Technology and Intelligence: Changing Trends in the IDF's Intelligence Process in the Post-Information Revolution Period

Jasmin Podmazo

This article addresses the changes that have occurred in the intelligence work of the Israel Defense Forces (IDF) in the period following the information revolution of the 1990s, and it examines how technological developments during this period have improved the intelligence process and how they have affected intelligence surprises. The article describes the effect of technological developments on each stage of the classic "intelligence cycle"—collection, processing, analysis, and dissemination. It also provides a comparative analysis of the processes before and after the information revolution, based on open sources. The technological changes have resulted in three main trends: 1) way in which classic intelligence work is done is changing; 2) the access of operational units to intelligence has improved; and 3) the room for intelligence surprises has become increasingly narrow.

Keywords: Intelligence cycle, technology, information revolution, collection accessibility, jointness

Introduction

The information revolution, which began in the 1990s, is the most significant transformation since the industrial revolution of the nineteenth century. Like

Jasmin Podmazo is a master's degree student in the Security Studies Program at Tel Aviv University.

the latter, it had a profound effect on the economy, politics, and technology. The main feature of the information revolution is broad access to knowledge and rapid connectivity that enables the global transfer of information in the shortest amount of time. This is accomplished through an evolutionary process of change and innovation, mainly in the technological sphere. During the information revolution, the information technologies (IT) came of age and formed the basis of the technological developments of this century. It is hard to distinguish between the end of the information revolution and the period that followed, which constitutes a further evolution of technology and information. This article will focus on the first two decades of the twenty-first century, which will be referred to as "the period following the information revolution of the 1990s."[1]

Today, in an era of information overload and of dynamic and changing arenas, intelligence work done in Israel and abroad faces new, extremely complex challenges. Technological innovation and wise and informed management of the voluminous information available are critical for building the best intelligence picture, which ultimately affects our ability to deal with various adversaries and our deterrent capability concerning unusual events.

The classic function of intelligence is, first and foremost, to clarify the existing situation behind enemy lines. Therefore, high-quality and precise intelligence is tremendously important for dealing with any type of surprise both in times of routine and emergencies. The prevailing view is that high-quality intelligence is a critical source of power in the battlefield (before and during war). Modern technology, which creates advanced information collection and processing capabilities, has enabled us to learn about the enemy and reduce our uncertainty about it. Military supremacy is, to a large extent, gained due to high-quality and precise intelligence about the other side. Intelligence makes it easier to gain control of the field and to prevent the enemy's actions in advance. The more precise the intelligence is, the more focused the operations against the enemy it will enable while reducing peripheral damage. In addition, political and military decision makers rely

1 It is common to attribute the information revolution to the period spanning the end of the 1990s and the beginning of the 2000s, with the technologies developed then influencing the processes taking place around the world today. However, there are those who argue that we are now in a different period, possibly even the next revolution, which features the increased use of cyber and unmanned tools in the field of combat. From an historical perspective, the current decade may be only a stage in the revolution that will remain with us in the coming years as well.

on intelligence as it allows for better control over events both before they happen and as they are taking place. We must remember, however, that the intelligence process is always exposed to potential failures, particularly cognitive ones, which are an inseparable part of the thought and decision-making processes in conditions of uncertainty.

The information revolution of the 1990s and the technological developments in the world of intelligence in the period thereafter significantly improved the ability of intelligence agencies to provide responses to research questions and to build a reliable and optimal picture of the enemy. One of the challenges facing intelligence research today is how to maximize the information and develop technological tools for dealing with it. The information revolution has also significantly affected the other side: The adversary is not resting on its laurels and is constantly working to gather information on the other side and develop tomorrow's tools of combat. Moreover, the enemy is learning about the capabilities of the other side and changing its own behavior accordingly, making it more difficult for the other side to gather intelligence about it.

This article seeks to understand how technological developments in the field of intelligence in the period following the information revolution of the 1990s have improved the intelligence process, including the handling of surprises. The article will examine the changes that have taken place in the wake of the information revolution and the cornerstones that have formed the basis of intelligence work: collection, processing, analysis, and dissemination. Specifically, the article will focus on changes that have taken place in the IDF's intelligence branch in the past two decades. Although the focus here is on the changes that have occurred in each stage of the Israeli intelligence cycle, similar processes taking place elsewhere should not be ignored. The IDF is a single test case within a much broader context of technological change in military intelligence processes in the United States, Britain, China, and elsewhere since the 2000s.[2]

The discussion of each cornerstone will include examples of the effects of technological developments on the ability of the intelligence agencies to build a full and reliable picture that enables warnings and identification of potential surprises. The article will analyze a number of test cases and will

2 About the effect of technological developments on the various intelligence stages within the US intelligence community, see Margaret E. Kosal, ed., *Technology and the Intelligence Community: Challenges and Advances for the 21st Century* (Springer, 2018).

argue that the technological developments have a positive impact on how intelligence work is conducted. At the same time, the age of information overload presents challenges in separating the grain from the chaff and sometimes requires organizational adjustments and changes in order to provide the full intelligence response. Moreover, dealing with an adversary that learns and continues to constantly improve also requires proper adaptations.

On Intelligence Work in the Post-Information Revolution Era

Technological capabilities in the field of information have grown and strengthened since the early 2000s until now following the information revolution. The flood of information, accessibility, and rapid global connectivity have created new challenges. Within this framework, we can identify two main trends that are mutually dependent. The first trend relates to the change in how technology for creating information is used, and as a result, the exponential increase in the quantity of available information. The second one relates to technological developments in the field of information analysis, resulting from the need to analyze and process large quantities of information in short periods of time.[3]

One of the more significant and influential developments in the field of information processing is the Big Data revolution. The world of big data developed as a result of a number of parallel technological developments: 1) improved ability to gather large quantities of information with a wide variety of sensors, which led to increased data storage capacity; 2) immense growth in the quantity of information throughout the world, due to the increasing use of technologies that leave a digital signature; and 3) improved computational ability, enabling rapid and parallel processing and analysis of large quantities of information.[4]

According to the classic approach, there are a number of stages in the intelligence process known as the "intelligence cycle": information collection, processing of the material collected, analysis of the materials, and dissemination of the intelligence product to its consumers. The stages

3 Lt. Col. T., "Intelligence Derivatives of the World of Big Data," in *Intelligence in Theory and in Practice*, no. 3 (May 2018): 24–32 [in Hebrew].

4 M., deputy principal of the Israel Security Agency's school of intelligence, "Angels in the Skies of Berlin": New Intelligence Questions in a World Steeped in Data," in *Intelligence in Theory and in Practice,* no. 3 (May 2018): 55–60 [in Hebrew].

repeat themselves in a circular fashion (see figure 1 below) and are directed by the essential elements of information (EEI) sought, in other words, by the research questions that must be answered. The process begins with analysts sending questions regarding EEI to information collection personnel, and then those personnel continue the process by working to bring in the required information. In the next stage, the raw material is processed, and it is then disseminated to its consumers.

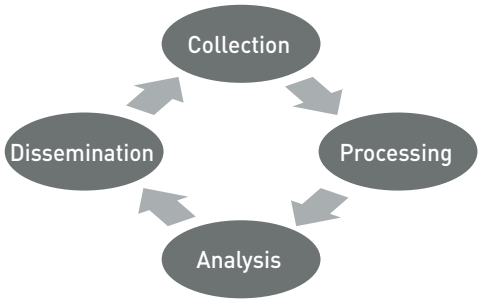

Figure 1. The intelligence cycle

When we examine the information revolution's effect on the classic intelligence cycle, we can see changes in each stage of intelligence. The clear trend in **intelligence collection** is the growth and improvement of cyber capabilities, which is the newest dimension of warfare. In the digital age, many types of information can be converted into bytes, which are connected to various information networks. In this kind of world, where everything is connected on the network, the basic assumptions of intelligence work in the fields of information and knowledge change. The quantity of information that is currently available to intelligence personnel creates a new challenge in terms of utilizing it: filtering out the information that is relevant to the research questions. Moreover, in the digital age, intelligence personnel potentially have accessibility to collect information and must have new skills to mine it.

Intelligence agencies today are flooded with information from the various sensors deployed in areas of interest and from access to databases in cyberspace that are constantly being filled and renewed. In places where access to information is complex due to security and encryption parameters, the job of the intelligence personnel is to develop cyber tools to exploit security breaches and weakness on the other side. The main challenge,

however, is the storing of large volumes of information, which involves considerable costs. Therefore, Israel's Military Intelligence Directorate has decided, for example, to not allow certain intelligence materials into their databases—despite the resources invested and risks taken to obtain those materials—and also to limit the duration for which materials are to be kept. This method poses challenges for researchers, since it limits their ability to ask intelligence questions based on learning processes over time.[5]

Intelligence collection also has developed in the field of satellites. Satellite capabilities make it possible to obtain pictures from all over the world through advanced optical systems, aiding intelligence research of distant sites of interest. Technological developments in the field of photography and optics have resulted in high-quality products with high resolutions and are used in deciphering during site analysis.

In the field of satellite-based visual intelligence collection, the information revolution enabled the transition from the analog era to the digital age. The analog era was characterized by a lack of raw material (imaging)[6] and long manual processing, while the digital age has enabled a quicker processing time and a better quality of the raw material. Today, a wealth of satellite imagery is available at resolutions that are constantly improving, at various wavelengths (multispectral and radar), and covering vast areas.[7] Multispectral satellites, for instance, help provide a response to complex EEIs, helping to study the adversary who tries to maintain a low signature profile and in complicated areas, either densely urban or covered with vegetation. For example, imagery of various wavelengths makes it possible to identify a depot of metals camouflaged by vegetation and to find hidden launch sites in a forested area. Another type of satellite used in intelligence is the Synthetic Aperture Radar (SAR) satellite, based on controlled transmission of electromagnetic radiation. The main advantage of these radars is the ability

5 Lt. Col. T., "Intelligence Derivatives of the World of Big Data," 27–28.

6 Imaging is a visual presentation of a picture, obtained through various methods, tools, and types of measurement that are not necessarily optical; that is, they are not necessarily based on visible light.

7 Lt. Col. A., "Geographic Intelligence – From Paper Napkin to 'Geo-Network'" in *The Challenges of the Israeli Intelligence Community*, ed. Shmuel Even and David Siman Tov (Tel Aviv: INSS, 2018), p. 99 [in Hebrew].

to generate images of a given area at any time and under any weather and visibility conditions.[8]

In recent years, space has become increasingly filled with satellites, with the number today almost two-and-a-half times greater than it was two decades ago.[9] The information collected by the satellites reaches intelligence agencies in accordance with EEIs. Geographical applications make the information directly accessible to intelligence researchers, who can use the material themselves without the involvement of professional deciphering agencies. This is an additional element that underlines the need for jointness between intelligence agencies (see below).

The use of unmanned aerial vehicles (UAVs) is another element in visual intelligence collection. The past decade has witnessed an upward trend in the use of various types of UAVs to help field echelon units in their tasks. For example, UAVs outfitted with high-quality sensors that are able to remain in the air for prolonged periods help connect the real-time situational picture in the field to both intelligence personnel working to identify the targets and force operators seeking to close in on the targets as quickly as possible. In addition, using small UAVs and drones for tactical intelligence collection and for helping field forces during combat has increased. The access to advanced technologies and low production costs have facilitated the widespread production of various types of UAV, including commercial drones. As a result, they have become accessible for many countries and even non-state military actors.[10]

From the **intelligence analysis** point of view, cyber, to some extent, has created a joint intelligence space in which collection and research personnel share skills. Technological developments in the Military Intelligence Directorate in recent years have created "the intelligence officer's new work table," including applications for networked intelligence spaces. One example is the "Tracebook" system, to which collection personnel, engaging in preliminary processing, upload raw excerpts of intelligence before Unit

8 Ami Rojkes Dombe, "Seeing Everything, From Everywhere, Any Time," *IsraelDefense*, November 29, 2014, https://www.israeldefense.co.il/he/content-מקום-כל-מכל-הכל-לראות/זמן-כל-בכל [in Hebrew].

9 Herzi Halevi, "Military Intelligence 2048 – Intelligence Supremacy in the Digital Age," *Ma'arachot*, no. 477 (2018): 28–29 [in Hebrew].

10 Liran Antebi, "The Watchful Eye in the Sky – Advantages and Challenges in the Use of UAVs for Intelligence Collection," in *Challenges of the Israeli Intelligence Community*, pp. 113–120 [in Hebrew].

8200 (the main collection unit of the IDF's Intelligence Corp) fully processes them in accordance to its standard.[11]

Other technological developments for dealing with vast amounts of data, such as automatic photo identification technologies or speech-to-text (STT) technologies, are also be employed by intelligence agencies. Currently, technologies in the civilian sector can convert sound files to text files based on natural language understanding models. Companies such as Google, IBM, and even the Israeli Verbit company have developed transcription engines that make it possible to save many hours of work transcribing recorded discussions.[12] The use of STT technologies by intelligence agencies may lead to a revolution in the volume of sound that is translated in a given time period and could create warning mechanisms based on queries defined in advance according to the relevant EEI.

The world of visual intelligence has developed additional methods of information processing methods. The transition from the analog era to the digital age shortened the amount of time it takes to produce intelligence, enabled the fusion of information from various intelligence disciplines, and has led to applications that visually present geographic layers of information. These capabilities made it possible, for example, to combine information from optical and radar imagery together with other layers of information of infrastructure in the field. The result has been a marked improvement in being able to complete the circle from the collection stage to the real-time attack stage and the process of producing targets in general.[13]

In terms of imagery information processing, computerized imagery and machine learning have made it possible to identify objects, discern changes in territory, and discover patterns of phenomena. The use of algorithms to compare pictures and automatically identify changes in infrastructure and land cover, applied to large quantities of images, could save intelligence agencies many hours of deciphering and could help analyze a tremendous amount of material in the shortest possible time. In the future, algorithms may be able to provide warnings of visual intelligence incidents.

---

11 Or Glick, "The Walls Were Not Broken – The Story of Tracebook," *Bein Haqtavim* 18 (2018): 164–165 [in Hebrew].

12 Ehud Maximov, "Vocabulary: Has the Ultimate Solution to Transcription been Found?," *Makor Rishon*, August 19, 2018, https://www.makorrishon.co.il/magazine/70017 [in Hebrew].

13 Lt. Col. A., "Geographic Intelligence – From Paper Napkin to 'Geo-Network,'" pp. 98–99.

The technological capability of **disseminating intelligence** has also developed since the 1990s, making intelligence increasingly more accessible to field operatives, based on cooperation between the Military Intelligence Directorate and land forces. One of the lessons of the Second Lebanon War (2006), however, was that intelligence products intended for the use of field units did not reach their intended recipients, partly due to the information being highly compartmentalized.[14] In recent years, the development of the intelligence-based combat (IBC) doctrine in the IDF has also affected the dissemination of information. This concept focuses on the need to provide relevant intelligence to field forces so that they will be more effective and efficient in terms of their maneuverability and with the understanding that the enemy has changed and that the IDF must deal with sub-state terrorist organizations, which operate differently than the military forces of a state. This concept has led to developing real-time intelligence-gathering sensors and adapting the classification levels of the information to facilitate its dissemination. Digital command-and-control systems have also been developed and employed by the IDF. In addition, network combat units were established to realize the vision of network combat and adjust it to the new capabilities and challenges.[15]

The Digital Ground Forces (DGF) project within the land forces began in the early 2000s. As part of the project, the Elbit company developed command-and-control systems for the entire land forces.[16] The systems connect intelligence collection personnel with command echelons and fire-and-attack elements based on a fiber optic network and encrypted wireless communications. Among other things, the project includes video systems, systems to manage field combat on computerized maps, and a comprehensive and relevant intelligence picture, which now reach the field forces in record time. The system has both stationary and mobile configurations, and one of its advantages is its resilience against jamming so that when it is jammed, all the information stored on the system at that time is saved.

One technological development that has facilitated intelligence access to combat forces is the augmented reality glasses device developed by the

14 Compartmentalization prevents certain parties from being exposed to information for information security reasons.

15 Gabi Siboni and Sagi Ben-Yaakov, "Intelligence-Directed Land Combat," in *Challenges of the Israeli Intelligence Community*, p. 78.

16 The system was fully deployed in most IDF land forces by 2014.

IDF's Unit 9900.[17] This device provides the combat soldier with geographic information about the adversary's territory and activity.[18] The unit adapted the device to the needs of the IDF with an off-the-shelf product by Oculus, which produces masks for gamers. The main idea behind the device is to incorporate most of the existing information from the collection personnel and make it accessible to fighters. Through the augmented reality glasses, targets can be labeled, information on rocket launches can be sent in real time, and the soldier can look "inside" buildings. The main challenge that the device tries to address is the surplus of information. The final product reflected in the system has been processed and is relevant for undertaking both training and operational tasks.

It should be noted that many of the technological developments used by the IDF originate in the civilian sector, which has inspired the military to adapt the technology to its own sphere. Some examples are tools based on the Google search engine used in order to extract information from the databases of Unit 8200; development of applications based on civilian websites for use by intelligence analysts, such as "Tracebook," which was discussed above; and technological developments created by civilian companies, such as the augmented reality glasses by Oculus. The advanced technologies embedded in the military have provided significant support for intelligence and field personnel.[19]

The Beginning of a New Paradigm in Intelligence Work

The information revolution created the foundation for a new paradigm in intelligence work, partly due to the increased use of cyber tools.[20] In recent years, the new technologies have transformed the classic functions of collection and analysis and have blurred the difference between the two. These changes weakened the classic "intelligence cycle" and underlined the

17 Unit 9900 is a unit in the Intelligence branch that deals with visual intelligence.

18 Inbal Orpaz, "From the People Who Brought You 8200: Meet 9900 – The Ambitious Younger Sister," *TheMarker*, March 31, 2015, https://www.themarker.com/technation/1.2603595 [in Hebrew].

19 Florin-Eduard Grosaru, "The Revolution in Military Affairs in Information Age and its Impact on Defense Resources Management Performance," *Conference Proceedings of eLearning and Software for Education (eLSE)* 1 (April 2015), pp. 445–452.

20 David Siman Tov and Noam Alon, "The Cybersphere Obligates and Facilitates a Revolution in Intelligence Affairs," *Cyber, Intelligence, and Security* 2, no. 1 (April 2018): 73–92.

need for a new paradigm for dealing with reality. This is consistent with the theory presented in the 1990s by Andrew Marshall and Richard Hundley, who addressed revolutions in military affairs and argued that technology itself could not lead to a revolution but must be accompanied by organizational adaptations and changes for a revolution to occur.[21]

The term "jointness" refers to operations and actions in which more than two military branches take part. In the context of intelligence, jointness refers to the processes of organizational change that have taken place within the intelligence agencies, as a result of cooperation between separate frameworks. The advantages of each are fused into a new organizational unit, with the capabilities exceeding those of each one separately.[22] Although each organization must obtain and develop its own knowledge, most of that knowledge is, in fact, found in the space between organizations. Mediation is necessary as a result, and it should be accomplished through contacts and cooperation, even though that cooperation does not always exist, partly because each organization seeks to maintain its own independence and prestige.

The terrorist attacks in the United State on September 11, 2001 exemplifies a lack of jointness. The committee investigating the attacks concluded that the United States had ample information and could have thwarted the attacks. The problem was that none of the US intelligence agencies understood the complete picture, as the collection of information and its analysis was spread among various intelligence agencies. Those agencies did not share information with one another due to a lack of cooperation that had been entrenched over the years in addition to unnecessary compartmentalization.

Today, the United States is the leader in jointness, which it had begun to develop already in the late 1970s. The September 11 attacks led to the establishment of the office of Director of National Intelligence (DNI), which serves as a framework for managing the American intelligence community. The DNI was given authority to formulate the US intelligence doctrine, recommend the appointment of senior officials in the intelligence community, and set up joint teams among the country's intelligence agencies. The concept

21 Richard O. Hundley, *Past Revolution Future Transformation* (Washington DC: RAND, 1999), pp. 1–17; Andrew W. Marshall, "Some Thoughts on Military Revolutions," Memorandum for the Record, Office of Secretary of Defense, Office of Net Assessment, July 27, 1993.

22 Kobi Michael, Dudi Siman Tov, and Oren Yoeli, "Development of the Jointness Concept in Intelligence Organizations," in *Intelligence in Theory and in Practice*, no. 1 (May 2017): 6.

behind the DNI was to increase jointness, advance cooperative efforts, and synchronize the various intelligence agencies to prevent a recurrence of events like those of September 11.[23]

A Future Look at Advanced Technologies

One of the newest developments is the Internet of Things (IoT), which enables advanced communication between devices that contain electronics, software, sensors, and camera components. IoT describes a world in which day-to-day objects are equipped with microcomputers that can monitor their surroundings, display information, and execute actions with a certain degree of independence. Communication between these objects creates the opportunity to collect information by accessing the networks to which these objects are connected.[24]

In the next few years, jointness is expected to expand as will the ability to monitor and access information around the world so that it will be possible to know what is happening at any point of interest at any given time. Consequently, the field of IoT also will grow significantly and will require methods of data analysis, processing, and storage to change accordingly. The expansion of the IoT and the accessibility of the information collected by their components will create new opportunities for intelligence agencies to gather information and to develop a new intelligence field that will enable intelligence analysts to obtain information that complements the other fields of intelligence.

The world of IoT can provide intimate information on specific human targets by connecting to networks that are linked to the targets through their watches or smartphones, for example. Thus, it is possible to learn about the targets' routine activities and to use this information as necessary as a means of incriminating them and to help thwart actions. It is also possible to connect to devices, such as smart TVs, which can transmit what is heard in their vicinity, to which there was no access beforehand. In addition, visual intelligence on distant targets around the world can be obtained not only

23 Kobi Michael, Dudi Siman Tov, and Oren Yoeli, "Jointness in Intelligence Organizations: Theory Put into Practice," *Cyber, Intelligence, and Security* 1, no. 1 (January 2017): 5–30.

24 Tal Steinhartz, "Internet of Things – Cyber Protection in the IOT World," *IsraelDefense*, May 23, 2015, https://bit.ly/2JIgISC.

through high-quality satellite images but also by connecting via cyberspace to security cameras at a particular site.

Analysis of the Changes

Given the above, it is evident that intelligence work has changed following the information revolution. This leads to the question of whether the age of information overload is helping intelligence agencies to deal with potential intelligence surprises, or whether it is actually making it more difficult to separate the grain from the chaff and to identify the bits of information that hint at the next surprise.

During the Yom Kippur War, for example, the IDF was caught unprepared for Egypt's use of advanced anti-tank and anti-aircraft missiles; this technological surprise cost the IDF losses in lives, infrastructure, and weapons. One of the missiles used by the Egyptians was the Soviet Sagger missile. Despite that the Military Intelligence Directorate had information about this missile at the time, it was kept highly classified and it did not reach the force-building entities or field forces. In other words, the threat theoretically had been recognized but no appropriate efforts were taken to prepare for it neither at the levels of intelligence, combat, or force buildup in order to develop the capability to defend against it.[25]

In Operation Protective Edge in 2014, the IDF was forced to deal with the threat of Hamas' attack tunnels, which the public and the military interpreted as a strategic surprise in terms of their widespread and efficient use. Despite the knowledge of the threat, the decision-making echelon did not fully understand the central role of the tunnels in Hamas' new military strategy and did not address them in terms of force buildup, combat, or their eradication. The state comptroller's report on Operation Protective Edge addressed the following points in which the intelligence was deficient in handling the tunnel threat:

- *Intelligence cooperation between the Military Intelligence Directorate and the Israel Security Agency regarding the tunnels and the division of responsibility between the agencies for what was happening in Gaza.* From the time the IDF and the Israel Security Agency (ISA) had left Gaza in 2005, and until 2015, Gaza had not been defined as a "target country" that

25 Effi Melzer (ed.) *Military Technology: Weapons and Intelligence* (Reut: Effi Melzer Ltd. – Military Research, Journalism and Publication, 2012), pp. 86–87.

required analysis, and the division of intelligence responsibility between the agencies had not been examined. As such, the ISA was responsible for collection of intelligence and prevention of threats in Gaza while the Military Intelligence Directorate, Southern Command, and the Gaza Division operated alongside it.

- *Inclusion of the EEI of the tunnels in the EEI of national intelligence, the Military Intelligence Directorate, and the ISA.* The tunnel threat was included in the national EEI only in 2009, and even then special intelligence attention was not devoted to it. As a result, there was no change in the attitude to the threat of the tunnels in the following years.
- *The collection efforts of the intelligence agencies regarding the tunnels*. There was not any joint intelligence collection efforts by all the intelligence agencies and the Military Intelligence Directorate. Even the ISA, which had invested a lot of resources in Gaza between 2008 and 2012, increased its collection efforts regarding the tunnels only in 2013.
- *The intelligence analysis of the tunnels threat in Gaza*. In 2012, the head of the Military Intelligence Directorate at the time determined that the Southern Command and the Gaza Division would deal with the intelligence assessment of the tunnels threat rather than the research department of the Military Intelligence Directorate. Thus, the IDF's main research unit had to suffice with the picture that emerged from the Southern Command and the Gaza Division, rather than deal independently with the matter.
- *The quality of the intelligence on the tunnels that was provided to the field forces.* Significant gaps were found in the intelligence transferred to the field forces as it related to the tunnels, which made it difficult for them to locate, neutralize, and destroy all the attack tunnels, and it limited their capability to thwart attacks launched from the tunnels into Israeli territory.[26]

The deficiencies listed above reveal significant intelligence gaps regarding Hamas' attack tunnels in the period prior to Operation Protective Edge, which affected the IDF's handling of the threat during the operation itself. One of the gaps was the fact that in the years following the Second Lebanon War, the national intelligence EEI focused mainly on the northern front, with most resources directed there. The issue of the tunnels in Gaza remained a

26 Office of the State Comptroller, "Operation 'Protective Edge': Decision Making in the Cabinet Regarding the Gaza Strip Before the Operation and at its Beginning: Dealing with the Tunnel Threat – Special Comptroller's Report," Part 2, 2017, pp. 13–19.

lower priority in the EEI, which affected the intelligence work on that issue and the existing knowledge at the onset of Operation Protective Edge. One of the lessons learned from the investigation of the tunnels in Protective Edge was that more investment must be made regarding collection and analysis of the threat posed to the tunnels along the northern front. In his report about Operation Protective Edge and especially concerning the intelligence handling of the tunnels threat in the Northern Command, the state comptroller wrote that "over the years since the Second Lebanon War, until around the time of Protective Edge, there were many collections and analysis operations regarding the Hezbollah organization, but only partial work was done regarding the tunnels infrastructure in Lebanon."[27]

The tunnels in Gaza put the focus on the subterranean field and gave it a higher priority in the EEI of national intelligence. The understanding that Hezbollah is apparently working at building tunnels to penetrate Israeli territory as part of its attack plans for the next war led to large collection efforts intended to provide intelligence about the tunnels. A special team was established, combining intelligence and technology factors, with the aim of obtaining high-quality, precise, and reliable intelligence that would help in planning actions to locate and eradicate the tunnels.[28] Some of the information came from the world of cyber and helped engineering forces during Operation Northern Shield locate and neutralize six Hezbollah tunnels that crossed into Israeli territory.

The surprise use of the Sagger missiles during the Yom Kippur War illustrates what the intelligence reality was like prior to the information revolution. It was characterized by the classic "intelligence cycle" conducted by distinct research and collection bodies and with limited capabilities to disseminate the intelligence to the field. The ability to provide real-time warnings of the missile threat was clearly limited at the time, and there were no advanced means to transmit intelligence to the field. Without any long and focused prior preparatory work, it was impossible to prepare forces for dealing with the existing threat.

In the period following the information revolution, intelligence forces improved access to information while the time frame for obtaining the information became shorter. The improvement was also reflected in the

27 Ibid., p. 19.

28 "Developing the Complete Answer to the Threat: Behind the Scenes in Operation Northern Shield," IDF website, December 6, 2018 [in Hebrew], https://bit.ly/2RBsjqY.

ability to respond to complex intelligence questions, which previously had left room only for analysts' assessments. The example of dealing with the threat of penetrating tunnels along the northern border illustrates how the proper focus, prioritizing EEIs, and the use of existing collection capabilities make it possible to obtain high-quality precise intelligence for carrying out operations to eradicate the developing threat.

The penetration of an Iranian UAV into Israeli airspace in 2018 was another example in which high-quality intelligence also provided a warning and enabled the IDF to prevent a surprise attack. On February 10, 2018, an IDF combat helicopter shot down an Iranian UAV that had been launched from the Tadmor area deep in Syria and had penetrated Israeli airspace, breaching Israeli sovereignty. The air defense systems identified the UAV at an early stage, and had been tracking it until it was shot down. The UAV's ground control station later was attacked in the area from which the UAV was launched.[29] We can assume that the other side had planned the penetration of the UAV for a long time and that Israeli intelligence apparently had prior information of the enemy's intention to execute the action. A surgical and precise attack on the ground control station would not have been possible without real-time intelligence of its precise location, which was made possible thanks to advanced collection capabilities used before and during the incident.

Although the information revolution and the period thereafter did not completely solve the uncertainty in various intelligence matters, intelligence analysts now have a greater possibility of obtaining missing information. As in the past, analysts must answer the proper questions that will lead them to resolving the intelligence gaps, but as table 1 below shows, the information revolution is having a marked effect on each of the stages in the intelligence process. This revolution also requires intelligence personnel to learn and acclimate themselves to existing capabilities.

In an age when the means of gathering intelligence can provide a response to almost any matter, we must choose the EEIs in which to invest efforts in collecting and processing information. This leads us to the importance of prioritizing EEI. In the past, when collection was more limited, certain EEIs simply were not answered. Today, the bottleneck affects the processing needed to deal with the immense amount of information that has been collected.

29 Yoav Zaitoun et al. "The IDF Shot Down an Iranian UAV that Penetrated Into Israel; Attack in Syria; An F-16 Crashed in Israeli Territory," *Ynet*, February 10, 2018, https://www.ynet.co.il/articles/0,7340,L-5102924,00.html [in Hebrew].

Without prioritizing the EEI, the ability to respond to each intelligence matter is almost impossible due to cost, manpower, and time considerations.

Table 1. The stages of intelligence research before and after the information revolution

	Before the information revolution	After the information revolution
Collection	Based on classic SIGINT and VISINT.[30]	Cyber as a new dimension; Big Data; increasing number of platforms and sensors.
Processing	Done by professionals—manpower and training; manual means and analog tools.	Development of automated tools to deal with massive amounts of data; technological developments allow information from various intelligence disciplines to be integrated.
Analysis	Clear distinction between analysts and collection personnel; the analyst "waits" to receive processed intelligence material.	Development of tools and applications make raw intelligence material accessible to the analyst; jointness between collection personnel and analysts; "technologists" as new intelligence professionals.
Dissemination	Partial transfer of information to the field; compartmentalization as an impediment.	Technological developments make the intelligence accessible in real time to fighters in the field.

As previously shown, the current blurring between collection and analysis personnel has lead to organizational changes intended to respond to intelligence needs. In an age where cyber takes up a significant share of intelligence work, a new environment has been created in which all parties must work together and share common knowledge and skill, such as the ability to search through pools of data, find the relevant information, and process it. Although collection personnel do not deal only with information collection as they did in the past, their role is different from that of "technologists."

30 SIGINT refers to signals intelligence, based on the collection of information transmitted through the broadcast of electronic signal while VISINT is visual intelligence obtained from various visual sources.

Collection personnel must have a basic understanding of the research topics being addressed by the analyst who works with them, and their work should be reflected in the creation of technological tools that will help the analyst ask the proper intelligence questions and find the proper responses. Similarly, the analyst must have a basic understanding and acquaintance with information technology and the ability to exhaust the information, as well as a basic understanding of networks and more. For example, the Military Intelligence Directorate is now thinking about "new military intelligence bases" that will provide a response for these joint frameworks. Jointly organizing the intelligence agencies will provide an opportunity to streamline work processes and will utilize the advantages of each one to improve the intelligence products and shorten their dissemination time.

The environment of the information age is rapidly changing, leading to innovation and changes on the part of the adversary as well. In addition, Israel faces a special challenge, since it must deal not only with external threats but also with internal ones, such as terrorist attacks or the "Knife Intifada" of 2016. General Herzi Halevi, former head of the Military Intelligence Directorate, argues that the coming decades will be characterized by a blurring of the line between the physical and digital dimensions. According to Halevi, whoever achieves supremacy in information and knowledge in the digital age will be the one to control the main processes.[31] He refers to it as "intelligence supremacy," that is, the ability to gather the missing intelligence information and turn it into knowledge about the enemy, in a way that will allow us to affect the adversary at the relevant time.

Winning wars in the age of the information revolution will require a different kind of intelligence, and the source of that intelligence will be, to a great extent, in the cyber dimension. Cyber capabilities can be learned and cyber tools are accessible, which enables their development by the other side as well. As the former head of the Military Intelligence Directorate argues, "the advantages of the digital revolution are also available to our enemies, and there is no reason to assume that they will rest on their laurels."[32] In the information age, when everything is open and accessible, the adversary is also able to develop learning capabilities, is more dynamic than in the past, and is therefore capable of surprising us with his abilities. Similar to the

31 Halevi, "Military Intelligence 2048 – Intelligence Supremacy in the Digital Age," pp. 26–27.

32 Ibid., p. 28.

O-RMA ("the other revolution in military affairs"),[33] which describes the reactions and developments of the other side in relation to the revolutions in military affairs, we can look at the information revolution and the period thereafter and argue that the adversary also lives in a global technological reality and enjoys the benefits of that same revolution. The adversary also learns and develops, recognizes the advantages of the opposing side, and tries to improve and attack the other side's weak spots. This poses a challenge for intelligence organizations, since access to information by all players may erode the traditional relative advantages that intelligence organizations previously had.[34]

Conclusion

We can point to three main trends that reflect technology's influence on intelligence agencies in the period following the information revolution. First, since the information revolution and the technological developments in the field of intelligence, we have gained a sharper understanding of how the process of classic intelligence work is changing and that we must adapt to new methods at the organizational level as well. Jointness between collection and analysis bodies, as well as changes in the capabilities required of the personnel, have created new work processes in the field of intelligence that differ from the past.

Second, the accessibility of intelligence has improved for the operational forces as a result of technological developments, which have enabled the secure and timely transfer of large quantities of different types of intelligence information. Improving the accessibility of the intelligence better serves the needs of operational forces and makes it easier for them to deal with unplanned incidents in real time. Moreover, the quality of the intelligence product and its connection to field operatives directly affect their ability to deal with surprises.

Third, technological developments in the use of intelligence have helped diminish room for surprise. The information age has significantly improved the ability to respond to the intelligence questions with technologies that have been incorporated into each stage of the intelligence cycle. We are

33 Itai Brun and Carmit Valensi, "The Revolution in Military Affairs of the Radical Axis," *Ma'arachot*, no. 432 (2010): 4–17.

34 D. P., "The Approach as a Guide to Technological Intelligence Force Buildup" in *Intelligence in Theory and in Practice,* no. 3 (May 2018*):* 137 [in Hebrew].

now in an era in which practically all information is open, accessible, and connected. While the level of uncertainty is declining, the challenge is now developing the skills that will enable us to attain the essential information. In contrast to the era before the information revolution, the likelihood of obtaining information today is exponentially greater today as a result of the deluge of information and the many ways of accessing it. Nonetheless, despite the efforts to make information accessible to the field echelons, there are still difficulties due to the compartmentalizing of some components of information. This requires some thought, mainly in terms of overcoming this compartmentalization so that it will not harm the preparation and readiness of the field echelons for any situation they may encounter.

The effects of the information revolution are an important and significant factor in the work of the intelligence agencies. They are apparent in all the cornerstones of intelligence work, as this article shows, while technological developments—a direct outcome of the information revolution—affect daily the ability of the intelligence agencies to provide precise information at the right time and place in order to warn and prevent the next surprise. It must be noted that while technology has significantly improved the intelligence processes, the adversary also continues to learn and improve, and we must therefore adapt in order to maintain our technological superiority.

In looking forward, where will we be in another decade, two decades, or even more? It is clear that currently the quantity of information available online is continuing to grow exponentially, and this trend will continue to influence intelligence work, challenge collection, processing, and analysis personnel, and require them to develop creative solutions that will provide answers to the questions of the EEI. Additional questions include what place will the analyst have in intelligence work, and how much time will be invested, for instance, in developing cyber tools in order to benefit collection and analysis, compared with the time invested in the analysis itself, in order to provide warnings? How many processes will become automated, and what place will the analyst have in preventing the next surprise? These questions are worthy of further study.

The importance of technology in the intelligence process will continue to develop and an increasing number of tasks will become automated and replaced by computer algorithms. This will help collection personnel deal with the large quantities of raw material—whether information from VISINT

or SIGINT—and will shorten the time currently required to process the information and disseminate it to its consumers. In the future, will the ability to warn against the next surprise remain in the hands of the human analyst, or will it be replaced in the future by computer algorithms? This question and others will continue to occupy intelligence personnel, and what may seem like science fiction today may become reality in the not-too-distant future. It is therefore worthwhile addressing this issue and preparing for its eventuality.