IDF Spokesperson

The Main Challenges Facing Strategic Intelligence

Itai Shapira

This article analyzes the main contemporary challenges facing strategic intelligence, particularly in Israel and the United States. These challenges derive from shrinking trust in state institutions; the decline in the status of truth in the post-truth and fake news era; the "addiction" bordering on absolute dependence of commanders and decision makers on operational and tactical intelligence; and the inherent limitation of the ability of intelligence to influence leaders' vision and ideology. Although these are not new challenges, they are intensified in today's day and age, in part by the interface between them. In the era of advanced technologies and big data, strategic intelligence might find it difficult to justify its epistemological and professional basis. This article recommends methodological reflection and a technological leap forward in strategic intelligence, which now, needed more than ever, must undergo a revolution within the greater intelligence world. It is precisely because of these multiplying challenges and their complex environment that while this is the darkest hour for strategic intelligence, it is also its finest hour.

Keywords: intelligence, strategic intelligence, post-truth, fake news, intelligence methodology, decision making intelligence, politicization of intelligence, terror, campaign between wars

Introduction

This article analyzes the main challenges currently facing strategic intelligence, stresses their singularity in relation to the challenges facing operational and tactical intelligence, and recommends some directions for addressing them. It focuses primarily on Israel and the United States, and in light of differences between national intelligence cultures (Crosston, 2016), it tends toward the "Anglosphere" (the United States and Western countries) (Aldrich & Kasuku, 2012).

The article does not present a comprehensive discussion of the nature of strategic intelligence, or of the relationship between intelligence and leaders; both subjects have been extensively studied (for example, Johnson, 2003; Gazit, 2004). For the purposes of this article, strategic intelligence (Brun, 2015) is seen first of all as a field that serves the strategic decision making echelons (in Israel: the politicians, and in a certain sense, the IDF General Staff and the heads of organizations in the intelligence community). Second, the field deals with the strategic environment (the strategic echelons of adversaries, rivals, and friends, and with elements that influence strategy—the stability of regimes, economies, technologies, and so on). Its primary purpose is to provide information, but also to create knowledge and insights that are relevant to the planning, implementation, and critical review of strategy. It is also in charge of clarifying reality on a strategic level[1] and for creating insights that affect strategy. In turn, this should lead to changes in reality (Dado Center, 2016).

The article covers a variety of challenges: sociological, philosophical, methodological, and technological; challenges connected to the nature of the leaders; and others relating to the environment in which intelligence operates. It posits that unlike in operational and tactical intelligence, most of the challenges derive from the difficulty of strategic intelligence to establish its epistemological and professional authority. While most of the challenges are not new, it appears that changes in the strategic environment, together with significant improvements in operational and tactical intelligence, the unique character of some decision makers, subversion of the status of truth and facts in decision making processes in the post-truth and fake news era, and technological changes in the information age intensify familiar challenges.

A recent description of the glass ceiling of strategic security intelligence proposes learning from the world of business (Barnea, 2019), but this article argues that in the current era, there is actually an increase in the added value strategic intelligence can provide for commanders and leaders. In order to meet these challenges, national strategic intelligence must engage in methodological reflection and implement advanced technologies. It must undergo the same Revolution in Intelligence Affairs (RIA) as did operational and tactical intelligence.

Context

A recent article (Palacios, 2018) offers a sharp description of the challenges faced by strategic intelligence "in the post-everything age" and hints at the ramifications of post-modernism, post-truth, and fake news. First, strategic intelligence competes for the attention of decision makers against other elements that create strategic information, knowledge, and insights; second, traditional intelligence grew and developed in the modern era in which it was important to clarify the truth, but in the post-modern era the status of truth is undermined and is replaced with narratives; third, traditional intelligence developed on the basis of a perception that the exposure of secrets would help complete the puzzle, but today it is necessary to deal more with mysteries and complexities; fourth, traditional intelligence focused on countries and organized entities, but today must deal with non-state and non-organized entities, and identify emerging units; fifth, a considerable number of leaders' decisions today are based on opinions,

perceptions, beliefs, and their derivatives, rather than on intelligence; sixth, strategic intelligence is used to support decisions that have already been taken, and in effect help the leaders to "market" narratives to the public; and seventh, intelligence organizations strive to strengthen their influence by means of strategic intelligence, while decision makers are more interested in operational and tactical intelligence, and even use intelligence for other needs, such as covert diplomacy. This analysis forms the basis for the challenges discussed below.

Contemporary Challenges to Strategic Intelligence

Competition and the National Intelligence Monopoly

Competition for attention of leaders and the loss of the national intelligence monopoly have been mentioned in recent years largely in the context of information overload (Treverton, 2004) and the availability of open information and intelligence (William & Blum, 2018). In 2005 it was even suggested that intelligence analysis could become less relevant for decision makers (Teitelbaum, 2005). Some have referred to "the rise and fall of intelligence" in the 20th century (Warner, 2014), while others argue that intelligence is currently the business of many elements apart from security intelligence, partly in view of the development of artificial intelligence and machine learning (Brantly, 2018). In other words, for the last decade strategic intelligence has been fighting for its place.

Presumably in cases where operational and tactical intelligence is required—to launch air attacks, frustrate terrorism, level focused economic sanctions, and so on—national intelligence faces no real competition. But at the strategic level, the situation is different.

The first potential area of competition is linked to the possibility that leaders do not rely only on intelligence to clarify and understand situations, but rather base their decisions on their own direct understanding of the strategic environment as well. For example, US President Trump, responding to an assessment by the American intelligence community of January 2019 that Iran was not taking the steps necessary to develop a military nuclear project, said that the intelligence personnel "should go back to school," since in his opinion they were "passive and naive" (Oprysko, 2019). Trump's different assessment regarding Iran was ostensibly not a case of deliberate deflection or politicization of intelligence (Hastedt, 2013), but reflected his own assessment of the strategic environment, which in this specific case differed from that of the intelligence professionals. To be sure, the phenomenon of leaders "ignoring" intelligence that does not match their own perceptions is not new (Handel, 1989); however, in recent years leaders have apparently acquired greater access to the strategic environment, inter alia through direct meetings between the leaders themselves, and through the use of technology that enables them to consume "customized" information. Therefore, it is possible that they have a stronger sense that strategic intelligence created by national state institutions offers no added value in relation to their own understanding of the situation.

Presumably in cases where operational and tactical intelligence is required—to launch air attacks, frustrate terrorism, level focused economic sanctions, and so on—national intelligence faces no real competition. But at the strategic level, the situation is different.

The second possible area of competition is linked to the security and civilian research institutes and think tanks that are engaged in strategic analysis. Much of the output of these institutions is designed to influence strategy and policy (e.g., Institute for National Security Studies—INSS; RUSI; Chatham House; Washington Institute; Belfer Center for Science and International Affairs). Research studies created by these civilian institutions examine

interactions between arenas and beyond arenas; deal with more than military aspects; analyze developing technologies; and create an assessment and long term forecast. They also include a combination of observations of "the red" (the environment) and "the blue" (own forces) in net assessment/thinking (such as Marshall, 1972)—a subject that is sometimes absent from security intelligence products, which are ostensibly not supposed to analyze "the blue side." In Britain, for example, the study produced by a long term analysis of the strategic environment was not written by an intelligence entity (Ministry of Defence, 2018).

The main challenge, therefore, derives from the possibility that some decision makers feel that there is a substitute for strategic intelligence. This position might have existed in the past, but the leadership style of some contemporary decision makers intensifies it.

The main challenge, therefore, derives from the possibility that some decision makers feel that there is a substitute for strategic intelligence. This position might have existed in the past, but the leadership style of some contemporary decision makers intensifies it. Moreover, it appears that leaders do not have the same approach to operational and tactical intelligence. If this hypothesis is correct, it explains why strategic intelligence might face difficulty in establishing and justifying its epistemological basis and demonstrating to the leadership its unique added value.

The Decline of Truth and the Rise of Narrative

The common assumption is that intelligence is an institution to clarify reality and discover truth (Brun, 2015). A notable reflection of this perception is the way the American intelligence community describes their relations with senior members of the administration, namely, "truth to power" (Morrell, 2018). Brun and Roitman (2019) argue that in the post-truth and fake news era it is difficult to clarify reality, and this harms decision making in the fields of national security. In their view, such decisions are often made on the basis of beliefs, opinions, and feelings, rather than on the basis of orderly processes (that includes strategic intelligence) conducted by professionals—as part of the broader trend of a loss of faith in state institutions. RAND even gave the trend a name: "truth decay" (Kavanagh & Rich, 2018). Brahms (2019) described the link between post-truth and the difficulty of discovering objective truth, and the era of technology and information overload. Michlin-Shapir and Padan (2019) use the concept "liquid modernity" and claim that today's prevalent approach holds that there is not one single truth but a range of narratives, and there is no central authority that is able to judge which narrative is correct. These issues are relevant to the discussion of strategic intelligence.

National intelligence developed in the modern age, which prioritized truth and deemed science the main institution for its discovery. In this sense, it is a clear product of the Enlightenment (Hayden, 2017). In Israel there was an emphasis on the need to use scientific methods in intelligence practice (Ben-Israel, 1999), and the terminology used by the American intelligence community—based on the tradition of Kent (1949), who saw intelligence as a scientific discipline—shows how they carried the torch of the search for truth. Perhaps not surprisingly, etched into the wall of the lobby of the CIA Original Headquarters Building is a verse from the Book of John (8:32): "And ye shall know the truth, and the truth shall make you free."

However, the literature recognizes the limitations of intelligence to function only as "an institution for discovering truth." As far back as the early 1960s, Wasserman (1960) wrote about erroneous basic assumptions—naive realism and inductionism—that lead to intelligence failures. Wasserman attacks the perception that can be called "objectivist," which maintains not

only that the objective truth exists, but also that intelligence can reveal it using scientific methods. In Israel, Granit (2006) was one of the most prominent opponents of this perception, which he called "the realistic paradigm." The American application of this approach was recently thoroughly researched (Marrin, 2020).

In addition, the term "post-modern intelligence" has arisen often in recent years (Rathmell, 2002), and studies claim that scientific approaches should be combined with creative approaches (Cavelty & Mauer, 2009). It is possible that intelligence has remained planted in the positivist approach, while it is in fact other disciplines in the fields of social sciences and the exact sciences that are liberating themselves from this paradigm (Manjikian, 2013).

At the same time, it does not appear as though leaders have stopped asking intelligence to uncover the truth. In 2018, for example, Israeli Prime Minister Netanyahu presented the operation by the Israeli intelligence community to disclose the Iranian nuclear archive. He claimed that Iran had lied to the international community about its military nuclear project (Hai, 2018), and also revealed the sites used by Hezbollah in Lebanon to convert rockets into precision missiles (Azoulay, 2018). The implication is that not only does the Prime Minister deem truth important; he also uses intelligence to reveal it. In the United States, while the Trump era is perceived as an expression of post-truth and deliberate lies (Cassidy, 2018), it also looks as if the American President is not questioning the importance and place of truth and facts, but rather arguing that national intelligence institutions have not engaged in clarification of the relevant facts. The President claimed—contrary to the facts presented by the intelligence community in January 2019—that Iran had conducted tests with rockets, that the Iranian economy was collapsing, that North Korea had stopped testing missiles and returned the American prisoners, and more (Oprysko, 2019). In fact, the President did not present narratives that were not dependent on truth, but focused on facts and truths, including the "alternative facts" (Bradner, 2018) that supported his narratives.

While the subversion of the importance of truth is a challenge for intelligence in general and strategic intelligence in particular and may have intensified recently, it appears that leaders are not necessarily questioning the ontological basis of the truth. However, they are perhaps questioning the epistemological, institutional, and methodological basis of intelligence for the discovery of truth. Moreover, since strategic intelligence deals fundamentally with abstract phenomena that are open to interpretation and less with physical facts defined by orderly and generic behavior (Shapira, 2020), it is harder to apply the concepts of "truth" and "facts" to it. It appears therefore that strategic intelligence has difficulty justifying its epistemological basis mainly for the purpose of an abstract description of the strategic environment. Operational and tactical intelligence do not face a similar challenge, since they deal mainly with the discovery and exposure of factual and physical truths. They are concerned with secrets, while strategic intelligence focuses also (although not only) on puzzles and mysteries.

Secrets, Puzzles, and Mysteries

Many argue that today's intelligence must deal mainly with highly complex mysteries (Treverton, 2004), whereas formerly—for example, in the struggle against the Soviet Union during the Cold War in the American context, or in the location of military preparations for war on the part of Syria and Egypt in the Israeli context (Gazit, 2003)—it was primarily concerned with revealing secrets.

Nevertheless it appears that strategic intelligence has dealt with mysteries for many years (Hulnick, 1999). A study of the archives of National Intelligence Assessments in the United States illustrates this, and a similar phenomenon is found in Britain (Cradock, 2002). However, it appears that the mysteries have become more complex. For example, in

its National Intelligence Estimates, American intelligence presents issues relating to advanced technologies, artificial intelligence, energy, climate, organized crime, and cyber. In order to locate developments in these areas, a different kind of strategic intelligence is required, unlike its previous format in which it was mainly intended to warn of war preparations or report on regime stability. Moreover, many of the current mysteries are not focused on just one country, but are also linked to non-state entities.

In its National Intelligence Estimates, American intelligence presents issues relating to advanced technologies, artificial intelligence, energy, climate, organized crime, and cyber. In order to locate developments in these areas, a different kind of strategic intelligence is required, unlike its previous format in which it was mainly intended to warn of war.

Irregular and Non-State Entities, and New Cyber Challenges

Numerous studies have stressed the need to adapt intelligence to deal with terror (Herman, 2003a), and maintain that today's central challenges originate in irregular entities (Freedman, 2006). Terror organizations, cyber hackers, and international technology companies are prominent examples of such entities, but in recent decades intelligence organizations have made changes to deal with them, so these are not new challenges for strategic intelligence.

In Israel, for example, warnings of war preparations are a vital component in the concept of security (Hershkovitz, 2017) and in IDF strategy (IDF, 2018), but in recent years changes have been required in the functions of intelligence in this context. Kuperwasser (2007), for example, described changes introduced in the first decade of the new millennium; Kochavi & Ortal (2014) and Brun (2015) described changes in the IDF Intelligence Directorate since 2011, based in part on the need to produce additional output apart from war alerts. In fact it appears that Israeli intelligence has succeeded in adjusting to the challenges of terror (Kabir, 2019; Shpiro, 2012), and for some years has focused on irregular and sub-state entities, whose activities also find expression in interactions between arenas and beyond arenas (A. E., 2016). This issue in itself does not create a new challenge.

Moreover, the need to deal with state and regular issues is actually returning, and to a large extent presents itself as in the Cold War period (Hennigan, 2018). A study of documents published by the US administration dealing with national security issues in 2015-2019 national security strategy (The White House, 2017; The Pentagon, 2018; Joint Chiefs of Staff, 2015; Office of the Director of National Intelligence, 2019; and Coats, 2019) illustrates the greater priority given to the two countries that create strategic competition (the great powers competition)—China and Russia—and the lower priority given to two rogue countries—North Korea and Iran. In April 2019 the CIA Director remarked that in recent years the Agency had focused on fighting terror and supporting military operations, but had neglected its traditional capabilities vis-à-vis states (Central Intelligence Agency, 2019).

Thus it appears that the need to deal with irregular and non-state entities, together with the necessity to engage once again in traditional intelligence concerning states, does not create new challenges for strategic intelligence. However, an examination of the challenges facing American strategic intelligence with respect to countries such as Russia, China, and North Korea leads to an assessment that it is no longer only a matter of issuing warnings when military force and expeditionary forces are activated, or about the deployment of nuclear weapons or the stability of the regime and the economic situation. American intelligence is required—in addition to, and not instead of the above—to analyze scenarios in the cyber

dimension. To a large extent this is a new challenge.

Although the literature is replete with studies of cyber as a dimension of warfare (Sharma, 2010); of the need to create a revolution in intelligence affairs in the reciprocal relationship between data collection and research (Siman Tov & Allon, 2018); of the difficulty of attributing a cyber attack to its source (Rid & Buchanan, 2015); of intelligence as the basis of creating cyber defense (Mattern et al., 2014); of the intelligence challenge posed by cyber attacks on national infrastructures (Rudner, 2013); of the challenge of exploiting cyber to track the sources of terrorist funding (Winston, 2007); of the cyber challenge created by states (Brantly, 2014); and more, it is hard to find a rich theoretical basis for a discussion of the link between strategic intelligence and the cyber dimension. Are concepts such as "strategic warning" or "a Pearl Harbor-type surprise" relevant in the field of cyber (Wirtz, 2018)? Is the link between operational/military intelligence that deals with capabilities and strategic intelligence that deals with intentions also relevant to the cyber dimension? How, for example, should strategic intelligence handle groups of Russian or North Korean hackers? And can it make use of a methodology similar to the one used to track operational expressions of the strategic logic of Russia and North Korea? The dearth of literature dealing with these issues and with the concept of "strategic cyber intelligence" to a great extent demonstrates the intensity of the challenge.

Intelligence and Leadership

Complicated links between leaders and intelligence, whereby intelligence is used to support decisions already made by leaders, existed in the past (Herman, 2003b; Bar-Joseph, 1998; Freedman, 1997). Matza (2017), for example, described strategic intelligence inter alia as the "spokesperson" that enables the leader to recruit public support for a decision that has already been made. The use of intelligence to facilitate the United States withdrawal from the war in Iraq in 2003 is an accepted example of this process (Hastedt, 2005; Freedman, 2004).

It appears that the relationship between a leader and intelligence—which is also influenced by the character and personality of the leader (Steinhart & Avramov, 2013)—could today, as in the past, lead to a politicization of intelligence. But it is possible that intelligence organizations are currently perceived as part of the traditional establishment, and certain leaders even demonstrate a lack of trust in them (Zelizer, 2018). In the United States, for example, it is argued that the CIA is going through a process of politicization, marked by opposition to the President's approaches (Gentry, 2018); some Agency employees have described liberal bias (Gertz, 2018); and even in the 1960s it was possible to discern political bias in its assessments (Freedman, 1997).

Strategic intelligence continues to struggle with a familiar challenge—the superiority that leaders ascribe to their own world view and ideology compared to the professional analysis, and certainly if the latter claims to be objective. Operational and tactical intelligence appears not to confront a similar challenge, since its main purpose is to enable the implementation of policy, and not to influence or change it.

There have already been some who argued that strategic intelligence analysis has had limited influence over American foreign policy (Marrin, 2017); that US presidents since World War II have arrived "prepared" for the presidency with perceptions and strategies, and intelligence only influences them to the extent that it supports their original views (Immerman, 2008); or that even though the strategic intelligence was high quality and relevant, the leaders often chose not to make use of it (Kovacs, 1997). In this sense, strategic intelligence continues to struggle with a familiar

challenge—the superiority that leaders ascribe to their own world view and ideology compared to the professional analysis, and certainly if the latter claims to be objective. Operational and tactical intelligence appears not to confront a similar challenge, since its main purpose is to enable the implementation of policy, and not to influence or change it.

But do today's leaders rely on beliefs, opinions, and feelings more than in the past? Does the debate that they lead today deal more with ideology than in the past, which means they have less need of intelligence that is designed to reveal the truth and presents itself as objective, or do they feel that they are less dependent on strategic intelligence than their predecessors? A full response to this question is beyond the scope of the present study, but leaders and commanders seem to rely increasingly on tactical intelligence.

Improved Operational and Tactical Intelligence: At the Expense of Strategic Intelligence?

Intelligence Gathering and Output

In recent years collecting and processing intelligence capabilities have greatly improved, thanks partly to advanced technology, artificial intelligence, and machine learning (Weinbaum & Shanahan, 2018). This allows more intimate access to raw information, which ostensibly gives a better reflection of what is happening in the area where the data is collected. It seems reasonable for leaders and senior commanders to demand and consume such information, which consists almost entirely of operational and tactical intelligence.

The importance of reading raw information and the "addiction" of leaders to such information are not new—at least in Israel (Ben-Porat, 1984; Bar-Joseph, 2013). However, it seems likely that these phenomena have intensified in recent years in view of the quality and intimacy of the data. Therefore, the more a commander makes use of intimate and sensitive information that symbolizes penetrating to the heart of the secret, the more information he or she feels is needed, and it must be more intimate. And the more intimate the information, the more powerful the addiction.

While the use of tactical information and intelligence is relatively intuitive, and leaders or commanders may feel that they experience the environment directly without the need of interpretation or mediation, this is likely not the case with strategic intelligence (in this context an American study even examined the difficulty for senior generals of using strategic intelligence; Wolfberg, 2017). While tactical intelligence is usually factual and therefore also concrete and deals with physical entities, strategic intelligence is usually abstract and vague, and deals with human phenomena that are difficult to quantify. Therefore it is difficult to point to a link between improved data collection and improved strategic intelligence, more than to the impact of improved collection on the quality of tactical intelligence. And since this is the case, leaders are apparently more and more "addicted" to operational and tactical intelligence, but not necessarily more dependent on strategic intelligence.

However, military actions that depend on tactical intelligence also require high quality strategic intelligence for their formulation and implementation.

The War on Terror in the United States, Prevention and Influence Strategy, and the Campaign between Wars in Israel

The strategy of prevention and influence is a central component of IDF strategy (IDF, 2018) "to frustrate the threats, to deter and postpone war, and to shape the area in a way that suits Israel…and damage the enemy's capabilities in order to create the optimal military, political, and cognitive conditions for the future decision of any war that may erupt, and to strengthen deterrence" (pp. 19-20). The campaign between wars (CBW) makes it possible to implement this strategy: "CBW activity is ongoing, exists in every arena of war, based on a situational assessment

and the facilitating intelligence…CBW activity is based on quality intelligence" (p. 24). In order to carry out an attack in Syria against Iranian and Hezbollah sites, to expose the Hezbollah tunnels on the Lebanese border (Mizrachi, 2019), or to attack the legitimacy of Hezbollah in the international community (Zeitoun, 2018), there is a need for high quality and intimate operational and tactical intelligence, at high resolution and in real time. And since CBW has become a central component of Israeli security activity (Zeitoun & Porat, 2019), the demand for this type of intelligence will probably grow.

But how far is strategic intelligence adapted to the format of CBW warfare? Intelligence at various levels, including the strategic level, is described as one of the conditions for its implementation (Allon & Freizler-Swiri, 2019). CBW planning and implementation requires the highest quality of strategic intelligence, which analyzes the strategic environment holistically and identifies windows of opportunity; possibly this was the process that in recent years led Israel to embark on a campaign against Iranian entrenchment in Syria (Even, 2019). However, a study of the professional literature reveals a significant gap in the methodological debate about the link between strategic intelligence and CBW. Apparently, CBW—given the high speed at which it is managed, the significant risks it involves, and its need to engage constantly with secrets, but also with puzzles and mysteries—creates a new challenge for strategic intelligence.

In the United States it is also possible to point to a link between the rise in importance and relevance of certain types of conflict—above all the war on terror (CT – counterterrorism) and insurgency (COIN – counterinsurgency)—and the prominence of operational and tactical intelligence. For example, there is a strong link between operational and tactical intelligence and the activity of the American Special Forces (Gentry, 2017) and these forces are the central component of the war on terror. But what is the place of strategic intelligence in these forms of action? Some argue that the American intelligence community has adopted an approach that puts the emphasis on information (information-centric intelligence) and by implication on tactical intelligence, more than on research and assessment (Dudley, 2018). In Britain it has been claimed that the roles of strategic intelligence are in doubt (Gibson, 2009). Moreover, in the United States there is apparently a trend of focusing on current intelligence in a way that leads to neglect of capabilities and skills that are more relevant to strategic intelligence (Marrin, 2013; Heinderich, 2007). A further illustration of the prominence of operational intelligence rather than strategic intelligence emerges from an analysis of the place of intelligence in the Revolution in Military Affairs (RMA) (Hundley, 1999). Such a revolution is usually the result of a combination of changes in technology, weapons, structure, organization, and perceptions (Adamsky, 2012). The latest revolution is based to a large extent on precision information, of high quality and high resolution, that facilitates the activation of an "information-crush combination" (Rosen, 2019). There is no doubt that this in fact refers to operational and tactical intelligence, but with regard to strategic intelligence, it is relatively absent from the literature on the subject, possibly indicating that strategic intelligence has not yet adjusted to changes in security thinking and practice.

Apparently, CBW—given the high speed at which it is managed, the significant risks it involves, and its need to engage constantly with secrets, but also with puzzles and mysteries—creates a new challenge for strategic intelligence.

The Revolution in Intelligence Affairs and Strategic Intelligence

While tactical intelligence is undergoing a Revolution in Intelligence Affairs, mainly by exploiting new technologies, strategic

intelligence appears to have been left behind. Underlying the theory of the RIA is the idea that a radical change in intelligence is influenced by technologies—particularly those relating to artificial intelligence and data analysis; combat efforts—in the intelligence context this refers mainly to information systems that enable data mining and use of big data; structural and organizational issues—mainly regarding units that fuse various intelligence sensors, but also those that combine intelligence with operations and technology; and new perceptions—mainly those relating to the search for an alternative to the "intelligence cycle" as the organizing idea of the intelligence process, while creating new combinations of collection and research. In the professional literature, it is common to refer to several revolutions in intelligence affairs over the course of history (Lahneman, 2007; Denece, 2014; Barger, 2005), but it is clear that the main catalysts for the current revolution are big data and the information revolution. The most relevant type of intelligence for this type of revolution is operational and tactical.

While tactical intelligence is undergoing a Revolution in Intelligence Affairs, mainly by exploiting new technologies, strategic intelligence appears to have been left behind.

Col. Y. of IDF Intelligence describes (2018) the potential of the digital age. He looks mainly at intelligence that facilitates the struggle against suicide terrorists, in other words, operational and tactical intelligence. As background to this discussion, in the Israeli context, the focus on improvements in operational intelligence is due inter alia to the gaps identified during the Second Lebanon War in 2006 (Bar-Joseph, 2007), and it appears that this was also one of the considerations for setting up the Activation Unit in the Intelligence Directorate (Buhbut, 2016).

Another expression of the role of operational intelligence in military and intelligence revolutions can be found in the literature dealing with changes underway in military intelligence (Ferris, 2005). In 2004, the emergence of the RMA was descried as the result of how intelligence is incorporated into net-centric warfare (Ferris, 2004), and clearly these are the consequences of the information revolution. Another study (Evans, 2009) describes the changes that are needed in the "traditional" model of the intelligence process—the "intelligence cycle"; this study also focuses on military intelligence, and implicitly on operational and tactical intelligence.

However, the literature dealing with the link between the information revolution and big data on the one hand, and strategic intelligence on the other, is rather limited. In the United States it is already argued that the CIA units that dealt with strategic intelligence did not fully exploit the information revolution (Berkowitz, 2007). There are many references to an article dealing with the use of big data for strategic intelligence purposes (Lim, 2016) but this is apparently the exception that proves the rule.

Conclusions, Further Research, and Recommendations

This article presents various challenges facing strategic intelligence, and even if most are not new, it appears that taken together they become more intense. It describes the sociological aspect of the loss of trust by the public and its leaders in institutions, of which state intelligence is one; the philosophical aspect linked to the weakening of the ontological basis of objective truth and in particular the epistemological basis of its discovery by means of facts and empirical findings; aspects relating to the difficulty of intelligence to influence vision and ideology; the growing demand from commanders and political leaders for operational and tactical intelligence, rather than strategic intelligence; and the methodological aspect, linked to the limited adoption of innovative technologies by strategic intelligence and only partial implementation of the Revolution in Intelligence Affairs.

The article presents the hypothesis that strategic intelligence has difficulty in establishing its epistemological and methodological authority. It has not sufficiently adopted innovative technologies, and is largely based on intuitions and familiarity with the environment and past experience; Brun (2018) calls this the "educational school" of intelligence research. At a time when information science and advanced technologies have become an important condition for making decisions, strategic intelligence has difficulty persuading leaders of its unique added value and its ability to make full use of technologies for the purposes of strategic analysis.

In order to validate or refute the hypotheses raised by this article, it is necessary to develop an empirical base and conduct interviews with leaders and senior members of the intelligence community (an example of over sixty years ago is Hilsman, 1956) from the very contention that intelligence studies do not sufficiently use interviews (Van Puyvelde, 2018) or observations. Empirical information should above all provide an understanding of the way in which leaders perceive strategic intelligence and its added value, and of course an understanding of the latest challenges now facing the practice of strategic intelligence. In addition, the concept "strategic intelligence" is vague and demands interpretation, and it is therefore possible that a different approach could refute the thesis developed by this article.

In addition, it seems that the literature on the subject of strategic intelligence continues to engage in the traditional subjects—surprise, warning, relations with leaders, politicization, organizational issues, cognitive deflection, and so on (for example, Betts & Mahnken, 2003; Johnson, 2003; Phythian, Gill, & Marrin, 2008). Although recently attempts have been made to emphasize the impact of theories on intelligence practice (Gill & Phythian, 2018; Coulthart, 2019), there is still a gap in orderly writing about the effect of technology on the practice of strategic intelligence, or in other words, a gap in research that combines practical, up-to-date knowledge with broad theoretical observation.

Furthermore, there is no satisfactory research into alternative models for the intelligence cycle in the context of strategic intelligence. In Israeli Military Intelligence (AMAN), for example, 2019 marked the start of implementing the Fifth Dimension project that is generating changes in the process of creating intelligence (Fishman, 2019). It appears that this project is indeed challenging the intelligence cycle and creating unique combinations of research and data collection, while utilizing advanced technology, and it is therefore recommended to use this framework to develop a theory and updated models that will also be relevant for strategic intelligence.

The ticket that gives intelligence personnel entry to the halls of national security was and remains operational and tactical intelligence, but strategic intelligence must also shape its own "room for strategic discussion." In effect it must undergo its own Revolution of Intelligence Affairs.

In order to deal with the challenges described in this article, strategic intelligence must engage in reflection, define its methodology, establish critical thinking (Hendrickson, 2008), and nurture the foundations of the profession (Coulthart, 2016). In that way it will be possible to raise its credibility in the eyes of the political leadership (Gookins, 2008), through a combination of quantitative analysis and abstract, qualitative analysis, giving expression to wise and innovative use of technology, particularly with respect to information science. The ticket that gives intelligence personnel entry to the halls of national security was and remains operational and tactical intelligence, but strategic intelligence must also shape its own "room for strategic discussion." In effect it must undergo its own Revolution of Intelligence Affairs.

The phrase "methodological reflection" does not refer only to the implementation of basic research methods such as scenario analysis, war games, reverse filming, red teaming, and so on. Strategic intelligence must also examine how the utilization of big data can help to locate patterns and thereby identify anomalies (Kuosa, 2010); a striking example relates to macro-economic and global trends (and not only the economies of countries). It must develop an orderly methodology for strategic warnings of cyber attacks, not necessarily on the part of official state elements, and also warn of emerging trade wars, such as between China and the United States. It must establish an approach using integrative models on data collection for strategic matters. For example, changes in the concepts of force buildup and deployment have made the serial process of data collection guided by defined questions (known unknowns) irrelevant, because these are cases of emerging processes that may not be related to decisions by leaders on the other side. Strategic intelligence must "take ownership" of methods linked to horizon scanning in order to identify trends that could develop in the long term. One example is the need to identify emerging technologies in the field of artificial intelligence, which could have an impact not only on the operational environment, but also on strategic competition between countries (Allon, 2018; Hershkowitz, 2019).

Political leaders appear to consume raw information and develop independent access to the strategic environment, but in fact, quality strategic intelligence can frame the strategic discussion, indicate which information requires further investigation and which is not currently relevant, show the possible directions for development in the strategic environment if specific strategies are implemented, and give politicians suggestions for alternative strategies to the ones already chosen.

The thread that runs through all these recommendations is the belief that strategic intelligence should not be deterred from the adoption of innovative technologies, maximization of capabilities in information science and artificial intelligence, focus on technologies as the subject of research, and systematic work on methodology. It must not leave the field open only for operational and tactical intelligence. Apart from the new tasks indicated above, it must continue engaging with the traditional tasks of intelligence, such as warning of war threats, political upheavals affecting enemies (and friends), and so on. In these cases, too, intuition and deep familiarity with the strategic environment are essential, but not sufficient.

What prospect, therefore, does strategic intelligence have in the current era? Paradoxically, the complex, challenging environment of information overload and rapidly changing technology; leaders who undermine a basic element of the discipline and methodology of state intelligence in general, and strategic intelligence in particular; and the difficulty of clarifying events—all these factors increase its added value. Political leaders appear to consume raw information and develop independent access to the strategic environment, but in fact, quality strategic intelligence can frame the strategic discussion, indicate which information requires further investigation and which is not currently relevant, show the possible directions for development in the strategic environment if specific strategies are implemented, and give politicians suggestions for alternative strategies to the ones already chosen. Quality strategic intelligence is a holistic product (and process) that constantly moves inwards and outwards, between details and the whole picture, and also between disciplines and different research issues. Today's complex environment demands such a holistic view. Relevant strategic intelligence is both artistic and scientific (Shapira, 2020)—like strategy itself (Brodie, 1998). True, these were its essence

in the past, but the sheer volume of today's challenges and information reinforce its ability to provide unique added value.

It is certainly difficult to measure the success of intelligence in general and strategic intelligence in particular (Moore, Krizan, & Moore, 2005), and thus a retrospective examination of the value of assessments is unsatisfactory. The true test of strategic intelligence is to a large extent its ability to influence the direction, planning, and implementation of strategy, and by implication, to shape the environment. It must do this by means of professional analysis, which, even if it does not claim absolute objectivity, must be based on facts, as well as on in-depth interpretation and the use of relevant conceptual frameworks. This is what creates the "strategic lenses" that lead to an understanding of a complex and dynamic environment in a way that also facilitates shaping it. Strategic intelligence is now needed more than ever: this could be its darkest hour, but also its finest hour.

*

The author wishes to thank Brig. Gen. (ret.) Itai Brun, formerly head of the IDF Intelligence Research Division and currently Deputy Director for Research and Analysis at the Institute for National Security Studies (INSS); Brig. Gen. Dror Shalom, head of the Research and Analysis Division of the Israeli Military Intelligence; the editors of *Strategic Assessment*; and the two anonymous reviewers for their professional and constructive comments.

The views expressed in the article are solely those of the author, and not of the IDF or Israeli Military Intelligence.

Col. (res.) Itai Shapira has over 25 years of experience of intelligence research in IDF Intelligence Division at the tactical, operational, and strategic levels. He is a graduate of the College of National Security, and holds a B.A. in Economics and Philosophy, and an M.B.A. from Tel Aviv University.

Sources

A. A. (2016). How intelligence deals with complex issues between arenas: The organizational aspect. *Intelligence—from theory to practice: Combinations in Intelligence* 1, 25-44. Institute for the Research of the Methodology of Intelligence at the Israeli Intelligence Heritage and Commemoration Center [in Hebrew].

Adamsky, D. (2012). *The impact of the strategic culture on the Revolution in Military Affairs in Russia, the United States and Israel.* Ben Shemen: Modan and Tel Aviv: *Maarachot* [in Hebrew].

Aldrich, R. J., & Kasuku, J. (2012). Escaping from American intelligence: Culture, ethnocentrism and the Anglosphere. *International Affairs, 88*(5), 1009-1028.

Alon, N. (2018). Horizon scanning: A process that assists decision making processes at national level—in depth study. Institute for the Research of the Methodology of Intelligence at the Israeli Intelligence Heritage and Commemoration Center. https://www.terrorism-info.org.il/app/uploads/2018/07/189_18_H.pdf [in Hebrew].

Alon, N., & Freizler-Swiri, D. (2019). "A marathon race and jamming sticks into the enemy's wheels": The campaign between wars (CBW) in the IDF. *Between the Extremes: Contemporary issues in the art of the campaign. On the way to digital transformation, 22*, 13-32. Ops Div.—Theory & Training, Dado Center for Interdisciplinary Thinking, Ministry of Defense — Publications [in Hebrew].

Azoulay, M. (2018, September 27). Netanyahu's full speech: The revelations, the accusations, and the hopes. *Ynet.* https://www.ynet.co.il/articles/0,7340,L-5359524,00.html [in Hebrew].

Barger, D. G. (2005). *Toward a revolution in intelligence affairs.* Santa Monica, CA: RAND Corporation. https://www.rand.org/content/dam/rand/pubs/technical_reports/2005/RAND_TR242.pdf

Bar-Joseph, U. (1998). A bull in a china shop: Netanyahu and Israel's intelligence community. *International Journal of Intelligence and Counterintelligence, 11*(2), 154-174.

Bar-Joseph, U. (2007). Israel's military intelligence performance in the Second Lebanon War. *International Journal of Intelligence and Counterintelligence, 20*(4), 583-601.

Bar-Joseph, U. (2013). Non-activation of "special collection means" and the intelligence failure in the Yom Kippur War. *Maarachot*, *448*, 46-53 [in Hebrew].

Barnea, A. (2019). Is it possible to break the glass ceiling of the strategic intelligence discipline? *Between the Extremes: Contemporary issues in the art of the campaign. On the way to digital transformation, 20-21,* 145-164,. Ops Div.—Theory & Training, Dado Center for Interdisciplinary Thinking, Ministry of Defense —Publications [in Hebrew].

Barnea, A. (2019). Big data and counterintelligence in Western countries. *International Journal of Intelligence and Counterintelligence, 32*(3), 433-447.

Ben-Israel, I. (1999). *The philosophy of intelligence.* Tel Aviv: Ministry of Defense [in Hebrew].

Ben-Porat, Y. (1984). Problems in intelligence assessments. *Maarachot, 296*, 19-24 [in Hebrew].

Berkowitz, B. (2007). Failing to keep up with the information revolution: The DI and "IT." *Studies in Intelligence, 47*(1), 67-74. https://bit.ly/30XCVmy

Betts, R. K., & Mahnken, T. G. (Ed.). (2003). *Paradoxes of strategic intelligence: Essays in honor of Michael I. Handel.* London: Frank Cass.

Bradner, E. (2017, January 23). Conway: Trump White House offered "alternative facts" on crowd size. *CNN*. https://edition.cnn.com/2017/01/22/politics/kellyanne-conway-alternative-facts/index.html

Brahms, Y. (2019). Philosophy of post-truth. Institute for National Security Studies. https://www.inss.org.il/wp-content/uploads/2019/09/Philosophy-of-Post-Truth.pdf

Brantly, A. F. (2014). Cyber actions by state actors: Motivation and utility. *International Journal of Intelligence and Counterintelligence, 27*(3), 465-484.

Brantly, A. F. (2018). When everything becomes intelligence: Machine learning and the connected world. *Intelligence and National Security*, *33*(4), 562-573.

Brodie, B. (1998). Strategy as an art and a science. *Naval War College Review, 51*(1), 26-38.

Brun, I. (2015). *Intelligence research: Investigating reality in an era of changes.* Institute for the Research of the Methodology of Intelligence at the Israeli Intelligence Heritage and Commemoration Center [in Hebrew].

Brun, I. (2018). Approaches to intelligence studies and big data in the "post truth" era. *Intelligence—From theory to practice: Big data and intelligence,* 3, 129-136. Institute for the Research of the Methodology of Intelligence at the Israeli Intelligence Heritage and Commemoration Center [in Hebrew].

Brun, I., & Roitman, M. (2019). National security in the era of post-truth and fake news. Institute for National Security Studies. https://bit.ly/2U6TxXA

Buhbut, A. (2016, April 22). The "godfather" of AMAN: The man in the shadows who decides when to bomb Nasrallah's bunker. *Walla! News*. https://news.walla.co.il/item/2955359 [in Hebrew].

Cassidy, J. (2018, October 16). Donald Trump, Jamal Khashoogi and the post-truth world. *The New Yorker*. https://bit.ly/2GtE5Ng

Cavelty, M. D., & Mauer, V. (2009). Postmodern intelligence: Strategic warning in an age of reflexive intelligence. *Security Dialogue, 40*(2), 123-144.

Central Intelligence Agency. (2019). *CIA Director Gina Haspel speaks at Auburn University*. https://bit.ly/36xcNjL

Central Intelligence Agency. *National Intelligence Estimates*. https://bit.ly/37xG2UL

Coats, Daniel R. (2019). *Worldwide threat assessment of the US intelligence community.* https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

Col. Y. (2018). The journey to investigate the perception and implementation of intelligence and operational superiority in the digital age. *Intelligence—From theory to practice: Big data and intelligence*, 3, 12-23. Institute for the Research of the Methodology of Intelligence at the Israeli Intelligence Heritage and Commemoration Center [in Hebrew].

Coulthart, S. (2016). Why do analysts use structured analytical techniques? An in-depth study of an American intelligence agency. *Intelligence and National Security, 31*(7), 933-948.

Coulthart, S. (2019). From laboratory to the WMD Commission: How academic research influences intelligence agencies. *Intelligence and National Security, 34*(6), 818-832.

Cradock, P. (2002). *Know your enemy: How the Joint Intelligence Committee saw the world.* London: John Murray.

Crosston, M. (2016). Bringing non-Western cultures and conditions into comparative intelligence perspectives: India, Russia and China. *International Journal of Intelligence and Counterintelligence, 29*(1), 110-131.

Dado Center. (2016). *Introduction to "Operational Art,"* Ops Div.—Theory & Training, Dado Center for Interdisciplinary Thinking, p. 10. https://bit.ly/2RORqoA https://bit.ly/2sxuOQF

Defense Intelligence Agency. (2017). *Russia military power: Building a military to support great power aspirations.* Washington, DC. https://bit.ly/2RsYpEX

Defense Intelligence Agency. (2019). *China military power: Modernizing a force to fight and win.* Washington, DC. https://bit.ly/30Yllil

Denece, E. (2014). The revolution in intelligence affairs: 1989-2003. *International Journal of Intelligence and Counterintelligence, 27*(1), 27-41.

Dudley, C. A. (2018). Information-centric intelligence: The struggle in defining national security issues. *International Journal of Intelligence and Counterintelligence, 31*(4), 758-768.

Evans, G. (2009). Rethinking military intelligence failure—Putting the wheels back on the intelligence cycle. *Defence Studies, 9*(1), 22-46.

Even, S. (2019). The campaign against Iran in Syria: Are Israel's statements helpful? *INSS Insight, 1134.* https://www.inss.org.il/wp-content/uploads/2019/02/No.-1134.pdf

Ferris, J. (2004). Netcentric warfare, C4ISR and information operations: Towards a revolution in military intelligence? *Intelligence and National Security, 19*(2), 199-225.

Ferris, J. R. (2005). *Intelligence and strategy: Selected essays.* London: Routledge. pp. 288-327.

Fishman, A. (2019, April 24). The combined brains. *Yediot Ahronot: Saturday supplement.* https://www.yediot.co.il/articles/0,7340,L-5499267,00.html [in Hebrew].

Freedman, L. (1997). The CIA and the Soviet threat: The politicization of estimates, 1966-1977. *Intelligence and National Security*, *12*(1), 122-142.

Freedman, L. (2004). War in Iraq: Selling the threat. *Survival, 46*(2), 7-49.

Freedman, L. (2006). A transformation in strategic affairs: Introduction. *The Adelphi Papers, 45*(379), 5-10.

Gazit, S. (2003). *Between warning and surprise: On shaping national intelligence assessment in Israel*. Tel Aviv: Tel Aviv University, Jaffee Center for Strategic Studies [in Hebrew]

Gazit, S. (2004). Intelligence estimates and the decision maker. In L. K. Johnson & J. J. Wirtz (Eds.), *Strategic intelligence: Windows into a secret world* (pp. 127-142). Los Angeles, CA: Roxbury Publishing Company.

Gentry, J. A. (2017). Intelligence services and special operations forces: Why relationships differ. *International Journal of Intelligence and Counterintelligence, 30*(4), 647-686.

Gentry J. A. (2018). A new form of politicization? Has the CIA become institutionally biased or politicized? *International Journal of Intelligence and Counterintelligence, 31*(4), 647-680.

Gertz, G. (2018). U.S. intelligence institutionally politicized toward Democrats. *The Washington Free Beacon.* https://bit.ly/2O4GWjU

Gibson, S. D. (2009). Future roles of the UK intelligence system. *Review of International Studies, 35*, 917-928.

Gill, P., & Phythian, M. (2018). Developing intelligence theory. *Intelligence and National Security, 33*(4), 467-471.

Gookins, Amanda J. (2008). The role of intelligence in policy making. *SAIS Review of International Affairs, 28*(1), 65-73.

Granit, E. (2006). *The development of the idea of intelligence in the American space* (Doctoral thesis, School of Humanities, Faculty of Humanities, Tel Aviv University) [in Hebrew].

Hai, S. (2018, April 30). Netanyahu presents secret Iranian nuclear files: "Proof of the lies." *Ynet.* https://www.ynet.co.il/articles/0,7340,L-5246747,00.html

Handel, M. I. (Ed.). (1989). *Leaders and intelligence*. London: Frank Cass.

Hastedt, G. (2005). Public intelligence: Leaks as policy instruments—The case of the Iraq war. *Intelligence and National Security*, *20*(3), 419-439.

Hastedt, G. (2013). The politics of intelligence and the politicization of intelligence: The American experience. *Intelligence and National Security, 28*(1), 5-31.

Hayden, M. (2017). *The role of intelligence in a post truth world*. Nobel Week Dialogue. https://www.youtube.com/watch?v=mOh85VHT_L8

Heinderich, J. G. (2007). The state of strategic intelligence: The intelligence community's neglect of strategic intelligence. *Studies in Intelligence, 51*(2). https://bit.ly/2U0rrgF

Hendrickson, N. (2008). Critical thinking in intelligence analysis. *International Journal of Intelligence and Counterintelligence, 21*(4), 679-693.

Hennigan, W. J. (2018, January 19). President Trump's new defense strategy is a return to the Cold War. *Time.* http://time.com/5109551/donald-trump-military-defense-strategy/

Herman M. (2003a). Counter-terrorism, information technology and intelligence change. *Intelligence and National Security, 18*(4), 40-58.

Herman, M. (2003b). Threat assessment and the legitimation of policy? *Intelligence and National Security, 18*(3), 174-178.

Hershkovitz, S. (2017). A three-story building: A critical analysis of Israeli early warning discourse. *International Journal of Intelligence and Counterintelligence, 30*(4), 765-784.

Hershkowitz, S. (2019). *The God in the machine: Emerging technologies and the future of intelligence—In-depth research*. Institute for the Research of the Methodology of Intelligence at the Israeli Intelligence Heritage and Commemoration Center. https://bit.ly/2PSWJCJ [in Hebrew].

Hilsman, R. (1956). *Strategic intelligence and national decisions*. USA: The Free Press.

Hundley, R. O. (1999). *Past revolutions, future transformations: What can the history of revolution in military affairs tell us about transforming the U.S military?* Santa Monica, CA: RAND Corporation.

Hulnick, A. S. (1999). *Fixing the spy machine: Preparing American intelligence for the twenty-first century.* Westport, CT: Praeger Publishers.

Hulnick, A. S. (2006). What's wrong with the intelligence cycle. *Intelligence and National Security, 21*(6), 959-979.

IDF. (2018). *IDF Strategy*. https://www.idf.il/media/34416/strategy.pdf [in Hebrew].

Immerman, R. H. (2008). Intelligence and strategy: Historicizing psychology, policy and politics. *Diplomatic History, 32*(1), 1-23.

Johnson, L. K. (2003). Preface to a theory of strategic intelligence. *International Journal of Intelligence and Counterintelligence, 16*(4), 638-663.

Joint Chiefs of Staff. (2015). *The National Military Strategy of the United States of America*. Washington, DC. https://bit.ly/2tMFiwI.

Kabir, E. (2019, May 16). Cracking the method of sending money to terror organizations in Gaza has created a new profession in IDF Intelligence. *Calcalist.* https://www.calcalist.co.il/internet/articles/0,7340,L-3762214,00.html [in Hebrew].

Kavanagh, J., & Rich, M. D. (2018). *Truth decay: An initial exploration of the diminishing role of facts and analysis in American public life.* Santa Monica, CA: RAND Corporation.

Kazimirsky, A., Grossman-Aloni, N., & Sari, A. (Eds). (2004). *Intelligence and the leader*. Tel Aviv: Ministry of Defense—Publications [in Hebrew].

Kent, S. (1949). *Strategic intelligence for American world policy*. Princeton, NJ: Princeton University Press.

Kochavi, A., & Ortal, E. (2014). "AMAN event"—A permanent change in a changing reality. *Between the Extremes: Contemporary issues in the art of the campaign,*

2. Ops Div.—Theory & Training, Dado Center for Interdisciplinary Thinking, Ministry of Defense — Publications [in Hebrew].

Kovacs, A. (1997). Using intelligence. *Intelligence and National Security, 12*(4), 145-164.

Kuosa, T. (2010). Different approaches of pattern management and strategic intelligence. *Technological Forecasting & Social Change, 78*(3), 458-467.

Kuperwasser, Y. (2007). *Lessons from Israel's intelligence reforms*. Washington, DC: The Saban Center for Middle East Policy at the Brookings Institution. https://brook.gs/2GzUgsl

Lahneman, W. J. (2007). Is a revolution in intelligence affairs occurring? *International Journal of Intelligence and Counterintelligence, 20*(1), 1-17.

Lim, K. (2016). Big data and strategic intelligence. *Intelligence and national security, 31*(4), 619-635.

Manjikian, M. (2013). Positivism, post-positivism and intelligence analysis. *International Journal of Intelligence and Counterintelligence, 26*(3), 563-582.

Marrin, S. (2013). Evaluating CIA's analytical performance: Reflections of a former analyst. *Orbis, 57*(2), 325-339.

Marrin, S. (2017). Why strategic intelligence analysis has limited influence on American foreign policy. *Intelligence and National Security. 32*(6), 725-742.

Marrin, S. (2020). Analytical objectivity and science: Evaluating the US intelligence community's approach to applied epistemology. *Intelligence and National Security.* doi: 10.1080/02684527.2019.1710806

Marshall, A. W. (1972). *Long-term competition with the Soviets: A framework for strategic analysis.* Santa Monica: RAND Corporation. https://www.rand.org/pubs/reports/R862.html

Mattern, T. et al. (2014). Operational levels of cyber intelligence. *International Journal of Intelligence and Counterintelligence, 27*(4), 702-719.

Matza, D. (2017). The four paths in the strategic intelligence "orchard." *Intelligence—From theory to practice: Combinations in intelligence* 2, 105-121. Institute for the Research of the Methodology of Intelligence at the Israeli Intelligence Heritage and Commemoration Center [in Hebrew].

Mejas, U. A., & Vokuev, N. E. (2017). Disinformation and the media: The case of Russia and Ukraine. *Media, Culture & Society, 39*(7), 1027-1042.

Michlin-Shapir, V., & Padan, C. (2019). Dangers, risks, and "unknown unknowns": National security in the global era. In V. Michlin-Shapir & C. Padan (Eds.). *National security in a "liquid" world* (pp. 13-29). Tel Aviv: Institute for National Security Studies.

Ministry of Defence (2018). *Global strategic trends: The future starts today*. London. https://bit.ly/2O2iWy8

Mizrachi, O. (2019). Operation Northern Shield: Interim assessment. *INSS Insight 1127*. https://www.inss.org.il/wp-content/uploads/2019/01/No.-1127.pdf

Moore, D. T., Krizan, L., & Moore, E. J. (2005). Evaluating intelligence: A competency-based model. *International Journal of Intelligence and Counterintelligence, 18*(2), 204-220.

Morrell, M. (2018). *Director of National Intelligence. Dan Coats speaks truth to power.* Washington, DC: Atlantic Council. https://bit.ly/2t3lLrf

Office of the Director of National Intelligence. (2019). *National Intelligence Strategy of the United States of America*. https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf

Oprysko, C. (2019, January 30). Trump tells intel chiefs to "go back to school" after they break with him. *Politico*. https://www.politico.com/story/2019/01/30/trump-national-security-1136433

Palacios, J. M (2018). The role of strategic intelligence in the post-everything age. *The International Journal of Intelligence, Security and Public Affairs*, *20*(3), 181-203.

Phythian, M., Gill, P., & Marrin, S. (2008). *Intelligence theory: Key questions and debates*. New York: Routledge.

Rathmell, A. (2002). Towards postmodern intelligence. *Intelligence and National Security*, *17*(3), 87-104.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1-2), 4-37.

Rosen, S. (2019). Military innovation and radiating strength. *Between the Extremes: Contemporary issues in the art of the campaign. On the way to military transformation, 20-21, 22*, 33-45. Ops Div.—Theory & Training, Dado Center for Interdisciplinary Thinking, Ministry of Defense—Publications [in Hebrew].

Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and Counterintelligence, 26*(3), 453-481.

Sciutto, J., & Cohen, M. (2019). Trump skeptical of using foreign spies to collect intel on hostile countries, sources say. *CNN Politics*. https://cnn.it/2vsPb2Z

Shapira, I. (2018). What can security strategy learn from business strategy? *Maarachot, 480-481*, 58-62 [in Hebrew]

Shapira, I. (2020). Strategic intelligence as an art and a science: Creating and using conceptual frameworks. *Intelligence and National Security, 35*(2), 283-299.

Sharma, A. (2010). Cyber wars: A paradigm shift from means to ends. *Strategic Analysis, 34*(1), 62-73.

Shpiro, S. (2012). Israeli intelligence and al-Qaeda. *International Journal of Intelligence and Counterintelligence, 25*(2), 240-259.

Siman-Tov, D., & Alon, N. (2018). The cybersphere obligates and facilitates a revolution in intelligence affairs. *Cyber, Intelligence, and Security 2*(1), 73-92.

Steinhart, A., & Avramov, K. (2013). Is everything personal?: Political leaders and intelligence organizations: A typology. *International Journal of Intelligence and Counterintelligence. 26*(3), 530-549.

Teitelbaum, L. (2005). *The impact of the information revolution on policymakers' use of intelligence analysis.* Santa Monica, CA: RAND Corporation. https://www.rand.org/content/dam/rand/pubs/rgs_dissertations/2005/RAND_RGSD186.pdf

The Pentagon. (2018). *Summary of the national defense strategy of the United States of America*. Washington, DC. https://bit.ly/2tXwXGf

The White House (2017). *National Security Strategy of the United States of America*. Washington, DC. https://bit.ly/2Rxl5DR

Treverton, G. F. (2004). *Reshaping national intelligence for an age of information*. Cambridge, UK: Cambridge University Press.

Van Puyvelde, D. (2018). Qualitative research interviews and the study of national security intelligence. *International Studies Perspectives, 19*, 375-391.

Warner, M. (2014). *The Rise and fall of intelligence: An international security history*. Washington DC: Georgetown University Press.

Wasserman, B. (1960). The failure of intelligence prediction. *Political Studies, 8*(2), 156-169.

Waxman, M. C. (1998). Emerging intelligence challenges. *International Journal of Intelligence and Counterintelligence, 10*(3), 317-331.

Weinbaum, C., & Shanahan, J. N. T. (2018). Intelligence in a data-driven age. *Joint Forces Quarterly, 90*(3rd quarter). Washington DC: National Defense University, p. 6. https://bit.ly/2Rylc2g

Williams, H. J., & Blum, I. (2018). *Defining second generation open source intelligence (OSINT) for the defense enterprise*. Santa Monica, CA: RAND Corporation. https://bit.ly/37BdERY

Winston, T. (2007). Intelligence challenges in tracking terrorist internet fund transfer activities. *International Journal of Intelligence and Counterintelligence, 20*(2), 327-343.

Wirtz, J. J. (2018). The cyber Pearl Harbor redux: Helpful analogy or cyber hype? *Intelligence and National Security, 33*(5), 771-773.

Wolfberg, A. (2017). When generals consume intelligence: The problems that arise and how they solve them. *Intelligence and National Security, 32*(4), 460-478.

Zeitoun, Y. (2018, October 22). A km from the northern border: IDF exposes the sixth Hezbollah observation post. *Ynet*. https://www.ynet.co.il/articles/0,7340,L-5377114,00.html [in Hebrew].

Zeitoun, Y. & Porat, S. (2019, January 13). Netanyahu in an unusual declaration: We have attacked Iranian weapon stores in Damascus. *Ynet*. https://www.ynet.co.il/articles/0,7340,L-5445807,00.html [in Hebrew]

Zelizer, J. E. (2018). How Trump channels the 1970s. *The Atlantic*. https://bit.ly/2U1SPen.

Notes

1 There is an ontological debate about "strategic reality," and an epistemological question regarding intelligence's capability to clarify it, but this is beyond the scope of this article.