The Cybersphere Obligates and Facilitates a Revolution in Intelligence Affairs

David Siman-Tov and Noam Alon

History is replete with examples of world powers, countries, and militaries that failed to identify the revolutionary potential of a new technology and, as a result, lost their advantage and relevance. This article addresses the gap between the essential technological changes that the cybersphere has created and facilitates and the outmoded functioning of intelligence organizations, which have remained rooted in the approaches, architecture, and tenets of the intelligence cycle paradigm that emerged between the two world wars. This gap creates a need for a systemic and conceptual change, but the lack of an awareness of crisis and urgency within the intelligence community as well as in the public discourse has delayed any transformation, even though discussion about the gaps between the functioning of the intelligence agencies in the cyber age and their approaches, culture, and structure has been underway for more than a decade. The main reason for this lack of awareness of crisis and urgency is that the intelligence community continues to function and make achievements even in its current format, particularly in operative and tactical spheres.

This article is significant in that it provides a clear and methodical presentation of the gaps and tensions in the intelligence community due to its delay in adopting a new paradigm.

Keywords: Intelligence, cybersphere, revolution in intelligence affairs, intelligence community, paradigm, intelligence cycle

David Siman-Tov is a researcher at the Institute of National Security Studies. Noam Alon is an expert in the fields of strategy and intelligence.

Introduction

History is replete with examples of world powers, countries, and militaries that failed to identify the revolutionary potential of a new technology and, as a result, lost their advantage and relevance.[1] The history of business companies is awash with similar stories that also resulted in the collapse of mega corporations and the rise of other corporations in their stead.[2] This history proves that merely identifying and adopting new technologies is not enough, since conceptual, cultural, structural, and value-laden changes are needed to fully realize the technological potential and crystallize it into a revolution that creates a new paradigmatic operational space.

This article addresses the gap that developed between the material technological changes that the cybersphere—in its broadest sense—has facilitated, including new approaches to the production of information and knowledge, the interactions between intelligence organizations and the environment and their intelligence targets, and the modus operandi of the intelligence organizations. To a great extent, these organizations have remained rooted in their approaches, architecture, and tenets from the intelligence cycle paradigm that emerged between the two world wars.[3] This gap creates a need for a systemic and conceptual change, but the absence of awareness of crisis in the intelligence community as well as in the public discourse has delayed this transformation. This lack of an awareness of crisis is mainly due to the fact that the intelligence community continues to function and achieve results, particularly at the operative and tactical levels. Another reason for the absence of change in the existing paradigm is because the public and many decision makers perceive the intelligence community as a "black box," inhibiting any critical discourse that could motivate change from outside.

---

1 Max Boot, *War Made New: Weapons, Warriors and the Making of the Modern World*, (Tel Aviv: Maarachot Publishing, 2015) [In Hebrew].

2 Well known examples are the collapse of both Kodak and Blockbuster due to their failure to adapt to the digital age, and Blackberry's loss of its dominance because of its fixation on the structure of its digital device.

3 The concept of the "intelligence cycle" defined a number of basic stages that comprise the intelligence process: information collection, information processing (i.e., analysis), and distribution of the resulting intelligence to the various consumers. For more on this subject, see David Siman-Tov and Ofer G., "Intelligence 2.0 – New Approach to the Production of Intelligence," *Military and Strategic Affairs* 5, no. 3 (December 2013): 27–29.

The Current Intelligence Paradigm: "The Intelligence Cycle"

A paradigm is a world view that defines the conceptual perspective and the structure and logic of the basic functions of a system and its components. The conceptual perspective is based on the social and organizational consensus that determines the relations between the various parties and explains and interprets the environment in which the individual and the organization operate.[4] Paradigms are challenged and naturally change as disparities multiply between the customary interpretation and the phenomena that it is supposed to interpret; however, any such change also triggers a crisis, due to the difficulty in adopting new perspectives and discarding the old ones. As soon as a new paradigm is formulated, it presents a conceptual system of beliefs, values, and concepts, and these are reflected in structures, processes, ethics, and the boundaries of what is permitted and prohibited. Well known historic examples of changing paradigms are the shift from the belief in faith and myths to the need to prove things scientifically and the shift from the assumption that the earth is flat and at the center of the universe to the recognition of the centrality of the sun and that the earth is round.

In the military context, it is customary to mention the "Revolution in Military Affairs" (RMA) in the information age, which conceptually transformed the way militaries fight.[5] In the intelligence context, military leaders in the old world directly managed intelligence. This was Moses' role in the biblical spy affair as well as Napoleon's role. Within the scope of this paradigm, intelligence was based on relations of trust between the leader and the human spies that he operated. A new paradigm emerged during the industrial age, which produced, inter alia, the invention of the telegraph and walkie-talkies. This paradigm focused on the ability to collect and decode signals (a representative example of this is the Enigma Code, the key intelligence project during World War II).[6] The new paradigm required

4 Thomas S. Kuhn, *The Structure of Scientific Revolutions* (Chicago: University of Chicago Press, 1970), 2nd ed., pp. 52–76; Amir Levy and Uri Merry, *Organizational Transformation: Approaches, Strategies, Theories* (Greenwood Publishing Group, 1986), pp. 10–14.

5 Deborah G. Barger, *Toward A Revolution in Intelligence Affairs* (Santa Monica: RAND Corporation, 2005).

6 David Kahn, *Seizing the Enigma: The Race to Break the German U-Boats Codes* (New York: Houghton Mifflin Harcourt, 1991).

establishing a more professional intelligence organization that would be based solely on direct communications with the military leader. This is how the intelligence profession developed on the political level. The dramatic increase in the volume of signals and in electronic warfare necessitated the establishment of intelligence organizations that would engage not only in collecting and analyzing information but also in organizing, interpreting, and making information accessible to the decision makers. This is the paradigm that was employed when strategic intelligence organizations were established after World War II, with one of its key principles being the concept of the intelligence cycle as the logic that organizes the relations between the collection and research entities and between the intelligence organization and the leader.[7]

The intelligence cycle paradigm, which still prevails today to a great extent, differentiates between the various components of the intelligence system and defines the modes of communication between the various types of units within the intelligence organization, especially between the collection personnel and the researchers. Within the collection unit, it has created sub-divisions distinguished by the various modes of information collection: signals collection (SIGINT), open-source collection (OSINT), visual collection (VISINT), and human collection (HUMINT). The intelligence cycle paradigm also has determined the communication between the various units of the intelligence organization as well as with the decision-making echelon. These communications are characterized by questions and answers and by the strategic echelon's guidance and direction of the intelligence system (evaluating critical information).[8] It also sets clear boundaries between the object of the intelligence—another country or adversary that constitutes an object of intelligence activity—and the country where those intelligence

7 The main proponent of the concept of the intelligence cycle was Sherman Kent, who was the head of the CIA's Research and Analysis Branch and previously had developed his world view in academia. See Sherman Kent, *Strategic Intelligence for American World Policy* (New Jersey: Princeton University Press, 1949).

8 Ibid.

organizations operate.[9] The main role of intelligence is to provide factual answers and to expose secrets about the reality "on the other side" and mainly to provide warnings.[10]

Attempts to Contend with the Changing Reality

The dominance of the intelligence cycle paradigm presently is reflected in the organizational structure, the functional divisions, and the ethos and logic that govern the intelligence work. However, in recent years, the intelligence environment began functioning differently, which in many cases has been inconsistent with the principles of the intelligence cycle. Thus, a situation has emerged whereby, on the one hand, the intelligence components and the defined relations between themselves and with the external environment have remained as they were; yet, on the other hand, new and different components and patterns began to emerge that have challenged the existing paradigm. This is characteristic of the situation whereby the paradigmatic system is in an interim phase: it does not change the basic conceptual system that defines it; at the same time, however, it allows the "weeds" to grow but also attempts to contain them so that they do not challenge the mainstream.

In fact, calls for a "revolution in intelligence affairs" already were heard more than a decade ago. At the time, a main argument was that the intelligence organizations' major failures of the previous decades were the result of the changes in the strategic environment and in the nature of the challenges and threats.[11] Authors of a comprehensive research conducted by the RAND

9 For a first-hand description of the paradigm and its implementation in the Israeli case, see Yehoshofat Harkabi, *Intelligence as a Government Institution* (Tel Aviv: Maarachot Publishing, 2015) [in Hebrew]. Prior to the establishment of the State of Israel, and in the absence of defined borders, the intelligence service of the Yishuv used to frequently travel to the capitals of the Arab countries in order to seek answers to questions that troubled the leaders of the Yishuv. They also considered intelligence as "a bridge to peace." After the establishment of the state, this mission was replaced by the primary mission of developing knowledge about Israel's adversaries, the strategic environment, expressed mainly by providing warnings of war.

10 Joseph S. Ney, "Peering into the Future," *Foreign Affairs* 73, no. 4 (August 1994): 82–93.

11 David T. Moore, *Sense-making: A Structure for an Intelligence Revolution* (Washington, DC: National Defense Intelligence College, March 2011); Russell E. Travers, "Waking Up on another September 12th: Implications for Intelligence Reform," *Intelligence and National Security* 31, no. 5 (2016): 746–761.

Institute at the beginning of this century expressed concern that the actions of the US intelligence following its failure to prevent the terrorist attacks of September 2001 and its erroneous assessment of Iraq's nonconventional weapons were merely reforms of the old intelligence paradigm and were insufficient to bring about a real change in the functioning of the intelligence community.[12] The actions included establishing an umbrella organization tasked with determining the intelligence strategy and directing the intelligence community (the Directorate of National Intelligence [DNI]) and forming joint research entities. The DNI also began to encourage information sharing between the various intelligence organizations.[13]

The Israeli intelligence community also attempted to improve the intelligence functioning, inter alia, by using new systematic ideas, which included structural and functional changes. These included organizational restructuring processes implemented by the heads of the Military Intelligence Directorate led by Major-General Aharon Ze'evi-Farkash and by Major-General Aviv Kochavi.[14] The process that Major-General Ze'evi-Farkash conducted included the formation of joint intelligence forums, led by a

12 Barger, *Toward a Revolution in Intelligence Affairs*; Gregory F. Treverton and Peter A. Wilson, "True Intelligence Reform Is Cultural, Not Just Organizational Chart Shift," *RAND Blog*, January 13, 2005.

13 Gordon Nathaniel Lederman, "Restructuring the Intelligence Community," in *The Future of American Intelligence*, ed. Peter Berkowitz (Stanford: Hoover Press, 2005), pp. 65–102. In his article "Waking Up on Another September 12th: Implications for Intelligence Reform," Russell Travers seeks to expand this trend so that it will include the entire American intelligence community. According to his approach, three major courses of action need to be taken: subordinate all US intelligence agencies to a single intelligence director who is vested with full responsibility and authority; establish supra-organizational taskforces above the existing intelligence agencies, which will handle all of the national challenges; and enable a relatively free flow of information and knowledge between the different agencies and the supra-organizational task forces.

14 Aviv Kochavi and Eran Ortal, "*Ma'asei Aman*" – Permanent Change in a Changing Reality," *Bein Haktavim* (Dado Center), no. 2 (July 2014) [in Hebrew]; Aharon Ze'evi Farkash and Dov Tamari, *And How Will We Know* (Tel Aviv: Yedioth Ahronoth Publishing, 2011) [in Hebrew]; Naomi Fassa Yosef and Sarit Shapira, "Bridge over Troubled Water: The Aman Endeavor in the World of Complexity," *Intelligence in Theory and Practice* (Israeli Intelligence Community Commemoration and Heritage Center), no. 2 (2017); Hagai Huberman, "The Director of the Israel Security Agency: To Adapt Our Assessments to the Changing Reality," *Arutz 7*, May 15, 2011, https://www.inn.co.il/News/News.aspx/219724.

head of the research division, for the purpose of designing an intelligence campaign. This process expired after a few years. Among the changes directed by Major-General Kochavi was the establishment of a social network for intelligence purposes (nicknamed "Tracebook," with Facebook being its source of inspiration); however, personnel in the intelligence system today claim that the network's potential is only being partially realized and that the intelligence discourse on the network is limited. The director of the Military Intelligence Directorate, Major-General Amos Yadlin, established the Operations Division for the purpose of improving the ability of the Intelligence Division to engage in operative issues and improve the joint functioning of its collection and research personnel.[15] On the other hand, the attempts to form joint task forces in the Military Intelligence Directorate encountered difficulties and constant tension vis-à-vis the collection units. The intelligence discourse in Israel raised the idea of creating shared spaces for the production of intelligence knowledge, as well as the need to break the intelligence cycle by exploiting new technological capabilities to improve the intelligence functioning and enable it to more easily contend with the environment's new challenges. These ideas have not yet come to fruition, and as a result, most of the intelligence knowledge continues to be developed in each separate research organization.[16]

In recent years, additional complaints have been raised about the functioning of the intelligence community, emphasizing the need for a systemic change. For example, some point out that the information and big data age requires intelligence organizations to make systematic adjustments that are not always compatible with their current structure and functioning.[17] Others call for a change in the intelligence collection field, inter alia, by giving expression to the idea of all-source intelligence.[18] Furthermore, there has been growing recognition of the importance of open-source intelligence and the need to

15 Amir Rappaport, "Upheaval in Intelligence," *Israel Defense*, March 2014 [in Hebrew].

16 Siman-Tov and Ofer G., "Intelligence 2.0 – New Approach to the Production of Intelligence," pp. 27–42.

17 Kevjn Lim, "Big Data and Strategic Intelligence," *Intelligence and National Security* 31, no. 4 (2016): 619–635.

18 Roberto Mugavero, "Challenges of Multi-Source Data and Information New Era," *Journal of Information Privacy and Security* 11, no. 4 (2015): 230–242.

establish new intelligence centers that will specialize in this field.[19] Calls for the establishment of intelligence centers that will synthesize intelligence from multiple sources have also increased.[20]

Intelligence researcher William Lahneman called for a paradigmatic change in the American intelligence community, due to the changing access to information as well as the nature of the threats (the emergence of supra-state and sub-state threats). According to his approach, organizational, conceptual, and process changes that reflect a more decentralized and less compartmentalized approach are necessary, and, by doing so, they will help develop agility in the face of the changing reality.[21] In a comprehensive research study, Lahneman enumerated the reasons why the reforms instituted by the American intelligence community after the 9/11 terrorist attacks were inadequate, arguing that they were merely evolutionary changes and that subsequently, the US intelligence agencies continued operating according to the traditional Cold War era paradigm. According to Lahneman, a systemic transformation is needed, given the changing nature of the threats and the opportunities as a result of integrating forces and knowledge sharing with the civilian environment. Lahneman proposed that two paradigms be maintained concurrently: the traditional paradigm, which would focus on solving puzzles through covert and classified sources, and a new paradigm that would contend with global trends and new threats challenging both the intelligence community and state and global civilian organizations and would also enable cooperation with private business entities by employing a new

19 Hamilton Bean, *No More Secrets: Open Source Information and the Reshaping of U.S. Intelligence* (Santa Barbara: Praeger, 2011); Michael Glassman and Min Ju Kang, "Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT)," *Computers in Human Behavior* 28, no. 2 (March 2012): 673–682; Hamilton Bean, "The DNI's Open Source Center: An Organizational Communication Perspective," *International Journal of Intelligence and Counterintelligence* 20, no. 2 (2007): 240–257.

20 Christopher G. Pernin, Louis R. Moore, and Katherine Comanor, *The Knowledge Matrix Approach to Intelligence Fusion* (Santa Monica: RAND Corporation, 2007).

21 William J. Lahneman, *Keeping U.S. Intelligence Effective: The Need for a Revolution in Intelligence Affairs* (Lanham, PA: The Scarecrow Press, 2011); William J. Lahneman, "The Need for a New Intelligence Paradigm," *International Journal of Intelligence and Counter Intelligence* 23, no. 2 (2010): 201–225.

concept of the flow of information. Robert Steele also addressed the need for sharing intelligence information with global civilian entities.[22]

The Cybersphere Penetrates the Paradigm's Boundaries

Despite the partial success of the attempts described above, after more than a decade, the conditions are now ripe for revolutionizing the way in which the intelligence communities are built and operate around the world as well as the relations between them and the external environment. What facilitates such a transformation and actually obligates it is the cybersphere, which, in the broad sense of the word, is "the missing piece" in the ideas that had been proposed in the past.[23]

The cybersphere includes the physical and non-physical space created by the following sources: computers, mechanized systems and networks, software, computerized information, content, and the users themselves.[24] At issue is a human, technological, and cultural phenomenon that emerged more in the last decade. The cybersphere is an artificial space (as opposed to sea, air, and land) and the communication between its components is carried out through bytes. This facilitates the creation of links and shared spaces between different intelligence disciplines, which in the past were compartmentalized and were only connected through people's minds.

Cybersphere, as a new intelligence environment, is changing the basic assumptions about information and knowledge. The volume of information that is available to intelligence agents—whether working in a research unit or in a collection unit—makes it impossible to know how much information exists on a particular subject, how much of the information they possess, and

22 Robert Steele, "Foreign Liaison and Intelligence Reforms: Still in Denial," *International Journal of Intelligence and Counterintelligence* 20, no. 1 (2007): 167.

23 "Information warfare is more than just information-enabled warfare, which albeit represents an important aspect of information or cyber warfare, but not in totality. Cyber warfare [should be perceived] as strategic warfare which can be used as a principle means to achieve strategic ends and as required by Luttwak's criterion for strategic warfare, the framework for the strategic cyber warfare is to be defined across all spectrum of affairs right from the grand strategy to the tactical level." The quote is taken from Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends," *Strategic Analysis* 34, no. 1 (February 2010): 62–73.

24 The definition is taken from an *ITU Cybersecurity Gateway* document.

whether they have all the relevant information.[25] Moreover, the intelligence organizations are incapable of fully utilizing most of the information in their possession, whether due to the deluge of information and knowledge from sensors or to the difficulty of contending with classified and non-classified databases. This state of affairs casts a dark shadow over the capacity to sustain the basic idea underpinning the architecture and functioning of intelligence in the intelligence cycle era; that is, the ability to sift information until a "golden nugget" is found or those pieces of limited information that, prima facie, provide objective and data-based evidence of the emerging reality on the other side.[26]

As stated, in the cyber age, intelligence personnel have potential access to infinite information; however, most of the researchers in the majority of the intelligence organizations continue to operate according to traditional practices by "emptying the magazine"; that is, by reading intelligence items based on the collection personnel's prioritization. The establishment of a "social intelligence network,"[27] which also symbolized a new approach to intelligence production, did not change the old habits—at least not in the Military Intelligence Directorate—nor did it create another format of consuming information or developing knowledge. Thus, while intelligence researchers in the civilian environment consume information and develop knowledge according to the digital culture and the "open code,"[28] in the classified intelligence system, they return to consuming information and developing knowledge as if they were still in the 1990s in keeping with the intelligence cycle.

The first handicap that impedes change is conceptual and not technological, since ideas about "webint for every researcher"—the idea that a researcher should be allowed access to the internet and classified databases and the

25 Barger, *Toward a Revolution in Intelligence Affairs*; Michael Warner, "Intelligence in Cyber and Cyber in Intelligence," in *Understanding Cyber Conflict: 14 Analogies*, ed. George Perkovich and Ariel E. Levite (Washington, DC: Georgetown University Press, 2017), pp. 17–31.

26 Bruce Berkowitz, "The Big Difference Between Intelligence and Evidence," *RAND Blog*, February 2003.

27 Kochavi and Ortal, "*Ma'asei Aman*" – Permanent Change in a Changing Reality."

28 Studies show that millennials make their first contact with news via the social media, and only if they are interested in a particular subject do they look for elaboration on regular news channels. See, for example, Roy Greenslade, "How the Different Generations Consume their Daily News," *Guardian*, July 22, 2015.

technological systems that facilitate this—had already emerged in the Israeli intelligence community at the beginning of the 2000s. This conceptual handicap causes intelligence researchers to not fully exploit the nearly infinite potential enjoyed by other researchers, such as in academia or in business.

As noted, the cybersphere enables the creation of a shared intelligence space. In the past, the separation between the collection units, which was based on wave lengths and various production characteristics, is swiftly being replaced by a shared byte-based digital space. In essence, the new collection agent is a technologist, and all of the rest of the intelligence functionaries, whether in collection or research, perform research operations at varying levels and quality and for different needs. The main problem of intelligence in the cyber age is no longer finding the "right" information and its analysis for the purpose of discovering the "secret," but rather asking the right question that creates new knowledge[29] and engages in creating and defining new conceptual categories.[30] This mission is no longer the domain of the researcher alone, just as the ability to locate relevant information and produce it is no longer the domain of only the collection agent; today, both the intelligence collector and researcher have the same basic knowledge and also share similar searching, identifying, and processing capabilities.

The cybersphere creates a shared domain with the adversary, while the intelligence cycle relies, to a great extent, on the geographic boundaries between us and our adversaries.[31] These boundaries enabled the creation of both conceptual and functional separation between research, collection, covert offensive operations, and preventive security; in the cyber age, however, these separations have become artificial and superfluous. A collection operation, which includes accessing a database, is not materially different from a covert

29 A.H., "Does Intelligence Research Need to Change and How?" *Intelligence in Theory and Practice* (Israeli Intelligence Community Commemoration and Heritage Center), no. 2 (2017).

30 Itai Brun, *Intelligence Research: Responsible Practice in an Age of Transformations and Changes* (Israeli Intelligence Community Commemoration and Heritage Center, 2015), pp 58–59 [in Hebrew]. For an elaboration on the creation of new categories and their importance to understanding reality, see Zvi Lanir, *Creating New Categories in the World* (Tel Aviv: Praxis Institute, 2008) [in Hebrew].

31 Robert D. Williams, "(Spy) Game Change: Cyber Networks, Intelligence Collection and Covert Action," *George Washington Law Review* 79, no. 4 (2010): 1162–1200.

offensive operation in cyberspace.[32] The very act of searching for information leaves digital footprints and changes in the web itself. These changes directly impact both the adversary and the side executing the operation, as well as civilians, other rival countries, and friendly nations. Researchers are no longer required nor can they restrict themselves to passive reading of information on the web. Accessing forums requires researchers to assume that they are visible to others, even if using a false identity. This trend greatly challenges the ability to separate between the passive and active intelligence functions, requires the researchers to have sophisticated tools to manage identities on the web, and enables them to become an active partner in the creation and consumption of knowledge on the web.

The cybersphere accelerates the environment's pace of change; the speed at which technologies are replaced, the ease in their dissemination, and their low prices create an infrastructure that allows for enemies, adversaries, friends, the internal intelligence arena, as well as the civilian and business environment to constantly shift. The symbiosis of all these changes creates a reality of constant movement and rapid transformation, which often transpires in an unanticipated, non-linear manner. This pace of change greatly challenges two basic roles of the intelligence cycle. Firstly, it hampers the ability of knowing the right question and thus also the capability of sustaining the "engine" of the intelligence cycle; one side has prioritized clear questions (decision maker or researcher) while the other side has prioritized clear answers (researcher or collector). Secondly, it challenges the ability to preserve the standards of an intelligence product, since the orderly, sequential process of creating information, constructing a stable intelligence picture, and disseminating it is prolonged and often exceeds the time constraints of the rapid events. Furthermore, the cybersphere has changed the kind of expertise required of intelligence personnel; if, in the past, intelligence agents needed expertise only in their specific field of research, in the cyber age, researchers require considerable competence in information technologies, languages, database management, a thorough understanding of networks, statistics and more, in addition to their disciplinary expertise.

32 These understandings led to ideas in the United States of consolidating the Cyber Command with the National Security Agency (NSA). See, for example, Jason Healey, "Shaking Up the Top of Cyber Command," *CIPHER Brief*, October 22, 2017.

The Cybersphere and Intelligence: A Paradigmatic Crisis

In the previous two sections, we presented the changes that the intelligence organizations have implemented in order to sustain the current intelligence cycle paradigm. In the following, we will present a number of examples that characterize the incompatibility of the intelligence work with the cyber age, notwithstanding those changes.

As stated, the intelligence cycle divides intelligence work into collection units and a central research entity. Despite that most of the collection units engage in the cyber era in bytes and the link between them—even before the material reaches the researcher—they continue to work separately, and the connection between them, if it occurs, is done mechanically or by force and does not remove demarcations nor does it become "natural."[33] Interim concepts created in recent years, like "Cyber-HUMINT" (the creation of virtual human entities) and "HUGINT" (combination of HUMINT and SIGINT), or stationing VISINT personnel in the SIGINT unit and vice versa in order to fully exploit the geo-cyber field,[34] convey the complexity of the current situation and the need to re-examine and ascertain whether the existing collection architecture is still valid.

The emergence of cracks in the conceptual walls has destabilized the "barrier" between the intelligence community and its consumers. And indeed, already about a decade ago, the former commander of Unit 8200 called for "demolishing the walls" between his unit—the Intelligence Corps' chief collection unit—and the research agencies.[35] Despite this, the architecture of the intelligence community, both in Israel and elsewhere, has remained unchanged, and the organizational and political barriers continue to determine the pace of the change, in effect, preventing any initiatives for profound changes.

---

33 For elaboration, see Lieut. Col A., "Geographic Intelligence – From a Paper Map to the Geo-Web," in *Challenges of the Intelligence Community in Israel*, ed. Shmuel Even and David Siman-Tov (Tel Aviv: Institute of National Security Studies, 2017); Avi Tal and David Siman-Tov, "HUMINT in the Cybernetic Era – Gaming in Two Worlds," *Military and Strategic Affairs* 7, no. 3 (December 2015): 93–102.

34 Lieut. Col A. V., "A Tactical Technological Body as Bringing Change to the Field Intelligence Deployment," *Intelligence in Theory and Practice* (Israeli Intelligence Community Commemoration and Heritage Center), no. 2 (2017).

35 Siman-Tov and Ofer G., "Intelligence 2.0 – New Approach to the Production of Intelligence."

In the past, the intelligence information production process had been based on an individual's expertise, such as the investigator in HUMINT, the translator or the network intelligence expert in SIGINT, and the expert researcher in that field. The prevailing understanding in the intelligence communities around the world today is that there is a need for cooperation beyond just telephone conversations or exchange of email. As a result, ad hoc entities are formed that rely on cross-organizational team work; however, a significant number of these entities are created as temporary organizations that are dissolved once the mission has been accomplished. Indeed, one can also point to revolutionary attempts, like that of the former director of the CIA, who formed task forces instead of the organization's professional divisions.[36] As a rule, however, the basic architecture that erects a wall between the collection organizations and the research organizations and between the collection organizations inter se prevents the establishment of permanent joint organizations that would also include representatives from outside the intelligence community. This situation is tremendously frustrating for those who are attempting to establish these types of organizations.

Another trend in the discourse is the nature of communications between the research entities in the intelligence communities. Inter alia, at issue is the establishment of organizations that would integrate representatives from all the research entities within the intelligence community,[37] as well as calls for the establishment of a shared research space both in Israel and in the United States. In the mid 2000s, there was an appeal within the Israeli Military Intelligence Directorate to establish an "Intelligence Wikipedia," and similar demands were also voiced in the American intelligence community.[38] Nonetheless, the various research entities in both communities still continue to develop their knowledge separately.

---

36 David Sternberg, "About the Change in the CIA: Task Jointness as an Adaptive Organizational Concept," *Intelligence in Theory and Practice* (Israeli Intelligence Community Commemoration and Heritage Center) no. 1 (2016) [in Hebrew].

37 For information about the term "jointness" and its implementation in military, intelligence and civilian systems, see Kobi Michael and David Siman-Tov, "Jointness in Intelligence Organizations: Theory Put into Practice," *Cyber, Intelligence, and Security* 1, no. 1 (January 2017): 5–30.

38 D. Calvin Andrus, "The Wiki and the Blog: Toward a Complex Adaptive Intelligence Community," *Studies in Intelligence* 49, no. 3 (September 2005): 63–70, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=755904.

An additional trend has been the call to produce shared intelligence products within a framework called "Living Intelligence." The idea was that any intelligence entity could update the product and avoid the endless chain of coordination and redundancies.[39] According to this methodology, the consumer was supposed to receive a "living" integrative product that is constantly updated and at a faster frequency than is customary today. Basically, most of these ideas were not substantively implemented and were apparently ahead of their time, blocked by the traditions of the intelligence communities traditions and their fixed work patterns.

One of the disciplines in which the need for a fundamental change has been felt and discussed for a long time is open-source intelligence.[40] The growing consensus is that open-source intelligence is no longer merely a collection discipline; as a result, the organizational positioning of open-source intelligence is disputed, and two alternatives usually are on the agenda: first, to position open-source intelligence in the collection space; and second, to integrate it in the research space. There is, however, a practical difficulty in implementing these changes. Thus, leaving it in the sphere of collection, at least in Israel, creates quite a few anomalies: the researchers swiftly and fully exploit the information to the point of investigative products even before the collection unit has processed and disseminated the information; the databases available on the web are investigated even before the collection unit has cataloged them; and investigative products and relevant civilian and business information collections are not fully utilized because of a lack of desire to establish a reciprocal relationship on the web.[41]

---

39 David A. Schroeder, "Efficacy and Adoption of Central Web 2.0 and Social Software Tools in U.S. Intelligence Community" (master's thesis, American Military University, March 2011), http://das.doit.wisc.edu/amu/Schroeder_Thesis_MAR11_Redacted.pdf.

40 Hamilton Bean, "The DNI's Open Source Center: An Organizational Communication Perspective," *International Journal of Intelligence and Counterintelligence* 20, no. 2 (February 2007): 240–257; Robert David Steele, "The Open Source Program: Missing in Action," *International Journal of Intelligence and Counterintelligence* 21, no. 3 (May 2008): 609–619.

41 An interesting example of using the open web as a learning space and not only as an information-collection space can be found in *Global Trends*, a periodic publication by the US-based National Intelligence Council (NIC) and in the UK-based Development, Concepts and Doctrine Center (DCDC), which publishes *Global Strategic Trends*. These entities cooperate and consult with experts and with the general public in designated forums, as part of the process of preparing their reports.

From analyzing the trends, it appears that there are flickers of change, but also constraints and obstacles, which are mostly conceptual and organizational. It is possible to identify potential dimensions of change in nearly every intelligence discipline, but the actual transformation is limited in scope. Consequently, we argue that a material change can only take place in the various levels of the internal and external intelligence functioning if a paradigmatic change occurs, and the intelligence community—as the body tasked primarily with the development of knowledge—might miss out on the revolution on this issue taking place in the civilian space.

As stated, among the factors preventing the change are organizational traditions and operational approaches, which are difficult to abandon, and the battles over prestige and resources that such a dramatic change could trigger.[42] Furthermore, many argue that the gradual route that the intelligence community is taking now, which does not jeopardize its existing assets, is preferable. Another key factor hindering change is the absence of a perceived crisis, from both an internal and external perspective. As presented earlier, the change in the American intelligence community occurred after the 9/11 terrorist attacks in the United States and the crisis in Iraq in 2003. In Israel, the intelligence community implemented significant changes following the Agranat Commission's report on the Yom Kippur War. The absence of awareness of a crisis, coupled with a perception of intelligence as being successful—mainly due to its outstanding work with operative and tactical intelligence and its successes with cybernetic intelligence collection—constitute tremendous obstacles that hinder achieving the needed change.

Outline of a New Paradigm: Cybernetic Revolution in Intelligence Affairs

We are currently in a transitional stage from an old paradigm—which is becoming increasingly challenging to sustain—to a new paradigm that has yet to be forged, but nascent inklings of its characteristics are already being implemented in the field. In this section, we will attempt to outline a number of principles of the new paradigm, which we call a Cybernetic Revolution in Intelligence Affairs (CRIA).

42 For a discussion about the issue of battles of prestige and organizational politics, as well as the absence of a sense of crisis in the intelligence community, see Michael and Siman-Tov, "Jointness in Intelligence Organizations."

A constantly changing open system

Itai Brun, the former director of the Research Division in the Military Intelligence Directorate, often stressed that intelligence, and particularly intelligence research, is at the forefront of contending with the uncertainty of the changing reality.[43] This reality, of constant accelerated change, obligates the intelligence community to develop an open approach and structure:

- A culture that encourages a rapid flow of information and knowledge within the intelligence space and between the intelligence space and the civilian space: Studies show that an organization that is less formally organized, less hierarchic, less centralistic, and more decentralized, flexible, and able to delegate authority to lower echelons has a better ability of contending with rapid changes in the environment, adapting, and finding solutions to complex problems.[44]
- Mission structures: The basic architecture of the intelligence community needs to shift from a longitudinal structure based on independent units that are responsible for all the tasks within their purview and the communications between them to a matrix structure, based on multi-disciplinary units that are responsible for a particular problem. Additionally, these mission structures will require maximum latitude to fulfill their needs, and this is done by developing connections with other mission structures and by forming mission-specific structures for necessary secondary tasks. Accordingly, these mission structures will need relative freedom of action to choose the mission and the way to accomplish it. There are two main restrictions to such a structure: the first relates to the need for a centralized management by the organization's directors and middle echelons; to this end, a matrix-style management culture should be developed;[45] the second restriction relates to force-building that will feed these mission structures

43 Brun, *Intelligence Research: Responsible Practice in an Age of Transformations and Changes*, pp. 11–18.

44 P. R. Lawrence and J. W. Lorsch, "Differentiation and Integration in Complex Organizations," *Administrative Science Quarterly* 12, no. 1 (January 1967): 1–47; Henry Mintzberg, *The Structuring of Organizations* (Englewood Cliffs, NJ: Prentice-Hall International, 1979).

45 Lieut. Col. N., "Intelligence Knowledge Community as a Mechanism of Action Providing Strategic and Systemic Flexibility to Aman," *Intelligence in Theory and Practice* (Israeli Intelligence Community Commemoration and Heritage Center) no. 1 (2016): 45–54 [in Hebrew].

and facilitate the continuing development of the basic disciplines. The new collection units that will focus on force-building can consolidate a number of disciplines, such as VISINT and SIGINT or special operations and HUMINT. Such a change could also enable the creation of significant shared spaces between the various intelligence organizations in favor of the force-building.[46]

- Partnership with the civilian, business, and academic sphere: This partnership needs to rely on open discourse and exchanges of information, insights, and assessments. Currently, the connection between the intelligence space and the civilian one is based on a bilateral discourse; whereby the intelligence community receives information and knowledge from external sources, the process is not reciprocal nor synergetic. A partnership between the intelligence and civilian spaces will enable the creation of new intelligence products and exchanges of information and knowledge which, in turn, could lead to fresh thinking about familiar problems, learning about unfamiliar issues, and enhancing the capability to solve various problems and improve existing solutions.

An active system

As we saw, the cybersphere dictates separation from the intelligence cycle paradigm and primarily, separation between active intelligence (which, according to the traditional paradigm, is attributed to collection) and passive intelligence (which is usually attributed to research and processing). A concept, theory, and doctrine need to be developed in which the researcher, in addition to understanding the reality, needs to also be responsible for significant components of intelligence collection (mainly open-source) and processing. This requires the collection units to redefine their role and the research units to provide their researchers with new skills required of "information research officers."[47] The traditional organizational division between some of the collection units and the research units might also change.

46 Yahel Arnon, "Force-buildup in the Intelligence Community in a Changing Reality, *Intelligence in Theory and Practice* (Israeli Intelligence Community Commemoration and Heritage Center), no. 2 (2017).

47 Major (res.) D.G., "The 'Information Research Officer': A New Concept in Intelligence Research," *Intelligence in Theory and Practice* (Israeli Intelligence Community Commemoration and Heritage Center), no. 2 (2017).

A system based on fusion technology, artificial intelligence, and machine learning

These technologies, which national intelligence organizations are only beginning to use (unlike, for example, in business intelligence), are expected to render redundant a significant part of the core intelligence collection and research work according to the intelligence cycle paradigm, especially as it pertains to categorizing information according to spheres of knowledge, interpretations, spheres of interest, and so forth; issuing recommendations for action based on past cases, analogies, and scenarios; and identifying clustering of information.[48] At the same time, a technologies-based system requires new roles to be defined (for example, a researcher of clustering) and new processes (such as quality control in lieu of searching information). This kind of system also renders superfluous the separation between collection and research, since some of the practices of processing and researching also will become technological and automated.

Conclusion

Some of the insights presented in this article are not new. The discourse about the growing gaps between the functioning required of the intelligence communities and their approaches, culture, and structure has existed for more than a decade, both within the American and Israeli intelligence communities. The attempts to generate change and adaptations are also not new. Nevertheless, the intelligence communities have remained loyal to the intelligence cycle paradigm and have failed to generate revolutionary changes. It appears that the main reason for this relates to the absence of a sense of urgency and crisis.

The importance of this article is that it presents clearly and methodically the existing gaps and tensions due to the delay in adopting a new paradigm and indicates that the cyber phenomenon has intensified these gaps and the tensions to the point that the intelligence system can no longer sustain itself in its current format. Concurrently, this article points to the cybersphere as a space that enables the intelligence community to extricate itself from the intelligence cycle paradigm and develop a new paradigm. Processes in this direction are already being partially implemented, even if a complete and total concept has not yet crystallized.

48 Paul Santilli, "Applying Machine Learning to Intelligence Problems," *LinkedIn*.

Clearly, abandoning an old paradigm and adopting a new one before it has been comprehensively designed is not a simple and risk-free process. However, opting to remain rooted in the intelligence cycle paradigm apparently is also not without risks. Moreover, it seems already discernable that hanging onto the old paradigm in the cyber age will quickly lead to major intelligence failures and especially to a failure to fully exploit the enormous potential that the new era offers the intelligence effort.