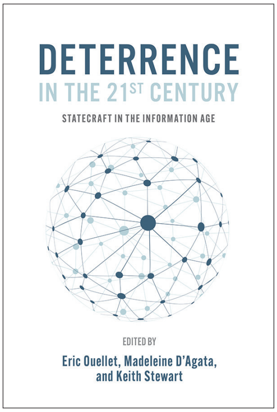
UNIVERSITY OF CALGARY
Press


DETERRENCE
IN THE 21ST CENTURY
STATECRAFT IN THE INFORMATION AGE
EDITED BY
Eric Ouellet, Madeleine D'Agata,
and Keith Stewart

DETERRENCE IN THE 21ST CENTURY: STATECRAFT IN THE INFORMATION AGE

Edited by Eric Ouellet, Madeleine D'Agata, and Keith Stewart

ISBN 978-1-77385-404-5

UNIVERSITY OF CALGARY
Press
press.ucalgary.ca

Acknowledgement: *We acknowledge the wording around open access used by Australian publisher,* **re.press**, *and thank them for giving us permission to adapt their wording to our policy* http://www.re-press.org

7

Resilience as a Framework for Deterrence in the Information Age: Lessons Learned from Israel about Information and Influence Operations

Oshri Bar-Gil

Introduction

The growing use of information and influence campaigns as part of hybrid warfare necessitates a new deterrence approach. Although such campaigns are on the rise, they are not new; since ancient times, they have been employed to defeat opponents and prevent rivals from acting. Even the writings of the ancient Chinese strategist Sun Tzu (2013) emphasized the need to obtain dominance and manage information to deter opponents. Throughout the last century, different measures have been taken to deceive the adversary, boost military morale, and motivate soldiers and leaders to battle. The purpose of indoctrination was to encourage the forces to continue fighting and to deter enemies. Propaganda, misinformation efforts, and "active measures" were employed in the struggle for narrative dominance. In this process, communication channels are utilized to influence attitudes, beliefs, and actions following the objectives of the influential sides. As part of "active measures," spies and influencers affected target audiences to reduce their motivation to act, and even increased the perceived cost of military actions to deter the adversary from fighting (Rid, 2020).

According to Mazarr (2021), deterrence is convincing one's adversary that the costs and hazards of a particular course of action outweigh its rewards.

While the search for deterrence strategies in twenty-first-century wars continues, one approach to establishing deterrence is through resilience, which can circumvent the opponent's aspirations and prevent him from achieving success in this domain.

The purpose of this chapter is to suggest ways to enhance resilience to deter adversaries from planning and implementing information operations. Looking at the Israeli case, it seeks to understand the strategies, techniques, and technologies that Israel used to detect, reduce, or minimize Iran's non-state proxy operations.

The chapter will examine the need for new forms of deterrence in the face of hybrid threats and how resilience may be one of them. It will then examine the changing context of the information battleground in the twenty-first century and the transition to hybrid warfare, which includes political, economic, and communication measures to disrupt trust and social legitimacy in Western democracies. Then it will provide an overview of global threats: first, the traditional Russian national model, followed by ISIS's operational model as a global terror organization, and then the broader international model of infodemic, which uses disorder to cause even more havoc. The last model will be the Iranian threat model, contextualizing the case presented in the chapter—Israel's efforts to deter Iran and its proxies.

The following section will cover general coping methods and responses to those threats. These involve the use of social media to acquire intelligence against those dangers, acting in a kinetic manner, and creating information inoculation tactics. Following a broad description of these strategies, it will concentrate on ways to establish national and military resilience as a means of deterrence, including ways to develop a framework or doctrine for influence campaign resilience. Based on the Israeli experience, the discussion section will determine whether resilience-enhancing tactics can truly dissuade actors from influence campaigns and other elements that should be considered when employing this strategy.

"New" Hybrid Warfare and Threats Call for New Methods of Deterrence

Deterrence can be defined as discouraging or restraining someone—in world politics, usually a nation-state—from taking unwanted actions, such as an armed nuclear attack or information campaign. It entails attempting to halt or prevent an action (Mazarr, 2021; Mazarr et al., 2018). The fundamental theme of this book is that disinformation should not be tackled solely with inward measures such as resilience development or information inoculation. The outward concept of understanding the adversary and how the adversary thinks about us is at the heart of deterrence, thereby allowing us to be significantly more proactive. While deterrence comprises the broad military dimensions (whether conventional, nuclear, or informational) and the means and capacity to respond to an external threat, resilience focuses on the preparedness that allows militaries to perform their duty. In other words, minimizing the military's and society's vulnerabilities reduces the possibility of an attack by decreasing its effectiveness and strengthening deterrence (Lasconjarias, 2017; Thiele, 2016).

In an age of hybrid warfare, cyber and information operations are intertwined to amplify enemy achievements through the information they reveal. Recently, at the Warsaw Summit in July 2016, NATO acknowledged the significance of resilience in deterring hybrid warfare as heads of state and government signed an official statement pledging to "continue to build . . . resilience against the full spectrum of threats, including hybrid" (Meyer-Minnemann, 2016; van Doorn & Brinkel, 2021).

Another hybrid aspect that can be used to guide the definition of resilience in the face of new hybrid threats is cyber resilience, which is defined by the US-based National Institute of Standards and Technology as "the ability to anticipate, cope with, adapt to, and recover from difficulties, pressures, or attacks on systems that use or are enabled by cyber resources" (Ross et al., 2019, p. 71). This resilience notion has three interconnected layers—preparation, inclusion, and adaptation—and it may provide some direction while trying to establish a resilience framework for influence campaigns.

Hybrid Warfare: From Clausewitz to the Information Battlefield of the Twenty-First Century

Born centuries before the Internet, Clausewitz argued that "war is not merely a political act but a real political instrument, a continuation of political intercourse, a carrying out of the same by other means" (Clausewitz, 1989, p. 65). Using incorrect, fake, and falsified information to undermine the fighting spirit, divide nations, and impair enemy capabilities can be seen as a continuation of policy in other ways. Military, intelligence, and operations personnel well understand "digital espionage" and its history. Nevertheless, there is still some ambiguity over the use of "disinformation," which further influences public opinion and politics through "active measures," or actions used by parties to sow mistrust and riots among the people while retaining intelligence operatives working behind the scenes.

The modern era of disinformation began in the early 1920s with the KGB's establishment of a foreign propaganda bureau. The KGB even coined the term "disinformation" in an attempt to sound French; Singer and Brooking (2018) contend that by doing so, the truth was buried alongside the term's genesis. In the meantime, the West referred to it as "political warfare." It also sought to capitalize on rumours, discrepancies, and incorrect or partial information within the adversary's political body (Goldschmidt & Wergan, 2017; Rid, 2020).

Over the last three decades, the Internet has become the primary medium for communication, messaging, and politics. This global information highway was designed in the 1960s under the sponsorship of the US Department of Defense as a conduit for communication within the United States and between it and the rest of the globe amid the threat of a nuclear strike by the Soviet Union. The Internet is now as crucial for business and social life as it is for governments, armies, and individuals. Everyone uses it to influence other people and to conduct information campaigns for economic and political benefit, as well as national and other reasons, aimed at winning not only on the Internet but also within the global mindset. Online forces' struggle alters the definition of war. Temporary battles impact the world by influencing everything from celebrity status to election results in countries around the world. Our physical senses, memories, and consciousness are all part of this war, and we are all engaged in wars of which we are unaware.

Information has become a potent weapon in international politics, and the practical tools utilized on the global battlefield have evolved in recent years. The attempt to develop new ideas of action in this area and the intensification of the national-military dialogue about it represent this transformation, as does the establishment of dedicated entities concerned with the problem. Weapons and concepts utilized in deterrence strategies have even shifted away from the military domain and toward the political, economic, humanitarian, and communicative domains, and influence campaigns play a key role in these areas (van Doorn & Brinkel, 2021).

These approaches are usually associated with the emerging concept of "hybrid warfare" (Chivvis, 2017), which includes using direct force with cautious and calculated methods, constantly weighing and adjusting the intensity of various combat efforts, and concentrating on local politics and the civilian population. In addition to cyber-attacks and influence operations, hybrid warfare employs proxies for broad impact (e.g., economic/commercial), political influence, extortion (among other things following cyber-attacks), and inflammation (Chivvis, 2017). With the introduction of new technology and the expansion of Internet culture, the global wave of disinformation is gradually building and increasing in the first decades of the twenty-first century. What was formerly a gradual, professional psychological impact is now a high-speed action that even the least competent, remote, and disassembled forces may conduct due to technological improvements (Rid, 2020). According to Schia and Gjesvik (2020), the weaponization of disinformation has been on the rise in recent years as the Internet and social media have grown in popularity (Bennett & Livingston, 2020; Rid, 2020; Singer & Brooking, 2018).

Deepfakes represent one newer technology that has recently undergone significant improvement. Its name combines deep learning, a machine learning technology used in artificial intelligence, and the notion of fakeness. The American intelligence community designated it a strategic threat to national security in 2019. It is a technology that allows the creation of synthetic video or audio, such as a video that puts words in the mouth of a leader (Hwang et al., 2021). Deepfakes symbolize, in a broader sense, the post-truth ethos, which makes the public more distrustful and calls into question the veracity of any content to which it is exposed. In other words, such technology distorts the human impression that what we see exists and thereby undermines the credibility of any movie or recording, hence lowering the value of truth (Andrejevic, 2013).

"Terrorism is theater," declared RAND Corporation analyst Brian Jenkins (1974) in an article that became one of the most recognized studies on terrorism. This mindset has guided terrorists for decades. They now have access to a new audience and battleground thanks to the Internet, online social networking, and new technological tools. Nations fight them in this terrain to defend their sense of security, prestige, and public legitimacy.

The affordances brought about by technological advancements and social transformations—the blurring of lines between attitude, opinion, and deception in the "post-truth" era—also impact national security. As conflicts no longer conclude in obvious wins, the importance of narrative struggles grows. Successes are not solely perceptual; however, the attitudes that troops and civilians have in countries worldwide significantly impacts how the success of military missions are evaluated. By building resilience against attempts to cast doubt on the military's capability and purpose, it will be possible to prevent opponents from misusing information to nefarious ends.

Overview of Threats from a Global Perspective

This section will briefly review the critical threat models discussed in the current literature: (1) the conventional Russian national model; (2) ISIS's operational model as a global terror organization; and (3) the wider global model of infodemic, which utilizes disorder to bring about further chaos, as in the case of COVID-19 disinformation campaigns. While these three models have received much attention, this chapter will focus on a fourth one, a unique model that is more pertinent to Israeli efforts to develop resilience as a form of deterrence—the so-called Iranian model.

NATIONAL INFLUENCE CAMPAIGNS COUPLED WITH ACTIVE COMBAT: THE RUSSIAN HYBRID MODEL IN CRIMEA

The actual conquest of the Crimean Peninsula was accomplished through military force, but the incursion "into the mind" of Crimean residents began far earlier. The 2014 invasion of Ukraine and annexation of Crimea were supported by a propaganda campaign conducted by Russian official media that was widely circulated on the peninsula at the time. When the Russian military offered "assistance" in annexing and safeguarding the peninsula, the local population was willing to accept this in part (Summers, 2017). Russia has undertaken cyber-attacks on Ukrainian government offices and crucial infrastructure, in addition to propagating fake news through social media (Greenberg, 2019b; Singer, 2014). These acts exacerbated societal problems and rifts while reinforcing public skepticism about the Ukrainian government's ability to safeguard its citizens. This "constant disruption of stability" contributed to the narrative that justified Russia's annexation of Crimea.

In so doing the Russian state emphasized the "Gerasimov Doctrine," named after Putin's favourite military intellectual, General Geresimov, which takes advantage of information asymmetry. Gerasimov is the creator of the Russian version of "hybrid war." Since 2014, Russia's military-strategic compass has emphasized a new focus on political, economic, and cyber warfare. Russia has committed significant resources to organizing its power through influence operations to upgrade the doctrine. It has since been conducting numerous initiatives worldwide to strengthen its positions in a way that allows it to exploit the disparity between it and Western democracies (Stengel, 2019).

INFORMATION TERRORISM IN THE MIDDLE EAST: THE ISIS DISINFORMATION MODEL

The meteoric rise of the Islamic State, or ISIS, terrorist organization demonstrates social media's enormous influence. The key to its success is its exceptional capacity to dominate social media and draw international attention, without distinctive military capabilities or a substantial cyber-attack capacity (Stengel, 2019). Its biggest weapon was the hashtag #AlleyesonISIS. During its peak, this the was the most popular hashtag on Arab Twitter, filling the screens of millions of users, including city residents and defenders. Thousands of the organization's messages terrified defence forces, prompting them to abandon helicopters, tanks, and other vehicles; the spread of terror can be matched by considering it as an unconventional weapon (Singer & Brooking, 2018).

THE USE OF COVID-19 INFODEMIC AS A BASIS FOR INFLUENCE CAMPAIGNS

One of Russia's most successful operations, Operation Infection, was triggered by an HIV outbreak. KGB agents have directed their colleagues to promote the myth that AIDS is a biological weapon created by the United States to kill Blacks and homosexuals. This information caused distrust in the US military, as seen in increased negative attitudes among Black and LGBT soldiers (Rid, 2020). Looking at the contemporary situation, we can see parallels with the COVID-19 pandemic. In early February 2020, the World Health Organization named the epidemic an "infodemic" owing to the information overload that accompanied it (Thomas, 2020). Since then, the infodemic has brought millions of people worldwide to their knees in a torrent of information as they tap WhatsApp screens and other social networks at an ever-increasing rate. This information crisis costs society dearly, resulting in uncertainty, worry, anxiety, misunderstanding, and the inability to make social judgments and engage in decision making at a critical time (Bar-Gil, 2020). In addition to the information epidemic produced by the uncertainties surrounding the new virus, some actors began influence attempts comparable to the prior exploitation of AIDS.

According to some, the coronavirus originated in Chinese biological weapons laboratories. Another report by Harvard's Freeman Center for Free

Communication claimed that Russia is trying to gain influence by promoting conspiracies surrounding the deployment of the fifth-generation communication network (5G) in the United States, claiming that the radiation it emits aggravates the disease (Bush, 2020). As nations raced to vaccinate a sizable section of their populations, there were reports that Russia was attempting to gain an advantage through hacks, data theft, and disinformation against the vaccine (Sabbagh & Roth, 2020). Russian motivations were likely to include a desire to weaken Western countries' trust in the ability of their vaccines to compete and restore the economy through widespread vaccination (Scott, 2020).

THE IRANIAN MODEL

US National Security Adviser John Bolton labelled Iran a "national security risk" in 2018. Surprisingly, it earned this status for its information efforts, which aimed to push topics and narratives in line with Iranian foreign policy, supporting "anti-Saudi, anti-Israeli, and pro-Palestinian themes, as well as support for certain US policies beneficial to Iran, such as the US-Iran nuclear deal" (Tabatabai, 2018).

Tehran is no stranger to information warfare. The Islamic Republic, like other authoritarian governments, exploited information as a form of hard political capital, and the disinformation strategies used by the Iran are as old as the Iranian revolutionaries who worked to depose the shah in the 1970s. Back then, they employed various techniques to amplify the voice of Ayatollah Ruhollah Khomeini by distributing brochures and cassette recordings with his speeches on them. The cassettes were inexpensive, quickly duplicated, and easy to hide from the shah's intelligence agency. Khomeini's voice and message acquired traction on Iranian streets thanks to the cassettes, even as he remained in exile in Paris. Khomeini's advisers, educated in the West, assisted him in marketing his messages to many audiences: Iranians at home and in exile, Shia Muslim communities in the Middle East, the broader Muslim world, and the West. Khomeini's supporters laid the groundwork for his ascension with a clandestine political strategy that combined propaganda and disinformation (Tabatabai, 2018). Nowadays, Iran employs a plethora of fake social media accounts, fake websites, and news outlets with cyber capabilities to further its policy objectives in many countries. The precise impact of these activities is unknown (ClearSky Security, 2018).

Iran, Russia, and China are active in today's regional and global information war. Iranian attitudes and experiences in such conflicts as the Iraq-Iran War and fears about foreign involvement have made information warfare a preferred tactic of the Iranian state over the years. Iran demonstrates to its adversaries that it can hurt their "soft underbelly," or the fabric of civilian life in their countries, by employing cyber and information warfare. Among other methods, Iran aims to hurt Israel through this dimension, which can bridge the significant distance between the nations.

Overview of the Israeli Case

As an introduction, it is critical to recognize that high degrees of trust and social legitimacy have evolved to play a growing role in the operations of the Israeli military and the State of Israel. In his article "The Clocks that Tapped Lazily," Guy Brooker (2011) cites several critical variables that determine the Israel Defense Forces (IDF) public legitimacy and allow it to maintain its military freedom of action: the sensitivity to social protest in democratic regimes complicates army operations, as seen during the First Lebanon War (1982), when public opposition was a primary concern in its administration (Toby & Rartner, 2007). The sense of vulnerability on the home front, as well as Operation Pillar of Cloud (2012), intensified pressure to stop the war during the Second Lebanon War (2006) and Operation Cast Lead (2009), on both the international and Israeli fronts. The Israeli public regards the IDF as a moral army, and any transgression of this paradigm may jeopardize its freedom of action and credibility at home. Globalization trends, which also exist in Israel, increase the role of the international arena in managing hostilities, and international legitimacy is primarily shaped by public opinion. This infringement was shown in Operation Grapes of Wrath (1996), which resulted in considerable internal and international pressure following a misdirected attack on a UN refugee compound.

Over the last twenty-five years, there has been a substantial practice in the battle for narrative in Israel. As part of this endeavour, the IDF Spokesperson's Unit has been bolstered, and the Prime Minister's Office now has a National Cyber Directorate. Preparations for the prospect of a negative effect on public discourse and democratic processes in Israel, particularly the Knesset elections, are essential in such attempts (Goldschmidt & Warren, 2017).

The IDF developed and published a doctrine on influence and information operations in 2017. The doctrine recognized and defined the threats to

IDF action posed by global environmental change. In particular, it recognized that "the enemy's influence effort is activated and developed via a comprehensive examination of the State of Israel's and its military power's strengths and vulnerabilities. Its underlying premise is based on the notion that the enemy will be using asymmetrical tactics to weaken the IDF's authority, affect its public image, and limit its freedom of action" (IDF, 2019, p. 3).

The more complex and advantageous a country's digital infrastructure, the more vulnerable it is to "asymmetric" information and cyber-attacks. Furthermore, the socio-cultural capital of Western democracies, whose citizens and institutions enjoy a higher level of trust, is more vulnerable than in low-trust countries (San-Akca, 2014). Compared to its adversaries, Israel has more to lose, and more "attack surface" in the form of information networks (Mazarr et al., 2022; Ross et al., 2019), and Israel's adversaries strive to compensate for this advantage through asymmetric warfare.

Some unique features distinguish the Israeli case, and while these may limit the generalizability of the research, they may also provide some insight into potential essential areas to consider when building a strategy for engaging and deterring threats. The first is the linguistic aspect. Hebrew, the most widely spoken language in Israel, is spoken by fewer than ten million people worldwide. This could present new difficulties and opportunities. It may call into question the availability of global information as well as the availability of language-based solutions to combat deception and disinformation. On the other hand, it provides superior control and the ability to discern communication trends. It is a significant barrier for those who seek to mount influence campaigns in areas where technical capabilities and English are insufficient. They must learn the language and culture to conduct credible influence operations.

Another distinguishing feature is the Israeli military's high level of trust. It is the most trusted institution in Israel (Shafran-Gittleman, 2022) and has one of the greatest confidence percentages of any of the world's militaries (Gains, 2021). With such high levels of trust, the IDF's ability to manage public dialogue may appear legendary, but this is not the reality. However, the opinions of military personnel (or ex-military personnel) are highly appreciated.

The next distinctive feature to evaluate is Israel's censorship and its connection with the institutional media. Its role is to develop the essential capacities to monitor, filter, and control content and information in order to avoid potential harm. It might be utilized as a significant coordinating and synchronization hub during times of conflict, influencing efforts conducted by other governments to weaken Israel's security and resilience. Some countries have similar bodies, such as the United States, Australia, Denmark, and Belgium (Bodine-Baron et al., 2018; Cooperwasser & Simen-Tov, 2019). They do not, however, have the communication-governance mechanisms of legislation and regulation developed in Israel. Those may be of interest and offer some insight in attempting to achieve the complex balance between public rights, the development of critical thinking, and the need to protect nations from foreign influence operations.

The main threat to Israel is the multi-layered Israeli-Iranian confrontation, which has been going on for years. Iran must find ways to bridge the physical distance between the two countries. Some of these ways include using proxies and acting in dimensions where distance is irrelevant, such as the cyber and information spheres. Iran's influence operations against Israel are part of a broader set of initiatives subordinated to the Iranian regime's top priorities. One facet of Iran's threat to Israel is the deployment of proxies, such as Hezbollah, trained and operated from Teheran, providing it with cyber deniability (Clarke, 2017; Schaefer, 2018). Iran employs three primary methods that reinforce one another in its influence campaigns against Israel: (1) the use of fake accounts to incite public dissent on social media (ClearSky Security, 2018); (2) fake news outlets portraying Israel as a weak state while delivering news favourable to Iran and its geopolitical objectives (Barel, 2021); and (3) using cyber capabilities to conduct hack-and-leak operations to undermine trust in Israeli officials and institutions and Israeli citizens' sense of security in the cyber domain (Hochberg, 2021). Former intelligence minister Eli Cohen recently cited reports about fake websites identified in the country (Cohen, 2018), claiming that Iran is not only attempting to influence public opinion in Israel but is also investing considerable resources in doing so (Halperin, 2020b). These efforts were carried out by operatives impersonating Israelis to stir social and political strife (Tony, 2020). It was revealed before the 2020 election that Iran utilized an army of bots and phony accounts to promote disinformation, bad talk, and provocation. It is also expected that the infrastructure of false accounts would be utilized for fraud to steal information and take over multiple electronic devices and user accounts (Rubinstein, 2019). Following a series of extortion operations attributed to Iranians, the media's attention has also intensified. Several such attacks have occurred recently, but the most well-known is the attack on the Shirbit insurance company.

It was announced in December 2020 that a group calling itself “Black Shadow” had targeted Shirbit. It obtained a vast array of data, including sensitive information on its policyholders and internal corporate data. The attackers later used media attention to humiliate the company and its insured customers by revealing several details and negotiating a ransom payment (Ziv, 2020).

Cyber-attacks and influence campaigns promote embarrassment, humiliation, media awareness, and trust erosion. However, Israel is not alone in the world; therefore, on the following section looks at global engagement strategies and their local implementation in Israel in a way that reinforces resilience and deterrence.

Deterrence Strategies: From Global Threat to Local Implementation

TURNING DISADVANTAGE INTO ADVANTAGE: USING SOCIAL MEDIA AS OSINT

If nations understand how to harness the asymmetry generated by the rising use of social networks, they can turn this to their advantage. Extensive information can be obtained from expanding open-source intelligence technologies (OSINT). The civic intelligence organization Bellingcat, which solved the enigma of Malaysian Airlines Flight MH17’s destruction over Ukraine, gained widespread attention (Bellingcat, 2018). The group was established soon after that tragedy. Following the plane’s destruction, members of the organization discovered numerous images and videos of a Buk missile launcher near the MH17 flight route on the day of the tragedy—within the separatist, Russian-supported zone (Singer & Brooking, 2018). The organization’s investigators were then able to locate the unit to which the missile launcher belonged. The Bellingcat analysts’ report presented compelling evidence to answer the mystery that troubled several Western intelligence organizations while relying primarily on visible sources, and they were able to expose the misinformation spread by Russia and direct the blame to specific personnel.

In Israel, the blogger “Abu Ali Express” engaged in similar actions and received institutional support. Abu Ali Express is a famous Israeli blogger who covers Arab matters on social media platforms such as Telegram and Twitter, as well as on his website. He bases his posts on gathering and evaluating open-source news and social media. He held the Telegram channel with the highest views per post in Israel as of September 2022, and his posts go viral in both social media and traditional news agencies. Despite his Arabic alias, the blog was founded by an Israeli citizen. In 2021, *Haaretz* newspaper exposed that he had been endorsed by the IDF in 2018 to administer the channel as an OSINT-based influence tool to expose disinformation and actors spreading it using his fast response and broad audience (Kubovich, 2021).

A KINETIC WAR INFLUENCED BY CYBERSPACE

Following the COVID-19 pandemic, the word "super-spreader" has become ingrained in our vocabulary. The role of these players on social media is significant. Social media can help spread a particular message in the real world. Their virtual networks allow nefarious actors to disseminate lies, hate, and other societal toxins. Some nations use kinetic power to harm these super-spreaders. Washington killed an ISIS spokesperson in 2019 to prevent ISIS from rallying people and resources against the United States via social media (Coles et al., 2019). There is no evidence that Israel had used firepower against social media influencers, but in May 2019, Hamas attempted to create cyber offensive capabilities in Israel. It acted from the Gaza Strip to attack Israeli cyberspace. The infrastructure failed to achieve its goal because all attempts and operations were identified and blocked technologically. As a result of counterterrorism operations, the IDF targeted a Hamas cyber array (Newman, 2019; Shahaf, 2019). One might consider kinetic attacks used to respond to cyberspace-based activities, such as cyber-attacks or influence campaigns, as the opposite of hybrid warfare—taking the cyber battle to a kinetic dimension to convey a message rather than simply stopping the activities in cyberspace.

Developing Military and National Resiliency to Deter Foreign Actors?

While the examples above may deter actors from conducting influence operations through social media influence or kinetic force, they do not do so by establishing resilience. The following section will illustrate various ways to develop resilience in general and as a deterrent to information operations. It begins by looking at the various ways of implementing national plans to improve critical thinking, trust, regulation, and governance processes. It then outlines how to increase the military's resilience and the role of technology products and partnerships before concluding with a concept for a resilience framework to influence campaigns.

Developing Nationwide Strategies

SUPPORTING SOCIAL CRITICAL THINKING MECHANISMS FOR SOCIAL NETWORKS

Could one of the possible solutions to our social media trust problem be a different type of social media? In many countries, social media is used to raise public awareness of how information is consumed, uncover fraud and lies, and promote civic demands (van Doorn & Brinkel, 2021).

Stanford University researchers examined information consumption behaviours among three groups: undergraduate students, history PhDs, and fact-checking specialists, and compared how they judged the accuracy of Internet content. Undergraduate and PhD students received poor grades. Despite their apparent intelligence, the study discovered that they focused on "vertical" information—evaluating only one source and assessing it from within their world view. As a result, they were susceptible to manipulation. The researchers concluded that dealing with inaccurate information requires learning the proper skills rather than being "clever" (Bergstrom & West, 2020). People should be able to identify and cross-reference sources, spot suspicious details, and use fact-checking websites to develop the requisite competencies (WHO, 2020). While these educational initiatives benefit individuals, societies can also benefit from comparable methods. Some civic organizations in Israel analyze facts and fight disinformation. For-profit news organizations even support some of these efforts, but institutionalized support can boost resilience to disinformation.

USING CHANGE AGENTS AND INFLUENCERS TO ENHANCE TRUST

Finland, Estonia, Lithuania, and Sweden, all neighbours of the former Soviet Union, developed initiatives over the years to prepare their citizens to resist Soviet influence, and these methods remain applicable to the post–Cold War context. These states' "immune systems" involve extensive initiatives for educating residents and monitoring public information for unfounded claims, deception, and foreign media involvement (Singer & Brooking, 2018). According to a World Health Organization study, persons who "doubted the extent to which they received the message," or who "did not pass on the communication," reduced their exposure to fraudulent messages by about 80 per cent (WHO, 2020).

Increasing trust and decreasing misinformation affect both individuals and societies. The well-known word "influencers" implies that the way information is consumed is influenced by virtual and traditional leaders in a given group. Influencers in various organizations can be trained to establish resilience against false and erroneous information. They can have the ability to hinder the success of information efforts. Any team member who decides not to share material they are unsure about should double-check such material or even question the distributor (Bennett & Livingston, 2020).

In Israel, one further step aims to capitalize on the high trust enjoyed by the country's military leaders by institutionalizing their role as influencers even on subjects that are not strictly military or security related.

REGULATION AND GOVERNANCE MECHANISMS

In 1933, the British Mandatory authorities decided to regulate the Jewish and Arab press through the Press Ordinance and other censorship agencies. Similarly, the British government enacted the Emergency Protection Regulations in 1945, which required all printed material—newspapers, magazine, books—to be approved by the censor before being printed. As soon as Israel was established, the Press Ordinance and Emergency Protection Regulations were written into Israeli law. Israel is the only Western democracy where censorship is enshrined in law and enforced by the military itself (Goldschmidt & Warren, 2017).

In his piece "The End of Censorship," journalist Guy Kotev (1999) argues that new media technologies have led to the demise of censorship, which only persists due to the reactive nature of the media. Digital online media necessitates a makeover of Israel's unique censorship stance and relationship with the institutional media (Altshuler & Lurie, 2016). It might help develop the tools required to monitor, filter, and control content and information in order to avert potential harm. It might be utilized as a significant coordinating and synchronization hub for foreign governments' influence operations to undermine Israel's security and resilience. Similar organizations exist in other countries, including the United States, Australia, Denmark, and Belgium (Bodine-Baron et al., 2018; Cooperwasser & Simen-Tov, 2019).

These countries do not, however, have the same rules and mechanisms as Israel. The regulations imposed elsewhere may be problematic since they impede the transparency and critical thinking required for a thriving democracy, however, adopting them can give Israel an advantage in establishing resistance to influence campaigns. On the other hand, such regulations can be why Israel's National Cyber Security Directorate[1] does not consider defence against influence operations as part of its mission, despite global trends that place a high emphasis on such efforts (Goldschmidt & Warren, 2017).

Developing Military Resilience: Train Hard to Fight Easy?

A simulated battle breaks out several times a year, forcing the media to cover the killing of uninvolved people and the foiling of potential terrorist acts in a replica of the Internet designed to mimic what happens in real-world wars in the cyber and social networking dimensions. The fabricated network comprises blogs, foreign news outlets, and social media profiles that work together to create a virtual war in response to the real one. As the units trained at this facility deploy on operations, the "people" who oppose them use social media to organize their attacks. Singer and Brookings's book *Like Wars* (2018) features an interview with a former intelligence officer involved in developing these scenarios. According to him, such exercises enable soldiers to deal with a large and complex information environment. The significance of training is found in its application. As a first step, commanders must approach this as a new and extensive operational problem. The drills give commanders a better grasp of how social media may impact fights and be utilized by the enemy to influence them. The operators also learn how their activities affect media, how information operations affect their susceptibility and the vulnerability of their peers, and so discover better ways to deal with them. This way, the units develop resilience and are better equipped to operate in the networked social media environment.

Some commanders' education includes a social media literacy component that aims to educate units to operate in a social media context and to be critical consumers of information. To complement the updating of the new online communication directive, the IDF's chief education officer created a comprehensive kit for social media usage.

Understandably, soldiers' and commanders' social networking participation is limited in Israel. During an emergency, military personnel will be bombarded with information. It will be up to their training to determine how they will contribute to the military and national resilience through crucial information consumption.

Resilience through Technology Development

This fight against disinformation does not have to be conducted by humans alone. For instance, it is possible to block information in a widely distributed environment, as seen, for example, through the technology used in the war on pedophilia. PhotoDNA is a pedophilia-fighting content-control technology. Employing a database containing over a million visual objects, it compares any image or video submitted on social media to its massive collection of pedophilic images to verify that the image posted on the Internet does not include or promote pedophilia. Any major social media platform is likely to eventually integrate this technique, drastically lowering the number of pedophilia and child pornography cases on social media (Singer & Brooking, 2018).

In reaction to the PhotoDNA system's success, Facebook has announced a similar initiative to combat the spread of revenge porn—private photographs obtained illegally or without permission and then published on social media to harm the person being photographed. Facebook encourages people to report photographs and films they suspect of falling into this category. Similarly, it is technologically feasible to create a digital "fingerprint" for incorrect or harmful visual or textual material spread on social networks in order to monitor and prevent its spread (Statt, 2017).

Disinformation is a global problem, and many technologies are available to aid in the fight. This can begin with browser extensions that can notify you when information is suspected to be fake, sites that check suspicious information among expert communities, and plug-ins that check the credibility of information sources and block the display of suspected fake sources. All these technologies might be converted to the local arena or used to inspire the development of comparable tools for soldiers and commanders to resist fabricated, inaccurate, and misleading information. New tools are always being developed and enhanced through competitions, grants, and other resources (Knight, 2020). The Israeli setting may present distinct obstacles and opportunities due to the use of the Hebrew language. Israel should encourage the use of local platforms and the formation of collaborative action teams with media platforms. Learning from other countries' and platforms' collaboration has been successfully integrated into the fight against ISIS, for example. Building partnerships between heads of state, regulators, and technological platforms is a major component of such efforts. A meeting in 2016 between US defence leaders and the heads of Facebook, Twitter, Google, and other firms to develop a coordinated plan to diminish ISIS's social dominance provides an interesting illustration of this (Wong & Yadron, 2016).

Creating a Framework for Influence Operations Resilience

The literature in international law provides several recommendations concerning cyber security, foreign influence, multinational regulation of social networks, and other broadly applicable recommendations that take a long time to execute (Bodine-Baron et al., 2018). This chapter aims to provide proposals that will help nations and militaries right now, until long-term global solutions can be established. One crucial recommendation is to develop a doctrine capable of deterring opponents from participating in information operations by building their internal resilience mechanisms. To this end, I endorse Padan and Elran's (2018, p. 7) definition of resilience: "Resilience is a system's ability to adjust flexibly to interruption and the inevitable functional degradation that ensues, then quickly recover, return to full or even increased functionality." The key proposal for developing resilience to threats in this dimension is to take a proactive strategy, which can be drawn from the concept of resilience to cyber-attacks, available in many military doctrines, and then expand it. Cyber resilience refers to the ability to foresee, cope with, adapt to, and recover from challenges, pressures, or attacks on systems that use or are facilitated by cyber resources. The expansion proposed here is based on the National Institute of Standards and Technology's ideas around cyber resilience, which contain three interconnected layers: preparation, inclusion, and adaptation (Ross et al., 2019). In this section, I will go through the changes that need to be made to cyber resilience policy and the emphases that will allow these updated measures to cope with influence operations, and possibly deter them, as well as the concrete recommendations that will result from such changes.

PLANNING, TRAINING, AND GATHERING DEDICATED INTELLIGENCE

To fully understand an opponent's abilities, it is necessary to assign sufficient intelligence resources. One type of data collection is exploiting open-source intelligence, which adversaries frequently use to coordinate attacks. This could involve identifying suspected negative influence attractors online, establishing analysis tools, and developing and exposing techniques for identifying bots, fake profiles, and coordinated influence networks.

Planning and gathering information intelligence is not enough, however. Practice makes perfect, and this is especially true when it comes to building resilience. Nations and militaries must brace themselves for influence operations that may undermine the public's faith in the military.

Monitoring and developing appropriate metrics and base rates are part of the preparation process. This should also include incorporating and enforcing the use of various monitoring technologies so that campaigns can be discovered and impacted. These tools should collect data on various parameters, such as posts produced by Israeli users versus posts published from other nations. Moreover, regularly monitoring and evaluating popular trust in the military is crucial. Such monitoring will allow for the detection of anomalous activities during ordinary operations, thereby contributing to our understanding of what works and what does not in the narrative battle over these topics, and developing methods for mitigating those impacts in emergencies and crises. Furthermore, regular monitoring will aid in detecting fake accounts influencing soldiers or preparing infrastructure for subsequent cyber activities.

DEVELOPING FAST INCLUSION AND RESPONSE

This phase is the time between the onset of an unrecognized campaign's effect and its discovery and containment to the point that it does not cause more damage. It is part of responding to an occurrence quickly and creating the resilience needed to continue functioning. Influence operations necessitate more resources, just as resources are required to cope with a significant occurrence. In a severe occurrence that undermines the credibility and legitimacy of army actions, damage must be identified and successfully addressed as well as attributed to specific causes. Specific counter-campaigns should be used to deal with such damage in order to reduce the short- and long-term harm.

Conclusion

Once the Internet became a battleground, its influence could potentially be felt by militaries and governments, civilians and operators, in the realms of politics and war alike. Identifying who might be hurt by such behaviour is critical in developing and evaluating coping mechanisms. The multiplicity of actors makes it difficult for militaries and governments to engage in initiatives in this area.

When a security organization, the IDF, or other forces monitor social media influence and messaging, a delicate balance must be struck that allows for the preservation of civil and democratic rights following legislation and regulations. While the Israeli context is unique, there is much to be learned from its experience with the threat from Iran in a systematic manner, considering the different contexts of other nations.

Can resilience deter opponents in this field? To date, resilience can be seen as a strategy to combat hybrid warfare campaigns. It can also be a potent deterrent for opponents in this arena by making it difficult for them to achieve their goals while also allowing the defender to exhibit a sense of readiness and preparedness that provides the ability to "bounce back" in the face of such campaigns and to diminish their intended impacts. Although Israel can further strengthen its resilience, the intensifying confrontation with Iran has yet to prove the role of resilience as a deterrent.

Disinformation divides societies and organizations into groups by exploiting psychological and sociological weaknesses. This is more than a scientific debate for us: How can we ensure that open access to information allows for a constant appraisal of various societal views while minimizing the potential damage caused by distorted and fraudulent information intended to weaken Western militaries and societies?

According to Paul Virilio (1991, 2005), a technology philosopher, every new technology is followed by an accident, a catastrophe caused by its unique point of failure. He asserted that the invention of the ship brought about the possibility of the shipwreck, the development of the plane brought about the possibility of the plane crash, and the discovery of the automobile brought about the possibility of the car accident. The spread of disinformation could be considered a social network accident or disaster. The greater the flow and movement of information, the more difficult it is to separate the wheat from the chaff and prevent foreign forces from being impacted via cyber or influence campaigns. As we become more dependent on digital systems, we add new risks to our lives—risks that we must strive to reduce in order to enjoy the benefits of the digital age fully. It is simply a question of seizing the opportunity before influence activities occur, as has happened worldwide.

This chapter indicates that resilience might complement deterrence in a novel way, reducing enemy achievements in this domain by action and supporting frameworks and doctrines that will bring about greater results without endangering the open and democratic society's resilience.

NOTES

[1] Located within the Prime Minister's Office, the National Cyber Security Directorate is the security entity responsible for protecting the Israeli civilian cyber space. For more information, see their web site at https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page.

REFERENCES

Altshuler, T. S., & Luria, G. (2016). *Censorship and security secrets in the digital age* [Hebrew]. Policy Research 113. Israel Democracy Institute.

Andrejevic, M. (2013). *Infoglut: How too much information is changing the way we think and know*. Routledge.

Bar-Gil, O. (2020). *In world media # 2: The coronavirus as an infodemia* [Internal report; Hebrew]. Applied Research Institute for Behavioral Sciences in the IDF.

Bellingcat. (2018, 20 November). Truth in a post-truth world [Dutch]. *BNNVARA*. https://joop.bnnvara.nl/videos/terugkijken-idfa-documentaire-bellingcat-truth-in-a-post-truth-world

Bennett, W. L., & Livingston, S. (2020). *The disinformation age: Politics, technology, and disruptive communication in the United States*. Cambridge University Press.

Bergstrom, C. T., & West, J. D. (2020). *calling bullshit: the art of skepticism in a data-driven world*. Random House.

Bodine-Baron, E., Helmus, T. C., Radin, A., & Treyger, E. (2018). *Countering russian social media influence* (RR-2740-RC). RAND Corporation. https://www.rand.org/pubs/research_reports/RR2740.html

Brooker, G. (2011). The clocks that ticked lazily: The army's conduct in the tension between legitimacy and the limits of the use of force [Hebrew]. *Between the Arenas*, 10, 12–33.

Bush, D. (2020, July 30). *Two faces of Russian information operations: Coronavirus coverage in Spanish*. Stanford Internet Observatory. https://fsi.stanford.edu/news/two-faces-russian-information-operations-coronavirus-coverage-spanish

Chivvis, C. (2017). *Understanding Russian "hybrid warfare": And what can be done about it*. RAND Corporation. https://doi.org/10.7249/CT468

Clarke, C. P. (2017, 19 September). How Hezbollah came to dominate information warfare. *RAND Blog*. https://www.rand.org/blog/2017/09/how-hezbollah-came-to-dominate-information-warfare.html

Clausewitz, C. von. (1989). *On war, indexed edition* (M. E. Howard & P. Paret, Trans.; Revised ed.). Princeton University Press.

Cohen, S. (2018, 6 September). This is not an Israeli site; this is Iranian propaganda [Hebrew]. *YNET*. https://www.ynet.co.il/articles/0,7340,L-5342357,00.html

Coles, I., Osseiran, N., & Donati, J. (2019, 28 October). Islamic State spokesman killed in U.S. airstrike. *Wall Street Journal*. https://www.wsj.com/articles/islamic-state-spokesman-targeted-in-u-s-airstrike-say-kurds-11572268364

Cooperwasser, J., & Siman-Tov, D. (2019). *The battle for consciousness: Strategic and intelligent aspects*. Institute for National Security Studies. https://www.inss.org.il/he/publication/the-cognitive-campaign/

Goldschmidt, R., & Wergan, J. (2017). *Dissemination of false information on the Internet and cyber-attacks to influence elections* [Hebrew]. Knesset Research and Information Center.

Greenberg, A. (2019a, 23 August). Cyberwar: The complete guide. *Wired*. https://www.wired.com/story/cyberwar-guide/

Greenberg, A. (2019b). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. Doubleday.

Halperin, J. (2020a, 22 October). Gil Schweid: "The future of the cyber world—scary" [Hebrew]. *People and Computers*. https://www.pc.co.il/news/324292/

Halperin, J. (2020b, 25 November). Minister of intelligence: "Iran is trying to influence Israeli public opinion online" [Hebrew]. *People and Computers*. https://www.pc.co.il/featured/326648/

Hwang, Y., Ryu, J. Y., & Jeong, S.-H. (2021). Effects of disinformation using deepfake: The protective effect of media literacy education. *Cyberpsychology, Behavior, and Social Networking, 24*(3). https://doi.org/10.1089/cyber.2020.0174

IDF (2019). *Field guide for information operations* [Internal report; Hebrew].

Jenkins, B. M. (1974). *International terrorism: A new kind of warfare* (No. P5261). RAND Corporation. https://www.rand.org/content/dam/rand/pubs/papers/2008/P5261.pdf

Kotev, G. (1999, 9 September). The end of censorship. [Hebrew]. *7th Eye*. http://www.the7eye.org.il/23579

Kubovich, Y. (2021, 18 August). Israeli army employs popular blogger for psyops on social media. *Haaretz*. https://www.haaretz.com/israel-news/2021-08-18/ty-article/.premium/is-the-idf-behind-popular-arab-news-telegram-channel/0000017f-dc61-d3ff-a7ff-fde14daf0000

Mazarr, M. J. (2021). Understanding deterrence. In F. Osinga & T. Sweijs (Eds.), *NL ARMS Netherlands annual review of military studies 2020: Deterrence in the 21st century—insights from theory and practice* (pp. 13–28). Asser Press. https://doi.org/10.1007/978-94-6265-419-8_2

Mazarr, M. J., Chan, A., Demus, A., Frederick, B., Nader, A., Pezard, S., Thompson, J. A., & Treyger, E. (2018). *What deters and why: Exploring requirements for effective deterrence of interstate aggression*. Rand Corporation. https://www.rand.org/pubs/research_reports/RR2451.html

Mazarr, M. J., Rhoades, A. L., Beauchamp-Mustafaga, N., Blanc, A. A., Eaton, D., Feistel, K., Geist, E., Heath, T. R., Johnson, C., Langeland, K., Léveillé, J., Massicot, D., McBirney, S., Pezard, S., Reach, C., Vedula, P., & Yoder, E. (2022). *Disrupting deterrence: Examining the effects of technologies on strategic deterrence in the 21st century*. Rand Corporation. https://www.rand.org/pubs/research_reports/RRA595-1.html

Newman, L. H. (2019, 6 May). What Israel's strike on Hamas hackers means for cyberwar. *Wired*. https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/

O'Connor, C., & Weatherall, J. O. (2019). *The misinformation age: How false beliefs spread*. Yale University Press.

Padan, K., & Elran, M. (2018). *Localities in the "Gaza envelope"—a test case for social resilience in Israel (2006–2016)* [Hebrew]. Institute for National Security Studies.

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2019). *Developing cyber resilient systems: A systems security engineering approach* (NIST SP 800-160v2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2

Rubinstein, R. (2019, 31 January). Report: The Iranian "bot" army trying to influence the Israeli elections [Hebrew]. *YNET*. https://www.ynet.co.il/articles/0,7340,L-5455832,00.html

Sabbagh, D., & Roth, A. (2020, 16 July). Russian state-sponsored hackers target Covid-19 vaccine researchers. *The Guardian*. https://www.theguardian.com/world/2020/jul/16/russian-state-sponsored-hackers-target-covid-19-vaccine-researchers

San-Akca, B. (2014). Democracy and vulnerability: An exploitation theory of democracies by terrorists. *Journal of Conflict Resolution, 58*(7), 1285–1310.

Schaefer, B. (2018, 12 March). The cyber party of God: How Hezbollah could transform cyberterrorism. *Georgetown Security Studies Review*. https://georgetownsecuritystudiesreview.org/2018/03/11/the-cyber-party-of-god-how-hezbollah-could-transform-cyberterrorism/

Schia, N. N., & Gjesvik, L. (2020). Hacking democracy: Managing influence campaigns and disinformation in the digital age. *Journal of Cyber Policy, 5*(3), 413–428. https://doi.org/10.1080/23738871.2020.1820060

Scott, M. (2020, 19 November). In race for coronavirus vaccine, Russia turns to disinformation. *Politico*. https://www.politico.eu/article/covid-vaccine-disinformation-russia/

Shafran-Gittleman, I. (2022, 10 January). Restoring public trust in the IDF. *Israel Democracy Institute*. https://en.idi.org.il/articles/38089

Shahaf, T. (2019, 8 May). *Hamas' cyber capabilities have been fatally damaged* [Hebrew]. *YNET*. https://www.ynet.co.il/articles/0,7340,L-5506315,00.html

Singer, P. W. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Singer, P. W., & Brooking, E. T. (2018). *Likewar: The weaponization of social media*. Eamon Dolan/Houghton Mifflin Harcourt.

Statt, N. (2017, 7 November). Facebook's unorthodox new revenge porn defense is to upload nudes to Facebook. *The Verge*. https://www.theverge.com/2017/11/7/16619690/facebook-revenge-porn-defense-strategy-test-australia

Stengel, R. (2019). *Information wars: How we lost the global battle against disinformation and what we can do about it*. Atlantic Monthly Press.

Summers, J. (2017, 25 October). *Countering disinformation: Russia's infowar in Ukrain*e. Henry M. Jackson School of International Studies. https://jsis.washington.edu/news/russia-disinformation-ukraine/

Thiele, R. D. (2016). Building resilience readiness against hybrid threats—a cooperative European Union/NATO perspective. *ISPSW Strategy Series: Focus on Defense and International Security, 449*. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/ISPSW-Building%20Resilience%20Readiness%20against%20Hybrid%20Threats.pdf

Thomas, Z. (2020, 13 February). Misinformation on coronavirus causing "infodemic." *BBC News*. https://www.bbc.com/news/technology-51497800

van Doorn, C., & Brinkel, T. (2021). Deterrence, resilience, and the shooting down of Flight MH17. In F. Osinga & T. Sweijs (Eds.), *NL ARMS Netherlands annual review of military studies 2020: Deterrence in the 21st century—insights from theory and practice* (pp. 365–83). TMC Asser Press. https://doi.org/10.1007/978-94-6265-419-8_19

Virilio, P. (1991). *Lost dimension*. Semiotext.

Virilio, P. (2005). *The information bomb*. Verso.

WHO (World Health Organization). (2020). *Immunizing the public against misinformation*. https://www.who.int/news-room/feature-stories/detail/immunizing-the-public-against-misinformation

Wong, J. C., & Yadron, D. (2016, 8 January). Silicon Valley appears open to helping US spy agencies after terrorism summit. *The Guardian*. http://www.theguardian.com/technology/2016/jan/08/technology-executives-white-house-isis-terrorism-meeting-silicon-valley-facebook-apple-twitter-microsoft

Ziv, A. (2020, 12 April). The cyber-attack on Shirbit—who is behind it and why it is worrying [Hebrew]. *The Marker*. https://www.themarker.com/technation/.premium-1.9348718