of Defense: The Nuclear Deal with Iran – Is Like the Munich Agreement

A poll conducted in April 2012 found that the vast majority of the Israeli public – 74 percent – believed that nuclear weapons in the hands of President Ahmadinejad could constitute an existential threat towards the State of Israel.[33] In August that year, it was found that 37 percent of the Israeli public believed that if Iran acquires nuclear weapons, a "second Holocaust" is indeed possible.[34] The cognitive campaign led Israeli spokespeople to disproportionately repeat certain elements of Iranian propaganda, and thus actually strengthened it.[35] For example, considerable emphasis was placed on Iranian statements regarding the ambition to destroy Israel, as well as on statements by senior Iranian officials that denied the Holocaust. The words and actions of President Ahmadinejad served the Israeli campaign well, as did pictures from the annual hate parades on Jerusalem Day and slogans from the conference on Holocaust denial that Iran organized.[36] As mentioned previously, the Israeli campaign identified the concept of a "nuclear Iran" with the motif of "destroying Israel." The combination of this identification and the frequent warnings of the pending materialization of the threat increased the anxiety of the Israeli public. On the other hand, some senior Israeli officials claimed that the main goal of the Iranian nuclear project was to create deterrence and not necessarily to attack Israel.[37]

The Option of a Military Attack on the Iranian Nuclear Facilities

Until 2009, when Benjamin Netanyahu returned to the position of Prime Minister, the public Israeli position was that the international community needs to lead the handling of the Iranian nuclear issue, that Israel will not conduct an independent attack on Iran's nuclear facilities,[38] and that it must

with Nazi Germany," *Ynet*, August 5, 2016, https://bit.ly/2Iz9cLj [in Hebrew].

33 Arutz Sheva poll, April 18, 2012.

34 *Maariv* poll, August 10, 2012.

35 See, for example, Ron Schleifer, *Psychological Warfare* (Tel Aviv: Maarachot, 2007).

36 Barak Ravid, "Ahmadinejad Denies the Holocaust in Order to Destroy Us," *Maariv*, December 11, 2006, https://bit.ly/2GDwLB3 [in Hebrew].

37 Former Defense Minister Ehud Barak made statements in this spirit on several occasions, for example in November 2011 in an interview with the Bloomberg network: "Barak: If I Were Iranian, I Would Probably Want Nuclear Weapons," as reported in *Ynet* on November 17, 2017, https://bit.ly/2E6bnjX [in Hebrew].

38 Then-Prime Minister Ariel Sharon made statements in this spirit, for example in

remain in the background on this issue. Although there were statements by senior Israeli officials during those years that Israel does not rule out an independent attack, these were not frequent and did not involve an organized campaign.[39]

During George W. Bush's presidency (2001-2009), the US held that Israel must refrain from attacking the Iranian nuclear program on its own,[40] and added an American commitment to prevent Iran from acquiring nuclear weapons.[41] At the same time, vis-à-vis Iran's leadership, the Americans tried to maintain the image of a credible military option led by the US, which even received support from the British Prime Minister at the time, Tony Blair.[42]

This was the background to the gradual rise during the years 2010-2013 of the Israeli attack option as a third component of the campaign. Dr. Daniel Sobelman discussed this aspect in a study published in the US in the summer of 2018.[43] Sobelman argued that Prime Minister Netanyahu and Defense Minister Barak decided that the way to prompt the Obama administration to take determined action against Iran was to pose an ultimate threat in the form of an independent Israeli attack on the Iranian nuclear facilities. This step aimed to cause the US and its partners to impose "crippling" sanctions on Iran and to isolate it diplomatically, to deter it by presenting a credible military option, and to secure an unequivocal commitment by the US administration to prevent Iran from acquiring nuclear weapons.[44]

---

an interview with Fox News in May 2005: Nathan Guttman, "Sharon: Israel is Not Considering an Attack on Iran," *Walla News*, May 14, 2005 [in Hebrew].

39 See, for example, Amos Harel, "Shaul Mofaz: Israel Must Prepare to Defend Itself against the Iranian Nuclear Threat, with All This Entails," *Haaretz*, January 22, 2006 [in Hebrew].

40 "The Washington Files," *State Department Briefery*, January 17, 2006; "Cheney Warns of Iran Nuclear Threat," *Washington Post*, January 21, 2005.

41 Udi Evental, "The United States and the Iranian Nuclear Challenge: Inadequate Alternatives, Problematic Choices," *Strategic Assessment* 9, no. 1 (2006): 24-32, https://bit.ly/2lVmvuO.

42 Parisa Hafazi, "Blair Urges UN to Consider Action on Iran," *Reuters*, January 11, 2006.

43 Daniel Sobelman, "Restraining an Ally: Israel, the US and Iran Nuclear Program, 2011-2012," *Texas National Service Review* 1, no. 4 (August 2018), https://bit.ly/2XtjTma.

44 Ibid.

According to Sobelman's study, in order to convey the message of being prepared for a military strike, Israel took a variety of steps, including air force exercises,[45] media statements, leaks to the press, and discussions with senior American officials. Ehud Barak, Defense Minister at the time, claimed in a 2017 interview that the intention behind the public demonstration of attack capability was twofold: to intensify the pressure of the world powers on Iran and to prepare the ground and receive legitimacy for an attack, if and when a decision to launch it were to be made.[46]

At the beginning of 2009, Barack Obama began his term as US President and continued the strong American opposition to an independent Israeli attack on Iran,[47] in part out of concerns that the United States would be drawn against its will into the military campaign. At the same time, Obama, from the start of his term, looked for an effective diplomatic path for handling the Iranian nuclear issue.[48] Early the following year, an assessment was published in the American media that Israel was serious in its intentions and preparations to attack the Iranian nuclear program, and that an independent Israeli attack should be taken into account.[49] According to Sobelman's study, starting at the end of 2011, many senior Obama administration officials believed that the Israeli government was seriously preparing for such an attack option. Administration staff even made public warnings to Israel not to do so.[50]

---

45 Different Israeli spokespeople emphasized the air force exercises. For example, Yaakov Amidror was quoted as saying that the air force had already practiced flights with ranges of 2,000 km: Eli Leon, "Amidror: Israel Can Attack Iran Alone," *Israel Hayom*, November 18, 2013, https://bit.ly/2IAmE1w [in Hebrew].

46 Barak interview with Nahum Barnea: "Why We Didn't Bomb Iran," *Yediot Ahronot*, April 27, 2017, https://bit.ly/2VaiIG0 [in Hebrew].

47 Ephraim Kam, "Military Action against Iran: The Iranian Perspective," *Strategic Assessment* 11, no. 2 (2008): 97-106, https://bit.ly/2kUH2iT.

48 Mark Landler, *Alter Egos: Hillary Clinton, Barack Obama and the Twilight Struggle over American Power* (Ebury Publishing, 2016); David Ignatius, "The Omani 'Back Channel' and the Secrecy Surrounding the Nuclear Deal," Belfer Center, June 7, 2016, https://bit.ly/2GGU2C4.

49 See, for example, the detailed article by Jeffrey Goldberg after many meetings in Israel and concluding that an Israeli attack is inevitable and expected in the spring of 2011: Jeffrey Goldberg, "The Point of No Return," *The Atlantic*, September 2010, https://bit.ly/2BP40NH.

50 For example, Secretary of Defense Leon Panetta in an interview with Fox News: "Panetta Warns Israel on Consequences of Iran Military Strike," *Fox News*, November

The public discourse on the issue of an Israeli attack on Iran's nuclear facilities peaked in the second half of 2012. At that time, windows of time were supposedly designated for carrying out the attack – first in the spring of 2012,[51] then in the fall, before the US presidential elections.[52] Decision makers in Israel briefed journalists for the purpose of sending alerts and messages, including to the Israeli public. An example of this is the article by the editor of the daily *Israel Hayom*, Amos Regev, on March 15, 2012, which was published the day after he had apparently spoken with Prime Minister Netanyahu.[53] In the newspaper's main article, under the headline, "Difficult, Daring, Possible," Regev outlined the reasoning for an Israeli military attack on Iran. The article was accompanied by two symbolic pictures: one of an Iranian enrichment facility and the other of Israeli Air Force planes flying above the gate of the Auschwitz extermination camp.[54] In the summer of 2012, *Haaretz* published a series of articles by journalist Ari Shavit that also dealt with this topic, titled "The Eastern Front." Shavit spoke, among others, with Defense Minister Ehud Barak (referring to him as "the decision maker"), who detailed the strategic reasoning behind attacking Iran.[55] The majority of the Israeli public supported the option of attacking Iran. A poll by the Jerusalem Center for Public Affairs taken in March 2012 found that 60 percent of the public believed that a military attack was the only way to stop Iran.[56]

18, 2011, https://fxn.ws/2XgyMYZ.

51 Yitzhak Benhorin, "Panetta Believes that Israel Will Attack Iran by June 2012," *Ynet*, February 2, 2012, https://bit.ly/2IzwUqL [in Hebrew].

52 Ari Shavit, "The Decision Maker Warns: We Can't Trust the United States to Attack Iran in Time," *Haaretz*, August 10, 2012, https://bit.ly/2ViD1RZ [in Hebrew]. In this interview, Ehud Barak provided a detailed account of all the considerations in favor of an Israeli attack.

53 According to records of the dates of conversations between Netanyahu and Amos Regev, as relayed to the journalist Raviv Drucker: *HaAyin HaShevi'it* (*The Seventh Eye*) website, https://bit.ly/2tA7yPp [in Hebrew].

54 Amos Regev, "Difficult, Daring, Possible," *Israel Hayom*, March 15, 2012 [in Hebrew].

55 See the concluding article of the series by Shavit, which includes references to all of the interviews that he held: Ari Shavit, "Israel Facing the Dilemma of its Life," *Haaretz*, September 28, 2012, https://bit.ly/2Iy4wp7 [in Hebrew].

56 Poll by the Jerusalem Center for Public Affairs, conducted by Camil Fuchs, March 26, 2012: "Majority of Israeli Citizens Support Attacking Iran" [in Hebrew].

In his speech at the UN General Assembly in September 2012, Prime Minister Netanyahu painted a red line on a drawing of a bomb and warned against the continued enrichment of uranium to a high level by Iran, while emphasizing the need to stop the enrichment beyond 20 percent. According to IAEA reports from that period, Iran had not increased its stockpile of enriched uranium and had not gone beyond Netanyahu's "red line."

Towards the end of 2012, the military tension decreased; the threat of an Israeli attack on Iran was less frequently highlighted in the media. From that point on, sanctions took on a more central role in the discourse as an effective way to stop the Iranian nuclear program.[57]

The public disagreement with the US administration surrounding the issue of attacking Iran fueled the mutual suspicion between Israel and the US and sometimes even led to accusations.[58] Historical narratives and examples were also recruited for the dispute: senior Obama administration officials recalled the bitter experience of the American entanglement in the Iraq War in 2003 – a war that erupted on the basis of a false intelligence assessment; in contrast, in Israel the analogy of the Begin Doctrine was used, along with the possibility of repeating the successful mission to destroy the Osirak reactor in Iraq in June 1981, while also hinting about the attack on the nuclear reactor in Syria in 2007.[59] Netanyahu continued to emphasize Israel's right and ability to attack independently. Thus, in an interview on the *Uvda* investigative television program in November 2012, he claimed that Israel can attack even without American approval, "just like Begin did in 1981," and that the Israeli political leadership alone would decide on this matter.[60]

---

57 Amos Harel, "With the Coming of Autumn, Talks of Sanctions Return," *Haaretz*, October 7, 2012, https://bit.ly/2tBqddo [in Hebrew].

58 For example, the Israeli accusation (by "political sources") that the United States was distorting the intelligence assessments and claiming that Iran did not intend to create a bomb soon in order to deny Israel the legitimacy for a military attack. See, for example, an article from February 2012, in which "sources in Jerusalem" briefed a *Ynet* reporter before the Prime Minister traveled to a meeting with President Obama: Attila Somfalvi, "Sources in Jerusalem against the US: 'They Are Waging a Campaign to Prevent Us from Attacking,'" *Ynet*, February 27, 2012, https://bit.ly/2tyuEpg [in Hebrew].

59 Mike Herzog, "The Destruction of the Syrian Reactor – Another Look," *Haaretz*, April 29, 2018, https://bit.ly/2HOr6FW [in Hebrew].

60 *Uvda*, November 5, 2012, *Mako* website, https://bit.ly/2GFN2Fu [in Hebrew].

A central difference between the Israeli attacks on the nuclear reactors in 1981 in Iraq and in 2007 in Syria, and a possible attack on Iran, was that the preparations for an attack in Iraq and in Syria remained completely secret, while in the Iranian case a lively public discourse had developed. This unusual behavior led senior American commentators to doubt the credibility of the Israeli attack threat.[61] In addition, there were reports of internal disagreements in Israel between the political leadership and the military leaders, some of whom opposed an attack. The most prominent among them was Mossad Director Meir Dagan, who, after completing his term, went so far as to sharply criticize the attack option, calling it "a stupid idea."[62]

The Campaign around the Negotiations Leading up to the Signing of the Nuclear Deal

From 2013, the Israeli cognitive campaign, led by Prime Minister Netanyahu, focused on its fourth stage – attempting to influence the negotiations that the US and the other world powers held with Iran. Most of this effort was aimed at the American administration, both directly and via Congress, but pressure was also applied on the other countries that participated in the negotiations, as well as on public opinion. Staunch Israeli opposition to the framework that was formulated in the negotiations was expressed even before the signing of the interim agreement with Iran in Geneva in November 2013, when it became clear that Iran would be permitted to retain some of its enrichment capabilities and that the agreement would be limited in time. Israel argued that the interim agreement was terrible and would enable Iran to later develop a large stockpile of nuclear weapons.[63] After the final agreement with Iran was signed in July 2015, Israel announced that it was not committed to it.[64]

Several months earlier, in March 2015, Netanyahu delivered an unusual speech before the US Congress that was intended to pressure its members

---

61 Dan Perry and Josef Federman, "Just a Bluff? Fear Grows of Israeli Attack on Iran," *AP*, February 5, 2012.

62 "Meir Dagan: Israeli Attack on Iran? Stupid Idea," *Walla News*, May 7, 2011, https://bit.ly/2Iz44Xu [in Hebrew].

63 Yair Altman, "Netanyahu: Iran Has Received Written Approval to Violate UN Decisions," *Walla News*, November 25, 2013, https://bit.ly/2tAErLB [in Hebrew].

64 Barak Ravid, "Netanyahu: After the Agreement, Israel Is Not Committed to the Deal," *Haaretz*, July 14, 2015, https://bit.ly/2NlRkCx [in Hebrew].

and make it harder for the Obama administration to carry out the negotiations leading to the agreement taking shape with Iran.[65] In response, the President's National Security Advisor, Susan Rice, called Netanyahu's presentation "a speech that is destructive to relations between the two countries."[66] The more time that passed after the speech, the greater the gap became between Israel's demands and the Obama administration's positions regarding the Iranian nuclear issue.[67]

The Netanyahu government's discord with the administration was at odds with the support that it enjoyed at home. After the signing of the agreement between the world powers and Iran, the Israel Democracy Institute's Peace Index poll, carried out in August 2015, found that the vast majority of the Israeli public (73 percent) was certain that Netanyahu was right when he described the nuclear deal as "an existential threat to Israel." An even larger majority (78 percent) believed that Iran would later violate its commitment to the agreement.[68]

The Challenges of the Israeli Cognitive Campaign

The Israeli cognitive campaign took place in a complex situation: first, the Iranian case proved that a long term integrated effort is usually necessary in order to deny nuclear weapons to a country determined to acquire them. Furthermore, unlike the Syrian nuclear issue, the Iranian case forced Israel to cope with a severe and direct threat to its national security without being able to entirely prevent it on its own. The practical possibilities for creating pressure on Iran to stop its nuclear program were dependent on American and international involvement; these included diplomatic and economic pressure, American military deterrence (which in 2003 indeed led to the suspension of Iran's military nuclear project), close international supervision of Iran's nuclear facilities, the option of undermining the Iranian regime, utilizing the diplomatic path to reach an agreement, and the possibility of an Israeli

65 Barak Ravid, "Netanyahu at Congress: The Deal with Iran Is Terrible and Will Lead to War," *Haaretz*, March 3, 2015, https://bit.ly/2SispR7 [in Hebrew].

66 In a television interview with Charlie Rose on February 25, 2015, an excerpt of which was broadcast on *Ynet*, https://bit.ly/2Vg26Nf.

67 Emily B. Landau and Shimon Stein, "Israel and the Nuclear Deal with Iran: Chronicle of a Failure Foretold?" *INSS Insight* No. 735, August 18, 2015, https://bit.ly/2ku6WtG.

68 Peace Index for August 2015, September 9, 2015, https://bit.ly/2XkH6a0 [in Hebrew].

attack – which, even if successful, would have required American backing for Israel and supervision of the continued Iranian nuclear development.

In addition to these challenges, Israel had different assessments than the United States and other parties regarding the severity and urgency of the Iranian nuclear threat. Israel's position, especially since 2010, held that Iranian progress in the field of uranium enrichment demanded immediate action, while the Americans and Europeans believed that Iran was not yet developing nuclear weapons and that it was necessary to wait to evaluate the impact of the sanctions imposed on the regime. While there were similarities between the interests of the Israeli government and those of the Bush and Obama administrations regarding the issue – in particular, agreement on the objective of preventing Iran from acquiring military nuclear capability – there was also a dispute between the US and Israel regarding how best to address the problem and the stages to achieving the objective: Presidents Bush and Obama strongly opposed a military operation and wanted the administration to retain the independence to lead the handling of the issue, while an Israeli attack on Iran would have taken control of the situation away from them.

The Israeli challenge also grew because the American administration was busy at the same time with a host of other problems. These included the need to disentangle itself from the protracted wars in Iraq and Afghanistan and the desire to prevent another military conflict, the global economic crisis that broke out in 2008, and afterwards the impact of the Arab uprisings (Arab Spring) and the rise of the power of ISIL.

The gap between these positions intensified when it became clear that the Obama administration recognized Iran's right to maintain and develop its uranium enrichment capabilities, thus adopting a position similar to that of the other world powers.[69] This was in stark contrast to Israel's position, and even contradicted the traditional American position, which demanded the suspension of enrichment as a condition for any agreement.[70]

---

69 Shimon Stein, "The European Union and the Iranian Nuclear Crisis," in *A Nuclear Iran: Confronting the Challenge on the International Arena*, eds. Tamar Malz-Ginzburg and Moty Cristal, Memorandum No. 103 (Tel Aviv: Institute for National Security Studies, May 2010) [in Hebrew].

70 Wendy Sherman, "How We Got the Iran Deal," *Foreign Affairs*, September 2018, https://fam.ag/2EqksFS.

As a rule, it is difficult to measure the impact of a cognitive campaign on the strategic decisions of the leaders of world powers and to isolate it from other variables. Indeed, this is the case here too. The Bush and Obama administrations acted according to their own developed worldviews, and the Israeli impact on them was limited, if it existed at all, to tactical aspects and not to the overall American strategy. During Bush's first term, the approach of his administration towards the struggle against the proliferation of unconventional weapons and the states that support terrorism was based on the use of force and on efforts to overthrow "rogue" regimes. This concept was at the center of American foreign strategy after the September 11, 2001 attacks, as pronounced in Bush's "axis of evil speech" in January 2002. The formulation of this concept, including the American commitment to prevent Iran from acquiring nuclear weapons, occurred separately and unconnected to Israeli influence. It was also at the basis of the Bush administration decisions to go to war in Afghanistan in 2001 and Iraq in 2003. While the Americans soon discovered that they had erred in their intelligence assessments regarding Iraq, the Bush administration's demonstration of power contributed greatly to the struggle against regional nuclear proliferation and led to the suspension of the AMAD project in Iran, to Libya's decision to give up its nuclear weapons program, and to stopping the activity of the Pakistani smuggling network under A. Q. Khan. As the Americans became more entangled in Iraq, the understanding deepened that the chances that the US would take military action against the Iranian nuclear program were dwindling. The publication of the US National Intelligence Estimate at the end of 2007 further constrained the administration, and added to the harsh public criticism of it following the Iraq war.

The Obama administration was interested in resolving the Iranian nuclear issue with a diplomatic agreement, as part of an ideological and political approach that was almost antithetical to that of the Bush administration – this, too, unconnected to the Israeli campaign. President Obama, who won the Nobel Peace Prize in 2009 for "his efforts to strengthen diplomacy," had already in June 2009 offered to negotiate with Iran in a speech that he delivered in Cairo, before Israel had changed the emphases of its cognitive campaign.[71] The efforts to begin secret diplomatic relations between the US

71 "The Full Speech of US President Barack Obama in Cairo: You Have the Ability to

administration and Iran continued from then almost uninterrupted.[72] In the final analysis, the Obama administration succeeded in its view in completely implementing its policy towards Iran: it brought on board the players in the international arena in a joint effort, reached an agreement with Iran and stopped its nuclear program for a certain time, and also prevented an Israeli attack and a large scale military conflict in the region.

We can assume that Israel did indeed assist in raising public awareness of the Iranian nuclear danger and provided important information and assessments on this topic. The significant and effective part of the Israeli campaign was the threat of an attack, which was prominent in the international discourse and influenced the application of pressure on Iran. The possibility of an Israeli attack was discussed at length in the American and international press starting from 2010, and was viewed as a serious and credible threat.[73] This strengthened the sense of urgency in Washington regarding the need to address the Iranian nuclear issue and create an effective system of pressure on Iran. According to then-Secretary of Defense Leon Panetta, figures in the administration believed the Israeli determination to take military action, especially in light of the attacks that Israel had carried out in the past on the reactors in Iraq and Syria. Others reckoned that the Israeli campaign pushed the administration to take action, and that it brought forward by a year the implementation of the planned system of international pressures on Iran.

Israel's attack threat does seem to have increased the motivation of the Obama administration to speed up the diplomatic efforts and reach an agreement with Iran.[74] Indeed, in 2012, secret, back channel talks began in Oman between the US and Iran, excluding Israel. The understandings reached in this channel were a basis for the open negotiations and the nuclear deal

---

Create a New World," *Haaretz*, June 5, 2009, https://bit.ly/2BSOfVT [in Hebrew].

72 Details on this can be found in the *Boston Globe*'s investigation that details the secret talks between the US and Iran via Oman in 2011, and the involvement of then-Senator John Kerry in these talks: Bryan Bender, "How John Kerry Opened a Secret Channel to Iran," *Boston Globe*, November 26, 2016, https://bit.ly/2SZpQJ3.

73 Aluf Benn, "Benjamin Netanyahu Sends Emergency Reserve Call-up to Himself and the Public," *Haaretz*, March 15, 2012, https://bit.ly/2GZrl2D [in Hebrew]; see also the assessment of a senior American military official: "It Is Possible that Israel Will Attack Iran without Warning," *nrg*, November 5, 2011, https://bit.ly/2U4E1IY [in Hebrew].

74 Sobelman, "Restraining an Ally."

that was reached in 2015.[75] The threatening rhetoric of the Israeli political leadership in those years had an additional cost: Israel was seen in the international arena as a potential aggressor that might ignite the entire region.[76]

The attack threat was not the only one that brought about the increased pressure on Iran; other important developments occurred at the same time. For example, on November 8, 2011, an IAEA report was published on Iran's covert nuclear activity, following which international economic pressure on it was greatly intensified. At the end of 2011, the Obama administration imposed trade sanctions on Iranian banks, in January 2012 the European Union imposed a total oil boycott on Iran, and in the middle of March 2012 Iran was disconnected from the SWIFT money transfer system. President Obama even declared then that the American administration had a credible military option against Iran, and the US army conducted well-publicized tests of a new bunker buster bomb. Obama also reiterated his commitment to prevent Iran from acquiring nuclear weapons.[77]

The motif of emphasizing the non-nuclear threats in the Israeli cognitive campaign was intended mainly to serve the ultimate goal of preventing the nuclear threat. The circumstances required prioritizing one central objective. Other serious threats, such as the development of the firepower and proliferation of missiles or Iran's regional aggression did not receive sufficient attention in Western countries. Neither did the cognitive attempts to connect Iran to the threats of global terrorism; contrary to the messages of the Israeli campaign, Iran was not seen in the West as equivalent to ISIL but as fighting against it, that is, as having shared interests with the West. The

---

75 Ignatius, "The Omani 'Back Channel' to Iran."

76 For example, in an interview with CNN in February 2012, the Chairman of the Joint Chiefs of Staff, General Martin Dempsey, said that an Israeli attack on Iran would not achieve the long term objectives and "undermine stability"; "Chairman of Joint Chiefs of Staff: An Israeli Attack Will Not Achieve its End," *Ynet*, February 18, 2012, https://bit.ly/2Ep58ZR; the Prime Minister of Japan at the same time warned Defense Minister Barak that an attack on Iran is "a very dangerous act that will lead to escalation in the region," in "Japan to Barak: Don't Attack Iran – It is a Dangerous Act," *Ynet*, February 15, 2012, https://bit.ly/2TfAr1q; the French Foreign Minister declared that an attack on Iran "would destabilize the entire region," in Reuters, "France: An Attack on Iran would Upset the Stability of the Entire Region," *Channel 13 News*, November 6, 2011, https://bit.ly/2SoTuSw.

77 "Obama Aipac Speech," *The Guardian*, March 4, 2012, https://bit.ly/2STiLta.

two main threats that the world powers urgently had to deal with, in their view, were a possible Israeli attack, on one hand, and the Iranian nuclear program, on the other. From their perspective, both were addressed in the nuclear deal with Iran.

The fourth motif, which focused on opposing the framework of the agreement with Iran, did not succeed in preventing American compromises on the way to formulating the diplomatic agreement, which, as mentioned, was seen as defective by Israel. It is possible that from the outset the Israeli cognitive campaign did not have much of a chance of modifying the determination of Obama and of his Secretary of State, John Kerry, or the American compromises that were made in the covert talks in Oman.[78] However, the cognitive campaign in 2013-2015, whose rhetorical climax was Netanyahu's Congressional speech in March 2015, served as the backdrop and preparation for the Israeli diplomatic campaign that was renewed after the election of Donald Trump as President, and contributed to the US withdrawal from the nuclear pact with Iran in May 2018. The four main Israeli motifs of the Israeli campaign – the danger of a nuclear Iran, the Iranian regional threat and the missile threat, the threat of an Israeli military attack, and the issue of the agreement with Iran – continue to characterize the Israeli cognitive campaign today in varying degrees.

It is not clear if the Israeli actions and threats have had significant influence on the Iranian regime. Iran warned Israel not to dare to attack it, threatened an overwhelming response, and frequently related, first and foremost, to the American military threats. Israel, for its part, dismissed the Iranian cognitive counter-efforts that aimed to reassure the West. A prominent example of such an Iranian action was the *fatwa* that was supposedly pronounced by Iran's spiritual leader, Sayyid Ali Hosseini Khamenei, rejecting the production, dissemination, and use of nuclear weapons.[79]

---

78 Jay Solomon, "Secret Dealing with Iran Led to Nuclear Talks," *Wall Street Journal*, June 28, 2015.

79 Michael Eisenstadt and Mehdi Khalaji, "Nuclear Fatwa: Religion and Politics in Iran's Proliferation Strategy," *Policy Focus* 115, September 2011.

Lessons Learned

A Cognitive Campaign as Leverage to Motivate a Superpower

The central goal of Israel's cognitive campaign against Iran's nuclear program was to use the United States as leverage. The complexity of the campaign stemmed from the differences in power and capabilities between Israel and the US, and from the necessity that Israel saw in refraining from jeopardizing its special relations with Washington, which, as we know, are a critical component of Israel's national security. In light of this, one lesson to be learned is that in any cognitive struggle, especially one that aims to influence the leaders of a world power, it is essential to fully control and balance the campaign messages in all channels. The Israeli leadership needs to well identify the interests and sensitivities of the US, including all of the parties within it. Israel should express its independent position, but at the same time also make sure not to be seen as carrying out a manipulative policy, or as pushing the US towards military intervention against its will.

The Strategic Conceptions and Interests of Leaders of World Powers Limit the Effectiveness of Cognitive Campaigns

Despite the Israeli attempt to tarnish Iran's image, the Obama administration and the leaders of the other world powers saw it as a rational actor that can be a partner in the struggle against ISIL and in regional agreements. In addition, President Obama had an interest in attaining a diplomatic achievement on the issue of Iran's nuclear program and leaving behind a legacy, one of whose headlines would be an agreement with Iran. The Israeli attempt to convince Obama that the agreement with Iran was problematic and dangerous in the long term did not change his determination.

Creating a Sense of Threat: A Central Factor in Accelerating Decision Making Processes among Leaders

Thus, the sense of threat from the United States that Iran experienced after the war in Iraq led it to freeze its military nuclear project in 2003. The threat of an Israeli attack on Iran and the fear of a resulting regional war seems to have created a similar feeling among the world powers. And in 2011-2012, the Iranian regime was swayed, most likely, by the heavy economic pressure and by the threat of severe international isolation. This influence led it to

decide to "drink the cup of poison" and begin direct negotiations with the US, which in the end led to the 2015 agreement.

Motifs in a Long Term Cognitive Campaign have a Limited Window of Opportunity

It is important to understand the limitations of the window of opportunity for realizing each of the motifs of a cognitive campaign. After the moment has passed, the specific motif should be changed and a different one should be emphasized. For example, after the regular motif of warning against the danger inherent in Iranian nuclear weapons did not lead to sufficient pressure on Iran until 2010, in the next stage the threat of an Israeli attack was added in an attempt to exert more effective pressure on it. This motif also ran its course when intensive negotiations with Iran began. At that stage, Israel's influence had become relatively meager.

Accepted Narratives among the Israeli Public are not Always Relevant in the Wider World

The Israeli public identified with the partly emotional cognitive campaign, which made use of imagery from the Holocaust and from Jewish history. The cost of a campaign with such motifs raised levels of anxiety among the Israeli public. These same messages were also somewhat effective for parts of the American public, where they aimed to explain Israel's authentic fears and the legitimacy of its reasons for taking action. However, their influence on other governments in the West seems to have been negligible. Thus, emotional local narratives are mainly relevant for the public that shares the same cultural worldview and conceptual framework, and are not necessarily well-accepted among foreign audiences.

Mixed Messages Can be Viewed as Manipulation

A possible Israeli attack was justified by the need to damage Iran's nuclear facilities in order to delay, at least by a few years, the implementation of its nuclear program. The agreement with Iran in 2015 also froze the nuclear program, in this case for at least 10 years, thus seemingly achieving the same goal as the threatened attack. Against this backdrop, Israel's opposition to the nuclear agreement met with skepticism, both in Europe and in the United States.

An Aggressive and Focused Cognitive Campaign Can Advance a Certain Cause, at the Expense of Other Issues

The Israeli campaign focused on the Iranian nuclear threat, and the diplomatic negotiations and the subsequent agreement also dealt only with that issue. The cost of this was that Iran has continued to develop and work intensively on non-nuclear fields, almost entirely without paying the price for this internationally. Today, these fields pose concrete and significant threats for Israel and other countries in the region. While the US administration, with Israel's encouragement, has been trying to rectify this situation and demanding Iranian compromises on all issues, including its missiles, regional intervention, and support for terrorist organizations, to date this has not yielded significant achievements.

The Threat of the Delegitimization of the State of Israel: Case Study of the Management of a Cognitive Campaign

Shahar Eilam and Shira Patael[1]

The fight over the international legitimacy of the State of Israel has taken place since its establishment, but its characteristics have changed over the years. Unlike campaigns against states and terrorist organizations in which the cognitive component is seen as complementary, the legitimacy campaign occurs, first and foremost, in the cognitive dimension. Even seemingly tangible steps, such as attempts to advance a boycott of Israel, aim, in effect, to erode Israel's public image and its diplomatic standing in the international arena to the point of undermining the legitimacy of its very existence as the nation-state of the Jewish people. Given this, the confrontation over the legitimacy of the State of Israel, with its different components, can also serve as a case study for learning about the cognitive campaign in its broad context and for examining perspectives and modes of operation in the field of influencing cognition.

This article examines the efforts to delegitimize Israel from the perspective of a cognitive campaign. The article begins by describing the roots of the delegitimization phenomenon and presents the framework of the counter campaign. It then presents the impact of the environment on the struggle of narratives within this campaign and concludes with an analysis of the

1 Lt. Col. (res.) Shahar Eilam is a research fellow at INSS, and manages the INSS research program on the delegitimization of Israel and BDS. Shira Patael is a former research assistant in the INSS research program on the delegitimization of Israel and BDS.

unique characteristics of this campaign. The article focuses on the structuring of the campaign's framework, its dynamics, and select characteristics as a cognitive confrontation. As such, the article does not examine in depth the campaign's contents and developments. It does not discuss the question of whether Israel's policy toward the Israeli-Palestinian conflict has influenced the delegitimization phenomenon. Our working hypothesis in this respect is that Israel's policy does influence the delegitimization phenomenon, but even if there are substantial changes in this policy, the delegitimization phenomenon will not subside considerably.

The Roots of the Phenomenon of Delegitimizing the State of Israel

The campaign to deny Israel's legitimacy as the nation-state of the Jewish people began before the establishment of the state. The Arab states led this campaign over the years, mainly through diplomatic, political, and economic means, the most prominent example being the Arab boycott. Since 2001, civil society groups, along with various Palestinian organizations, have assumed the leadership of the campaign to delegitimize Israel. These groups are mainly active in the West, with the goal of influencing broad populations and decision makers. Consequently, the public sphere – namely the media and social media – have become the main arena of operation, due to their increasing influence on the decision making processes in different aspects of life.[2]

The first Durban conference, which convened in 2001 in Durban, South Africa, was a notable turning point for the current constellation of the phenomenon of delegitimizing Israel. The conference, attended by over 1,500 civil society organizations, was supposedly dedicated to the struggle against racism and xenophobia in general, but a significant portion of its declarations related to the State of Israel and challenged its legitimacy, all under the auspices of the United Nations. Israel was presented at the conference as a colonialist, occupying state that was instituting an apartheid

2 For more on the roots of the delegitimization campaign, see Yehuda Ben Meir and Owen Alterman, "The Delegitimization Threat: Roots, Manifestations, and Containment," in *Strategic Survey for Israel 2011*, eds. Anat Kurz and Shlomo Brom (Tel Aviv: Institute for National Security Studies, 2011).

regime, violating the rights of the Palestinians, carrying out crimes against humanity, and violating international law.

One of the well-known and leading bodies in the campaign to delegitimize Israel is the BDS (Boycott, Divestment, Sanctions) movement, which was established in 2005 by some 170 organizations that adopted the call to boycott Israel. The BDS movement operates through networks, in a decentralized manner, lacking almost any hierarchy and unified direction. Hundreds of organizations around the world currently operate within its framework, organizing campaigns to boycott Israel, prevent investments in it, and impose sanctions on Israel and on those connected to it. The BDS movement includes a Palestinian umbrella organization called the BDS National Committee (BNC), which includes all the Palestinian organizations that are committed to the boycott of Israel. This organization purports to direct the policy of the boycott and tries to coordinate the various parties involved.[3] At the same time, other organizations involved in the BDS movement also collaborate together.

The pro-Israel camp fighting against delegitimization has also operated through networks in recent years, namely hundreds of civil society groups that operate both globally and in Israel, along with the activity of the Israeli government and its agencies in this field. Creating shared goals and coordinating when there are different ways of operating and so many actors are, of course, an especially complex challenge.

Unlike military campaigns, which are usually bilateral and between two distinct adversaries, the campaign for the legitimacy of Israel is a campaign between the pro-Israel ("blue") camp and the anti-Israel ("red") camp for the support of many different target audiences (Figure 1). Along with the pro-Israel camp's efforts to thwart the actions of the anti-Israel "red" camp, and in addition to its attempts to weaken or undermine it, the pro-Israel camp must also work to reduce the impact of the "red" narrative among the various target audiences and strengthen the exposure, dissemination, and impact of the pro-Israel narrative. The target audiences are not monolithic, and their attitudes toward Israel are influenced by their worldviews, their political and social frameworks, their socioeconomic class, education, culture, and additional characteristics. As a result, the attempt to influence

3 Palestinian BDS National Committee, https://bit.ly/2a5UIzG.

their perspectives, inclinations, and positions requires mapping them and identifying the most effective ways to influence them in the desired direction.

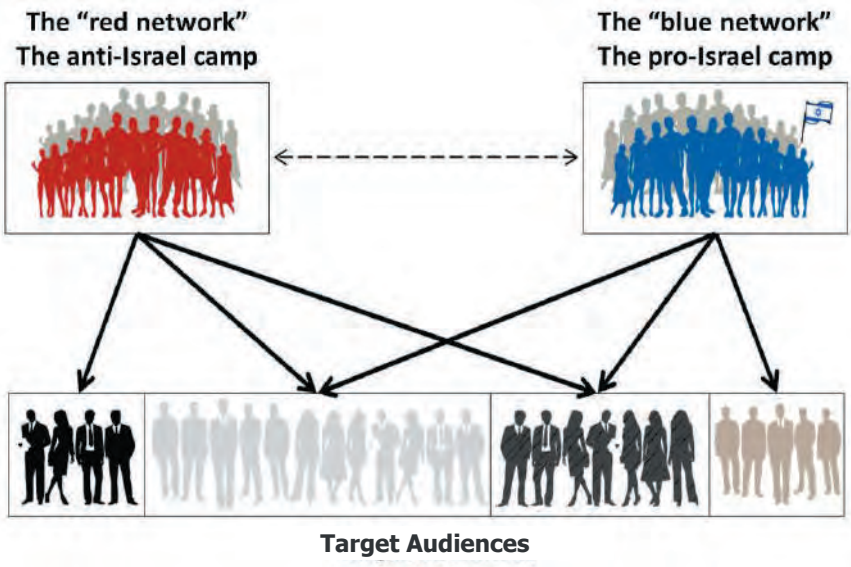


Figure 1: The Campaign for the egitimacy of Israel

The Environment of the Delegitimization Campaign: A Struggle over Narratives

In order to understand the environment of the delegitimization campaign and the way cognition is shaped, it is necessary to understand the conceptual-theoretical-ideological realm in which the delegitimization of Israel developed, as well as the zeitgeist. Major historical processes and social forces (such as ideological, social, economic, and cultural trends and movements) have influenced the shaping of cognition, and, in particular, the way Israel is perceived. All of these need to be considered when formulating the response.

The dominant metanarrative[4] today among many liberal and progressive populations in the Western world is hostile not only to the very existence and essence of the State of Israel but also to many foundations of Western culture and the existing world order. After the two World Wars and, even

4 A metanarrative is a large, comprehensive story regarding the source, moral purpose, and objective of humanity, which provides or denies legitimacy in relation to local narratives and actions in the reality of our lives.

more so, after the extent of the Holocaust's horrors became clear, an extensive process began in the West of challenging and reexamining the conceptions that formed the basis of the existing order. In the context of the rupture that occurred, post-modern philosophy developed, combining a number of worldviews, including post-colonialism, post-nationalism, and post-Zionism. In many cases, Israel serves as a scapegoat for post-colonial guilt, which is especially common today in Europe and the United States.

According to this worldview, Israel transformed from oppressed to oppressor. Its "crimes," as those engaged in delegitimization refer to Israel's policies on the Palestinian issue, constitute evidence of the racist-colonialist-imperialist oppressor's exploitation of the indigenous, native other, the "innocent victim." An expression of this worldview, for example, can be seen in the Great March of Return, the organized mass protests in the Gaza Strip taking place along the border with Israel since March 2018. The delegitimization organizations have adopted the Palestinian terminology to describe the events in Gaza, calling them "popular protests," "a peaceful march," "a non-violent march that is not identified with any political party,"[5] as well as a struggle between the Palestinian public marching "in favor of the most basic human rights," and an army "that fired all of the bullets."[6] They do this without referring to Hamas's involvement in organizing the demonstrations and without expressing any criticism of the violence and use of force by Palestinians during them.[7]

The worldviews that are hostile toward Israel and the Western world order enable the existence of the "green-red alliance," which includes Islamist organizations ("green") that are active alongside radical leftist organizations ("red"). This unwritten alliance has led the anti-Israel activity in the West during the past two decades and has succeeded in joining forces with additional groups, especially those that represent minorities and disenfranchised populations and whose main activity is struggling against the existing order, the elites, and the establishment. The attempt to connect

5 "Jewish Voice for Peace Horrified by Israel's Disproportionate Violent Response to Peaceful Protest," Jewish Voice for Peace, April 6, 2016, https://bit.ly/2Sn2rfc.

6 "Killed for Protesting: 6 Things to Know about the #Greatreturnmarch," Jewish Voice for Peace, April 5, 2016, https://bit.ly/2HAuk1V.

7 "News on Terrorism and the Israeli-Palestinian Conflict – May 9-15, 2018," Meir Amit Intelligence and Terrorism Information Center, May 15, 2018 [in Hebrew].

different groups, populations, and agendas into a joint struggle of all who are "victims" against all those depicted as "oppressors" is called intersectionality.[8] In this way, the delegitimization organizations have succeeded in placing the Palestinian issue on the agenda both in the local and global arenas, while creating an "alliance of the oppressed" and connecting their struggle with those advancing the rights of disenfranchised groups. These groups include blacks, LGBTs, migrants, women, environmental activists, human rights activists, labor unions, and more.

The use of intersectionality strengthens the narrative of the struggle for Palestinian rights as a legitimate struggle for the rights of a marginalized and oppressed group, thus recruiting many target audiences for the campaign, while blurring the real goals behind the core activists who have implemented the campaign, of denying the right of the State of Israel to exist as the nation-state of the Jewish people and placing the Palestinian issue on the global agenda.[9] In the view of those engaged in the delegitimization of Israel, this is a matter of principle and not an action based on taking advantage of specific opportunities.[10] Thus, Israel and diaspora Jews – who in the past were a model, a source of inspiration, and a natural partner for many minority groups struggling for rights, recognition, and status – now are perceived by the most recent generation as a clear example of "white privilege," and many groups

8 Clareta Treger, "We're Together in One Struggle," *Alachson*, July 20, 2016, https://bit.ly/2jzZJqX [in Hebrew].

9 For example, the Palestinian BDS National Committee (BNC) champions the values of liberty, justice, and equality and declares that its goals are ending the Israeli occupation in the Gaza Strip, Judea, and Samaria (including East Jerusalem) and the Golan Heights; achieving full equal rights for Arab Israelis; and implementing the right of return for all of the Palestinian refugees. The organization does not state its vision of the desired future political reality (one state, two states, and so forth) and ignores the fact that the implication of fully implementing the right of return in the name of the rights of the Palestinians is, seemingly, the denial of the right of Jews for self-determination in the Land of Israel. See https://bit.ly/2b07lw3.

10 See, for example, the three-way conversation that took place on February 1, 2018 between the director of the organization JVP (Jewish Voice for Peace) – a Jewish-American organization that supports BDS – with the director of the leading delegitimization organization in the UK (Palestine Solidarity Campaign – PSC) and with Omar Barghouti, one of the founders of the BDS movement. As part of this conversation, the three discussed the importance of intersectionality. The conversation was reported on the Facebook page of JVP. See https://bit.ly/2MNmBgy.

consider them responsible for the oppression of disenfranchised groups and for the wrongs committed against them. The ability of the proponents of delegitimization and supporters of BDS to unify these groups for a joint objective and to recruit them for efforts that harm Israel and Jews provides them with a significant source of power. On the other hand, the diversity of agendas, worldviews, populations, and objectives of these supporters is a potential vulnerability in their attempt to present a unified and stable front.

The decline in the power of truth could also explain the factors of influence among the different target audiences and the difficulty that the Israeli establishment has faced in presenting what the Israeli public has experienced. A study published recently by the RAND Corporation, entitled "Truth Decay," describes this trend and discusses the central characteristics and main factors that have led to it. While the study focuses on the American arena, similar trends can be identified elsewhere. According to the study, the current era is characterized by increasing disagreement in distinguishing between fact and fiction, the blurring of the boundaries between facts and opinions, the growing magnitude of opinions, and the waning confidence in sources and institutions that were once considered credible. The main factors involved are cognitive failures and the way people process information and make decisions; changes in information systems, such the growing importance of social media, which increased the volume of information, the variety of opinions, and the wide distribution of disinformation; and political, socio-demographic, and economic polarization, which increases disagreement.[11]

The internal political polarization in the American arena also influences attitudes toward Israel. A Gallup poll published in 2018 claims that 87 percent of Republicans in the United States identify with Israel, compared to only 49 percent of Democrats.[12] The Pew Research Center claimed even greater polarization between Republicans and Democrats regarding Israel. According to the Pew Research Center, 79 percent of Republicans identify more with Israel than with the Palestinians, compared to only 27 percent of Democrats. The institute's poll found that the situation is especially severe

11 Jennifer Kavanagh and Michael D. Rich, *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life* (Santa Monica, CA: RAND Corp., 2018), https://bit.ly/2D78Wff.

12 Lydia Saad, "Americans Remain Staunchly in Israel's Corner," GALLUP, March 13, 2018, https://bit.ly/2x46IfX.

among liberal Democrats, with only 19 percent of them identifying more with Israel, while 35 percent identify more with the Palestinians.[13]

This political polarization in the United States is characterized by a black and white reality, referring to "us and them." During the past two years in the United States, a significant protest movement against President Donald Trump has emerged, and since Israel is seen as an obvious ally of his administration, the waves of popular and political protest against the President sometimes intensify the delegitimization phenomenon. In this reality of polarization and division in American society, bipartisan support for Israel, which is perhaps the most important anchor of the special relationship between the two countries, is in danger. In addition, many American Jews are experiencing increasing tension between their stringent opposition to President Trump and their basic support for Israel.

Another unique challenge is that of measurement. The combination of physical, emotional, and cognitive dimensions that relate to stances, worldviews, and feelings makes it difficult to measure how the threat changes over time and the success or failure of the delegitimization efforts on one hand and the efforts of the pro-Israel camp to influence the worldviews and stances of target audiences on the other hand. This is especially true because shaping the cognition of these audiences is a long term process that is influenced by broader variables, which are difficult to isolate and attribute to one effort or another.

The Campaign for the Delegitimization of Israel

The phenomenon of delegitimizing the State of Israel threatens its national security, especially its freedom to make decisions and take actions in a variety of areas. In the modern global era, legitimacy is a necessary condition for a country to take action over time in almost any field or issue. In addition, the delegitimization phenomenon can have far-reaching consequences on the solidarity between Israeli society and Jewish communities around the world. In recent years, it has also had an increasing impact on the sense of security of diaspora Jews. As a result, the campaign that Israel and its supporters are waging against the delegitimization phenomenon aims to consolidate broad

13 "Republicans and Democrats Grow even Further Apart in Views of Israel, Palestinians," Pew Research Center, January 23, 2018, https://pewrsr.ch/2BQ4x1J.

global recognition and support for the State of Israel, recognition of its right to exist, its uniqueness, its contribution to humanity, its right to defend itself, and its being a society with equal rights and legitimacy within the family of nations. This is all in order to enable the State of Israel, its citizens, and world Jewry to live in peace and security alongside their neighbors and to create the conditions for personal, communal, and national well-being.

The threat of Israel's delegitimization combines cognitive and emotional dimensions with concrete steps in the diplomatic, legal, economic, cultural, academic, and other spheres. This is a multidimensional campaign that takes place in various arenas vis-à-vis diverse target audiences: the political-diplomatic ranks, municipalities, religious communities, the business sector, left wing organizations, human rights organizations, and more. Although the BDS movement has not caused any significant tangible damage to Israel thus far and its successes have mainly focused on individual, marginal achievements, it can be assumed that concrete steps and negative branding, which includes cognitive and emotional dimensions, constantly feed one another, even if the activities and efforts are not fully coordinated. Moreover, fostering negative attitudes toward Israel may cause long term damage to its security as well as to that of Jewish communities around the world. These attitudes may also influence consumer and business decisions, legal decisions, political activity, community preferences, parliamentary elections, and government policy on the local, national, and international levels.

The delegitimization campaign also harnesses events taking place on the operative-tactical level to leverage strategic objectives in order to achieve legitimacy and support. This often occurs by using primary materials, especially in the context of the Israeli-Palestinian conflict. Materials are made accessible by adapting them to the symbols and value systems of the target audiences around the world and sometimes by distorting them and taking them out of context, as well as by creating associative and emotional – and sometimes irrational – connections between the Israeli-Palestinian context and the symbols, sources of emotion, and actions from other contexts, places, and times. For example, the violent events in the Gaza Strip ("The Great March of Return"), during which tens of thousands of Palestinians demonstrated and dozens of Palestinians were killed, at the same time as the transfer of the US embassy to Jerusalem, has given momentum to the activity of delegitimization organizations. Beyond the very current events,

Israeli decisions and actions and statements by Israeli leaders also sometimes provide fodder for the delegitimization campaign.

The delegitimization campaign focuses on symbols and brands to achieve greater exposure and to raise awareness of delegitimization among the wider public. During the past few years, the boycott movement has conducted a series of campaigns against large, well-known international corporations, charging that their activity in Israel and in the territories assists Israel's occupation and "war crimes" against the Palestinians. It sometimes appears that the connection between the charges and the reality is incidental, as with the boycott campaign against the ice cream company Ben & Jerry's,[14] which eventually led it to contribute to the organization promoting the boycott; or the campaign to encourage Airbnb to stop advertising apartments in the settlements.[15] When the goal is to gain exposure and instill the message, it seems that all means are permitted. Against this backdrop, the boycott movement also focuses on cultural and sporting events that have broad exposure to millions of people around the world. Thus, the pressure placed on international artists to not appear in Israel has succeeded in influencing a few of them, while creating considerable international media attention and increased awareness about the existence of the boycott movement and its messages.

As of today, despite the delegitimization efforts, the majority of the leading elites, governments, and establishment institutions in the West have not substantially changed their relationship with Israel and certainly have not become hostile to its existence. However, the growing gap in the attitude toward Israel between governments, establishment institutions, and the elites on the one hand and public opinion on the other is certainly cause for concern. This concern increases when we add the intergenerational gap between the current elites and the next generation. As mentioned above, the source of these troubling trends is not only an increase in the efforts of those engaged in delegitimization but also primarily the combination of deep social and ideological trends in current politics and agendas both in Israel and abroad. These create serious difficulties in recruiting populations, especially liberals, to support pro-Israel narratives.

14 "It's Time to Boycott Ben & Jerry's," BNC, May 12, 2015, http://bit.ly/2U59ACz.

15 "Airbnb's Decision to Exit Israel's Illegal Settlements: A Partial Victory for Human Rights & Accountability," BNC, November 20, 2018, http://bit.ly/2EpxN1d.

Indeed, the threat of delegitimization should be seen as a long and ongoing "war of attrition" that aims at long term strategic objectives. Although these objectives are advanced through short term tactical efforts and achievements, they are cumulative. The most recent achievements of the State of Israel and its supporters, such as advancing legislation in Europe and the United States to undermine the legitimacy of the BDS movement and its freedom of action, have encountered countermeasures, such as the Right to Boycott campaign.[16] At the same time, however, many of the BDS movement's actions have had a negligible impact, or even have failed following successful countermeasures by the pro-Israel camp.

The rival anti-Israel and pro-Israel networks are learning campaigns and thus are in competition with one another. For example, during 2018, the delegitimization organizations undertook an organized and coordinated effort to gain support from different local councils throughout Europe and the United States. These efforts may have been the result of limited success of the BDS movement in advancing such steps at the governmental level, leading it to try to influence the establishment via local councils, while keeping their activity at the grassroots.

The Response of the Pro-Israel Camp

The complexity of the campaign for the delegitimization of Israel stems from its broad global deployment and its taking place in various areas with mutual connections, while its proponents are organized in a dynamic, non-hierarchical networked structure. Given the nature of the delegitimization campaign and the challenges it creates for Israel's national security, it should be addressed with an integrated response in Israel and abroad, including reactive and proactive endeavors, defensive, offensive, and preventive efforts, along with attempts to shape the desired reality and advance the objectives of the State of Israel and diaspora Jewry.

A prominent dilemma in formulating a response to the threat of Israel's delegitimization is the question of the organizational structure, including who is responsible for formulating and implementing the response, the relative advantages of the establishment versus the civil society groups, and the division of responsibilities between them. Many civil society organizations

16 "Right to Boycott," BDS, http://bit.ly/2Ve9HvJ.

were founded specifically to address the threat of Israel's delegitimization and given their "friction" with those engaged in delegitimization, these organizations have a good understanding of events on the ground, especially in terms of the civil society arena. These organizations are active abroad (and they often have representatives in Israel where they engage in activities) and are well-versed in the cultures, languages, attitudes, and value systems of the target audiences. For this reason, they are able to adapt and mediate the Israeli reality to these target audiences.

The Israeli government also offers many unique capabilities and resources, including a broad perspective of the challenge, response tools, and an understanding of the essence of the threat and its significance to the national security of the State of Israel and diaspora Jewry. The government has at its disposal the ability to direct the efforts and to more efficiently utilize the existing resources, based on being familiar with the organizations and their relative advantages. At the same time, government agencies have many legal and procedural limitations, certainly when it comes to activity focused on the civilian sphere and target audiences abroad. In addition, a significant portion of the members of the pro-Israel camp and many in the target audiences are critical of Israeli government policy and are not willing to act under its auspices or to receive instructions from it. Therefore, the state's presence at the forefront of the campaign does not help; rather, it is a hindrance.

The most effective response thus is a decentralized response, located somewhere in between a diffused and chaotic response in which each organization works entirely independently, and a hierarchical and centralized response led by the government. In our view, the pro-Israel network needs to act according to a shared vision and overall strategy, while maintaining the freedom of operation and independence of the various organizations.

The pro-Israel camp should act as a network. Improving networked functioning is based on a combination of utilizing the capabilities and relative advantages of the different components of the network, strengthening channels of communication, sharing information and knowledge, networked learning and cooperation between the different parts of the network, as well as developing core capabilities to improve the network's functioning and performance. However, this networking does not mean that the organizations should speak "with one voice." Improving the activity of the "blue" camp and

strengthening the connections between its components, while maintaining the diverse opinions and areas of activity, can pull the rug out from under the claims of proponents of delegitimization, who seek to present the Zionist movement as a racist enterprise and Israel as an undemocratic state that seeks to restrict the actions of its critics and limit freedom of expression.

The necessary response must address different elements of the problem. First, activity is needed to inoculate important neutral target audiences and central decision making junctures, in order to prevent them from being "poisoned" and to recruit their support for Israel. Second, the response must be based on strengthening and expanding the circle of supporters and activists within the framework of the pro-Israel camp (a broad coalition policy), based on the understanding that the delegitimization campaign is trying to undermine Israeli solidarity, which is a source of legitimacy and a vital resource in the pro-Israel campaign. These two elements are greatly influenced by Israel's policies regarding the Israeli-Palestinian conflict and by the question of its image as a state striving toward peace. Finally, as mentioned above, efforts are also needed to thwart the activity of the delegitimization campaign and reduce its ability to influence target audiences.

In this respect, a distinction must be made between Israel's critics and those who deny Israel's very legitimacy. This latter camp is generally led by those who support delegitimization and seek to destroy Israel. Alongside them are those who criticize Israel and oppose its policies; however, they are not full partners in the delegitimization ideology; they do not challenge the State of Israel's right to exist, and they are not necessarily part of the opposing system. The response needs to reduce the circles of support for the delegitimization campaign and create cracks in the solidarity of the anti-Israel camp by exploiting the differences of opinion, perspectives, and values of the various groups within it. It is important to expose the ultimate goals of the delegitimization efforts and the identity of the initiators and activists who support and fund it. As part of the response, it is necessary to distinguish between the proponents of delegitimization who seek to destroy the State of Israel and those who express legitimate criticism of its policies.

The response of the pro-Israel camp needs to be based on a combination of deep knowledge of the Israeli-Palestinian reality and the various target audiences as well as the ability to analyze them. Influencing the attitudes of target audiences toward Israel requires a long term ideological campaign

that reconnects the Zionist and Israeli narrative with the ideological and value system of Western society and diaspora Jewry.

Conclusion

The article analyzed the current campaign over the international legitimacy of the State of Israel as a case study of an ongoing cognitive campaign. This campaign involves strategic learning between the two rival network camps, which are working to influence diverse target audiences across the globe and to change their attitudes and positions. One key success in the delegitimization campaign has been harnessing and connecting local stories related to Israel, or developments in the Israeli-Palestinian conflict, to the value systems and agendas of other cultures and societies around the world. Thus, "our truth" and being convinced internally of the justice of our cause are not enough. Rather, we must understand what forms the basis of Israel's image and the attitudes toward it around the world and utilize this knowledge when setting the objectives of the campaign and the ways of achieving them.

Mindset and Social Resilience in Security Emergencies in Israel

Meir Elran, Carmit Padan, and Aya Dolev[1]

Much has been said in Israel in recent years on the topic of public mindset and its implications on defense issues, in the context of the Israeli conflict with sub-state neighboring actors. This discussion is impacted by the fact that despite Israel's clear military advantage, it has yet to achieve a decisive victory over its adversaries Hamas and Hezbollah.[2] Against this backdrop, many in Israel claim that the use of military force for the purpose of achieving a strategic objective is not sufficient, and that an additional effort is necessary, in reference to the abstract dimension of "the mindset."[3]

The "cognitive campaign" is not a new trend. The domain of the mindset, or consciousness, has always played a role in conflicts between states, including the many that have taken place between Israel and its state foes. In the past, Israel invested significant energies to influence the mindset of its adversaries – commonly termed "psychological warfare" – with less than considerable success, on the whole.[4] The present focus on the realm

1 Brig. Gen. (ret.) Dr. Meir Elran is the head of the Homeland Security Program at INSS. Dr. Carmit Padan is a research fellow at INSS. Major Aya Dolev is the director of the consciousness and research branch in the Home Front Command.

2 Meir Elran and Carmit Padan, "From Civilian Protection to a Civilian Front: The Triple Paradox," in *Six Days, Fifty Years: The June 1967 War and its Aftermath*, eds. Gabi Siboni, Kobi Michael, and Anat Kurz (Tel Aviv: Institute for National Security Studies, 2017), pp. 121-34.

3 Shay Shabtai and Lior Reshef, "Consciousness Efforts in the IDF," *Maarachot* 457, 2014 [in Hebrew].

4 Ron Schleifer, "Psychological Warfare in Israel – A Reexamination," in *Mideast Security and Policy Studies* No. 50 (Ramat Gan: Begin-Sadat Center for Strategic

of consciousness and its ramifications stems to a large extent from changes in the way conflicts are waged in the 21st century[5] and from the dramatic and rapid developments in the field of information technology that provide ever-new capabilities for mass dissemination of information and insights. These are commonly meant to create awareness and to shape the mindset of large segments of the target population, even if they are not always aware of the intentions behind these manipulations.

This article discusses one element of the cognitive campaign: its impact on the domestic public mindset in the context of the societal resilience of communities in Israel that are subject to security-related disruptions. It focuses on what is needed from the Israeli establishment to build emergency awareness,[6] so as to enhance communities' resilience, as a central element of their efforts to face the terrorist challenge.

The Conceptual Framework

"Consciousness" is a broad term, which entails three main components: the subjective, the cognitive, and the emotional. Though forged by the interaction between people and symbols, language, beliefs, and values, consciousness forever influences the self-perception of the individual acting in a given cultural and social context. The discussion of consciousness in this article refers to the conceptual realm of security, as part of the military context and the conflicts that the IDF and Israeli society are engaged in with the present enemies. Indeed, the IDF's approach regarding consciousness relates only marginally to the Israeli target audience (perhaps because of its hesitance to deal with the conduct of the civilian population), but it does suggest that its cognitive efforts vary in relation both to the object of influence (i.e., the

---

Studies, July 2002) [in Hebrew]; "Psychological Warfare, Documents, the Six Day War," *IDF Archive* (delivery 4/2016), http://bit.ly/2BSPW5H [in Hebrew].

5 Yossi Kuperwasser, "Battling for Consciousness," *Strategic Assessment* 12, no. 2 (2009): 41-50.

6 Emergency mindset is a perceived situation in which the individual (or community) senses that there is at present an emergency situation or event. A resilience mindset is a perceived situation in which the individual (or community) feels that he is able to cope with the challenge that the emergency situation poses and to bounce back quickly from its dire consequences. In both cases, these are individual/social interpretations, but while emergency consciousness refers to the present time, the consciousness of resilience is not limited to a given time frame.

adversarial target audience) and to the intended goal of the masterminding agent.[7]

The discourse of consciousness reflects the constructivist dimension that has developed out of post-modernist thinking, which suggests that reality does not have an independent existence without the meaning that is attached to it.[8] The dominance of the cultural context, which influences the way humans interpret (and thus perceive) "the reality" has led to the development of a conceptualization, which represents the understanding that "the cognitive campaign" is a sort of a competition over who succeeds in influencing the way target audiences perceive "the reality." Indeed, it appears that a struggle is taking place over the way the narrative is perceived and over the way it is expressed in the mindset of the various audiences. In this manner, each side uses the narrative to justify its objectives and actions in the conflict. In addition, a corresponding contest takes place over the legitimacy of the policies carried out in practice.[9]

In the military-security contexts, these ideas have influenced the world of war and the perception of conflicts in the mindset of the involved civilians. Thus, in order to achieve an impact on the various target audiences, it is necessary to relate to the conceptual dimension that shapes the way people and communities perceive "the reality." Simultaneously, one has to relate also to the dimension of time: before engagements take place, during the fighting, and afterwards. In the Israeli context this would be relevant also during the so-called "campaign between wars."[10]

In this framework the following definitions are proposed: consciousness refers to the multidimensional, dynamic, changing way a person or a public perceives the events that affect it. This perception is based on the concepts, feelings, thoughts, experiences, and spiritual life systems of the person or public. Consciousness is also influenced by the way people and groups

---

7 *The IDF's Concept for Cognitive Operations,* IDF, internal document, 2017 [in Hebrew].

8 Carmit Padan, *Social Construction of "Crises": Commanders as Constructors of Reality*, PhD thesis, Department of Sociology and Anthropology, Hebrew University, 2017 [in Hebrew].

9 Kuperwasser, "Battling for Consciousness."

10 *IDF Strategy*, 2015 version, http://bit.ly/2Iyc2jT [in Hebrew]; *IDF Strategy*, 2018 version, http://bit.ly/2H3OctA [in Hebrew].

understand and interpret the changing "reality" and by the meaning that they attribute it through their responses to the challenge in question.

Actions in the realm of consciousness are directed by different parties that utilize various means to shape the meaning and interpretation that individuals give to events that occur in their environment or that impact them. The goal of actions in the realm of a cognitive campaign is to construct, influence, and shape the perception of "reality" by individuals and communities according to the interests of the influencing parties. A discussion of the consciousness of individuals, of communities, and of the Israeli public as a whole under these circumstances needs to refer both to the designers of consciousness, on the one hand, and to the objects of influence on the other, namely those whose consciousness is shaped during emergency situations, thus constructing their actual conduct.

The factors shaping civilian consciousness in times of conflict include, first and foremost, the external physical threat that the enemy poses to the Israeli home front. This is a unique configuration of terrorism, manifested by frequent, continuous, and large scale launches of a variety of projectiles targeting civilian populations and critical infrastructure installations. This terrorist campaign can also include suicide bombings, offensive tunnels, attempts to conquer civilian localities along the border, and possibly cyberattacks, which might become more prevalent in future conflicts.

The extent of the military threat is very significant in the context of consciousness, with respect to the duration of the threat towards the home front, the consequences of the attacks in terms of numbers of fatalities, and the disruptions of daily routine, such as extended power outages or damage to sensitive facilities (hospitals, schools, etc.). As with all terrorist activities, these are aimed to cause fear and anxiety among civilians so as to create demoralization. The overall strategic intent of terrorism is to foster public pressure on the decision makers to change their policies towards the perpetrators.[11] Personal and social fear or

11 A. J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature* (New York: Routledge, 2017); Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: US Institute of Peace Press, 2006).

anxiety[12] are keys in shaping the consciousness of civilians in security-related situations of stress.

Terrorism can also be expressed in psychological warfare designed to adversely impact the mindset of the civilian public by conveying messages that fuel public fear[13] through diverse channels of communication.[14] This kind of effort is presently quite limited in the conflicts between Israel and Iran, Hamas, and Hezbollah, at least as far as its very limited impact on the Israeli public is concerned.

At the same time, and especially during conflicts, attention should also be paid to internal Israeli factors that clearly shape the public mindset, perhaps even more effectively than external ones:

a. Israeli public figures, at the national and local levels, who have diverse and sometimes conflicting political interests: on one hand, they may be interested in creating a mindset of stability, steadfastness, security, faith in the justness of the national cause, and societal resilience. On the other hand, some might be interested in creating a sense of public dependence, furthering a political agenda, demonstrating the incompetence of political adversaries, and more. This complex situation could lead to a sense of weakness, lack of security, increased sense of risk, and even fear among civilians.
b. The free media,[15] including social media,[16] have considerable influence on the public mindset,[17] in general, and in times of stress in particular. The mainstream media, especially television stations, may have an interest

12 On the distinction between fear and anxiety, see the Enosh website, http://bit.ly/2E6TFgp [in Hebrew].

13 See, for example, the speeches of Hezbollah leader Hassan Nasrallah.

14 Reuven Erlich and Yoram Kehati, *The War over Consciousness as Part of the Conflict between Terrorist Organizations and Israel: Hezbollah as a Case Study*, Intelligence and Terrorism Research Center, Israeli Intelligence Heritage and Commemoration Center, 2007 [in Hebrew].

15 Joshua Meyrowitz, *No Sense of Place: The Impact of Electronic Media on Social Behavior* (New York: Oxford University Press, 1986).

16 W. G. Mangold and D. J. Faulds, "Social Media: The New Hybrid Element of the Promotion Mix," *Business Horizons* 52, no. 4 (2009): 357-65.

17 54 percent of the Jewish population of Israel believe that media coverage harms or seriously harms social resilience, according to a public opinion poll by INSS in October 2018 (not published).

in intensifying the images of damage caused by terror, thus captivating viewers and boosting ratings.[18]

c. The government, the IDF via the IDF Spokesperson, and especially the Home Front Command, as the representative of the military on the civilian front, have a central role in creating the necessary cognitive balance in civilians' perceptions of the threat's intensity. This is part of their role of providing the population with security and a sense of safety, being, ostensibly, free from a political or economic agenda.

The Impact of the Public's Conduct on Consciousness

Some communities are characterized by a high level of societal solidarity, enjoying a social fabric that enables the crystallization of a social mindset, which contributes to a higher level of resilience to external threats. Here is a major role for the community to construct functional continuity, for the civil society's voluntary activism within the communities and for the local leadership to apply its inclusive dynamic function and to manage emergency situations.[19] As the Israeli public is far from monolithic; it comprises a variety of mindsets on all issues. Different groups, even in cohesive communities, have a range of opinions that influence the public mindset in diverse manners.[20] Consequently, just as it is difficult to monitor the components of consciousness, it is demanding to shape the public's mindset in general, especially in a vibrant democratic society as that found in Israel.

An interesting recent example of an attempt to influence the Israeli mindset could be found in the interview that Yahya Sinwar, the leader of Hamas in the Gaza Strip, gave to Italian journalist Francesca Borri for the Israeli daily *Yediot Ahronot* in October 2018:

---

18 56 percent of Jews and 54 percent of Arabs agree that the media in Israel describe the situation in Israel as if it were much worse than it actually is: *Democracy Index 2018*, chapter 8 (Jerusalem: Israel Democracy Institute), p. 165, http://bit.ly/2BKBSLl [in Hebrew].

19 Carmit Padan and Meir Elran, *The "Gaza Envelope" Communities: A Case Study of Societal Resilience in Israel (2006–2016)*, Memorandum No. 188 (Tel Aviv: Institute for National Security Studies, 2019).

20 A. Titz, T. Cannon, and F. Krüger, "Uncovering 'Community': Challenging an Elusive Concept in Development and Disaster Related Work," *Societies* 8 (2018): 71.

> The goal of the resistance is for your message to get across to the other side. The language of the resistance depends on the language that the other side understands…the tools of resistance change in accordance with the context of who you want to communicate with and what is the language that the other side understands. If I initiate an attack tomorrow, I'll be in the main headlines of all of the newspapers. But if I talk about a ceasefire, like now in this interview, it's harder to listen to me… the incendiary kites are not a weapon…they are a message: you are immeasurably stronger than we are; that is true. But you will never be victorious.[21]

This quote clearly suggests an action in the realm of consciousness that can be executed in the context of ongoing security turmoil. It aims to impact the Israeli public mindset.[22] It offers nothing new.[23]

Consciousness and Social/National Resilience: The Concept and Its Practical Expressions

The current military threat from Hezbollah and Hamas creates a significant cognitive challenge to the social resilience of the Israeli public. As with other types of terrorism, the threat of high trajectory projectiles, offensive tunnels, and incendiary balloons aim primarily to undermine civilians' sense of security by sowing fear and disrupting daily life.

The essence of "societal resilience" is not agreed upon by the researchers on this subject. The diverse literature offers different conceptualizations, some very broad and others more focused. This article defines resilience from the functional perspective, referring to the operative definition relating to the capacity of any system to flexibly cope with a severe disruption and

---

21 Francesca Borri, "From My Perspective, a Ceasefire Means Complete Quiet. And the End of the Blockade," *Yediot Ahronot*, October 4, 2018, http://bit.ly/2XiL7eW [in Hebrew].

22 Amira Hass, "The Story Behind the Interview with Sinwar," *Haaretz*, October 8, 2018, http://bit.ly/2XeMGe5 [in Hebrew].

23 See, for example, P. M. Taylor, *Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Era* (Manchester: Manchester University Press, 2013).

to rapidly bounce back from it.[24] Social resilience can be measured using different methods, the most familiar one being polls and surveys. Another benchmark is the monitoring of the unavoidable gap between the post-event degradation of functionality due to disruption and the level of a system's functionality following the initial recovery. A faster rebound will bring the system to a higher level of functionality, what we call a "bouncing forward" status, suggesting greater resilience.[25]

The range of challenges terrorism has brought to Israel's societal resilience over the past two decades is extensive. This includes "traditional" terrorism, such as that seen during the bloody second intifada (2000-2004), Hezbollah's intense rocket attacks during the Second Lebanon War (2006), and the three "rounds" of conflict with Hamas in the Gaza Strip (2008-2009, 2012, and 2014). In each of these instances, the civilian front was exposed to serious protracted disruptions with varying degrees of severity and damage. The physical risks counted in deaths and injuries, and the attendant financial and practical damage, such as lost work days and reduced production, can be measured by quantitative tools. In contrast, the damage in the realm of consciousness is much harder to gauge. Yet ongoing research offers a clear conclusion: the Israeli public has demonstrated, thus far, a high (albeit not uniform) level of societal resilience. This is influenced in part also by the intensity of the disruptions, as expressed in the number of fatalities and the duration of terrorist attacks.

The mindset of the Israeli public, and particularly of the communities directly affected by terrorism, has a direct influence on the level of societal resilience. A comparative study[26] that recently examined the resilience of communities in the so-called "Gaza envelope" over the course of a decade (2006-2016) shows several phenomena that reflect the centrality of mindedness:

a. Residents in the Gaza envelope are greatly aware of the security threats and potential consequences that they face in normal times and during

24 Meir Elran, "Societal Resilience in Israel, How Communities Succeed despite Terrorism," *Foreign Affairs*, March 23, 2017, https://fam.ag/2BRj0dI.

25 Meir Elran, *Social Resilience in the Face of Terrorism: The Conduct of the Israeli Public During the Second Intifada*, PhD thesis, Department of Political Science, Haifa University, 2017 [in Hebrew].

26 Padan and Elran, *The "Gaza Envelope" Communities: A Case Study of Societal Resilience in Israel (2006–2016)*.

emergencies and transitions from normal times to emergencies. In fact, emergency mindedness is a crucial element in their daily lives, even in relative calm periods. Such awareness serves as a strong basis for a relatively high level of emergency preparedness and community-wide organization in advance.[27]

b. Despite the fact that the Gaza envelope communities face similar threats, there are interesting distinct differences between them regarding what each one perceives to be the suitable approach to coping with the security challenges. For example, different communities have different approaches to the question of their own evacuation.[28]
c. The regional local leadership takes upon itself a central role not only in physical and social preparedness for emergencies, but also in value-based mental preparation.[29] This includes an ongoing dialogue with the local public, based on mutual trust, which in turn contributes to the enhanced societal resilience.
d. This consciousness-shaping discourse is also accompanied by cooperation between the military and the communities and their residents. Both sides understand that this intimate relationship contributes to the civilians' trust in the military, which is perceived as being willing and able to contribute not only to the communities' security, but also to assist them with practical solutions to emerging challenges in times of stress, while expressing sensitivity to the civilians' specific needs.[30]
e. As a result of all these, and against the backdrop of the ongoing experience of the Gaza envelope residents, an advanced emergency consciousness takes shape for most of them, which enables them to live reasonably under

27 Ibid., pp. 25-50 and 59-66, which detail the centers of resilience in the Gaza envelope. The chapter in the memorandum that analyzes the functioning metrics of each of the communities is the most relevant one in this context (including the resilience centers).

28 Ibid., pp. 26-32.

29 The significant role that leadership has during emergencies can be expressed through the construction of the narrative of the residents in the lead-up to emergency preparations (meaning, what story does the leadership tell its residents in the lead-up to emergency preparations) or in framing the emergency through the way the leadership structures the functioning of the community during emergencies. For more on this topic see ibid., pp. 78-79.

30 Ibid, pp. 70-75.

the constantly renewed threats, and to exercise their societal resilience. A clear example of this is the impressive growth of the city of Sderot, due in part to intentional effort by the mayor and his staff to shape a community consciousness that is based on local empowerment resources. The contribution of this higher level of societal resilience was highly visible during the traumatic Operation Protective Edge in the summer of 2014, very much in contrast to the situation under the city's previous leadership, which chose to emphasize its vulnerability, weaknesses, and dependence on external assistance.

Evidence relating to the level of societal resilience and the impact of the public mindset on it in other regions in Israel is lacking. Hence, it is not possible to draw a clear and detailed picture. However, public statements by heads of the Home Front Command and the National Emergency Authority allow us to estimate that the level of emergency preparedness in most of the country's communities and municipalities (except perhaps for those in Judea and Samaria) is much lower than that in the Gaza envelope, especially in terms of civilians' personal preparedness.[31]

Israelis place the responsibility for emergency preparedness on the government, and have even given it a reasonable grade in this role.[32] Years of relative calm on the northern front and relatively few severe terrorist attacks since the second intifada have created an understandable erosion of the once-perceived immediacy of a large scale military conflict and its potential dire consequences. Hence, it can be suggested that emergency consciousness among the majority of Israel's residents, in the sense of recognizing and understanding the implications of a large scale military conflict on the individual and the community, is rather low. This stems, in part, from an intentional government approach that refrains from creating a serious sense of threat during times of relative calm, in order to prevent panic and fear.

---

31 Israeli public opinion polls conducted by the Institute for National Security Studies clearly show that the majority of the state's citizens do not prepare for emergencies. 67 percent of the public reported in 2015/16 and 75 percent of the public reported in 2016/17 that they do not prepare themselves for emergencies.

32 40 percent of the public believes that the government does a good job of preparing for emergencies, while 44 percent believe that the government partially does a good job on this issue (according to public opinion polls conducted by INSS).

However, this can have a negative impact on societal resilience,[33] if and when the Israeli public (individuals and communities) is again challenged by a major security disruption (or, even more so, by a serious earthquake, which is expected at some time). Repeated attempts by the Home Front Command and the National Emergency Authority to arouse the interest of the civilian population in the consequences of a major disruption, for example, by encouraging people to participate in the annual exercises, have met with indifference. In general, the public tends to rely on the IDF to do what needs to be done and refrains from engaging in this issue in theory and practice.

This attitude entails a problematic cognitive paradox that needs to change or at least to seek equilibrium. The public's indifference between conflicts – which is understandably explained by the wish for a semblance of normalcy and quiet when possible – diminishes the level of preparedness, which itself is necessary to cope with the harsh challenges of renewed emergencies. The question of how to rouse the public from this apathy is an issue that needs to be examined by the state and the IDF Home Front Command.

Implications and Systemic Recommendations

A mindset of resilience refers to the public's self-perception of its ability to successfully meet the challenges of emergencies and to rapidly return to normative functioning after a traumatic event. The connection between consciousness and societal resilience is close and clear. This article claims that the clearer the emergency mindset is and the broader and more convincingly it is instilled in the public, the higher the level of resilience will be. The practical implication of this claim is that awareness, understanding, and absorption of the consequences of "the reality," as anticipated and perceived during times of emergency, can construct the necessary mindset that would enable the general public to more successfully cope with the challenges of security (and other) disruptions, and thus enhance its capacity to more rapidly bounce back – and bounce forward – to return to a similar, and perhaps even

33 See a document on the issue of the need to build a model for maximum utilization of civilian resources on the local level, in light of "a recognition of the need to integrate residents and community organizing, which currently do not sufficiently come into play, in activities during emergencies": "Connecting to Resilience during Emergencies: A Model for Inter-sectoral Cooperation," Prime Minister's Office, http://bit.ly/2SUz1tT [in Hebrew].

higher level of systemic functionality following a calamity, be it man made or natural. This is the very essence of societal resilience.

A number of factors combine in times of security emergencies to undermine the social resilience mindset. They might include the adversary's strength and the magnitude of attacks, and the scope of the harm inflicted on people and property. Also, the enemy's "psychological warfare" can play a role, as can the IDF's success (or failure) to reach its goals as defined by the government. Other detrimental influencing factors are rumors, especially those disseminated on social media, negative media coverage, and flailing social solidarity.

Other empowering factors that enhance the resilience mindset should be considered and facilitated:

a. Preparing the civilian front in advance by protecting the civilian front, along with distributing information on threat responses to reduce the potential surprise emanating from the gap between expectations and reality.
b. Clear success of the IDF in facing the enemy, defensively and offensively, within a relatively short time and with few casualties, and the failure of the enemy to disrupt civilian routines in Israel.
c. Building the responses prior to the outbreak of the conflict, including:
    i. Provision of a reliable, customized, and complete picture of the challenges expected due to the military (or natural) disruptions.
    ii. Community organization based on full utilization of the available human and social capital.
    iii. Local inclusive leadership that knows how to shape a constructive mindset of resilience and to fill it with the practical content of prior deployment.
    iv. Building public confidence in leadership institutions – municipal, local, and national, as well as the military.
d. Guidance by emergency agencies and the national and local media during the disruption. Such guidance can strengthen citizens' resilience by providing accurate and qualified reporting on the events at hand and by upending false rumors.

To conclude, three systemic recommendations are in order. The first is to address the need to shape and maintain a solid and trustworthy public mindset reflecting the capacity to maintain an "emergency routine" during times of severe disruptions, manmade or natural. This is feasible, and moreover the

civilian front in Israel will benefit if this approach is adopted in practice. it is the role of the state, first and foremost, via the Home Front Command and the IDF, as well as the local authorities, to take on the task.

The second recommendation is to adopt the resilience model developed over the past decade in the Gaza envelope in municipalities and communities all around Israel, adjusting it to suit the social structure of each one. This is necessary as most localities in Israel are subject to similar terrorist threats. Adopting this model will enable them to better cope with future security challenges, which, according to official estimates, could be much more severe than in the past. This will help bolster the public's resilience in advance of the next severe conflict.

The third recommendation is to completely change the current approach towards public indoctrination regarding the consequences of a future conflict. Up until now, the practice in Israel has been for the authorities to refrain from telling the full story of a developing threat to the public, keeping from them anticipated consequences and information regarding how they should respond during the disruption. In other words, the public is not being updated on critical elements of a threat, as was proposed in the reference scenario submitted to the security cabinet by the Ministry of Defense and the National Emergency Authority already in 2016. This is not highly classified information. And yet, the political outlook has remained that it is better not to "disturb" the public with worrying scenarios. This anachronistic approach does not acknowledge the significance knowledge and understanding of potential risks plays in strengthening the public's emergency mindset and, no less important, the public's need to be able to prepare for emergencies and how to act while they are ongoing. It is suggested that the government's prevailing ostrich-head-in-the-ground policy be replaced with an open, orderly, and methodical public disclosure of the important elements of a threat and the behavior called for in response so as to appropriately cope with the expected risks.

The Israeli public is entitled to know exactly what a forecasted scenario comprises in future conflicts. It needs this vital information in order to shape its mindset in the face of the threat and to build its resilience, on the personal, community, and national levels.

The importance of the cognitive campaign is recognized more and more in the State of Israel. However, steps taken so far display a lack of consistency and systematic activity, and range from improvisation stemming from necessity to ad hoc planning in individual cases. In a reality where the decisive importance of the issue is proven time and time again, there should be a national public diplomacy and cognition directorate within the Prime Minister's Office that would operate under the direction of the Prime Minister and coordinate all public diplomacy and cognitive war efforts. In this way, the cognitive campaign, like any other campaign, would be conducted in a coherent manner based on the policy dictated and approved by the political leadership, and include every public servant and soldier. Institutionalizing the governmental effort would also enable individual volunteers or organizations in Israel and abroad to receive reliable information and messages, and in turn contribute to the national cognitive effort.

Lt. Gen. (ret.) Moshe Ya'alon

This collection represents a collaborative effort by the Institute for the Research of the Methodology of Intelligence (IRMI) at the Israeli Intelligence Community Commemoration and Heritage Center and the Institute for National Security Studies (INSS). It includes articles on the challenges of the cognitive campaign in the era of modern communications from a variety of perspectives. As such, it is a significant contribution to the public discussion of cognition and to the development of a professional knowledge base among the security and intelligence community, both in Israel and abroad.

Brig. Gen. (res.) Yossi Kuperwasser is the head of the Institute for the Research of the Methodology of Intelligence (IRMI) at the Israeli Intelligence Community Commemoration and Heritage Center and Director of the Project on Regional Middle East Developments at the Jerusalem Center for Public Affairs. He served in the IDF Intelligence Corps, including as chief intelligence officer for the IDF Central Command and head of the Research Division of Military Intelligence. He is a former Director General of the Israel Ministry of Strategic Affairs.

Lt. Col. (res.) David Siman-Tov is a research fellow at the Institute for National Security Studies (INSS) and deputy head of the Institute for the Research of the Methodology of Intelligence (IRMI) at the Israeli Intelligence Community Commemoration and Heritage Center. He served in the IDF for twenty-five years, and has published widely about cognitive warfare, intelligence, and the cyber realm. He is the co-editor of the journal *Intelligence in Theory and in Practice*, and co-author of a book on the first decade of the Intelligence Corps in the IDF.

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

The Institute for the Research of the Methodology of Intelligence