Intelligence 2.0: A New Approach to the Production of Intelligence

David Siman-Tov and Ofer G.

In recent years, intelligence has undergone profound changes, both in relationships within the intelligence system and in relations between it and the political and military environment that it serves. These changes are also reflected in the practice of intelligence today and in the new concepts appearing in the discourse on intelligence, which are displacing the traditional approaches, now outdated. The developments in intelligence are the necessary result of the profound changes taking place in the human situation and in the nature of warfare in the twenty-first century. At their center is the profound change in the character of the enemy and the nature of wars and the profound change inherent in the transition from the industrial age to the digital information age. This article examines the changes that have taken place in intelligence and presents a number of problems which the intelligence community faces today. Its main argument is that intelligence capabilities can be significantly improved and brought into the twenty-first century if we adopt a new approach to intelligence that draws its main inspiration from Web 2.0.

Keywords: intelligence, Web 2.0, intelligence cycle, research collection relations, Wikipedia, blogs, research collection

In recent years, the field of intelligence has been undergoing profound changes both within the intelligence system itself and in its relations with the political and military echelons. These changes manifest themselves in the intelligence community's current practices as well as its discourse, where new perspectives are gaining attention and displacing traditional,

David Siman-Tov is a former researcher at the Military Intelligence Directorate's Institute for the Study of Intelligence. Lieutenant Colonel Ofer G. is a branch head in the Research Department.

outdated approaches. The changes in intelligence are the inevitable results of profound changes taking place in human reality and the nature of warfare in the twenty-first century. At the core of these changes is the profound change in the nature of the enemy and the character of warfare, as well as the profound change inherent in the transition from the industrial age to the digital information age.

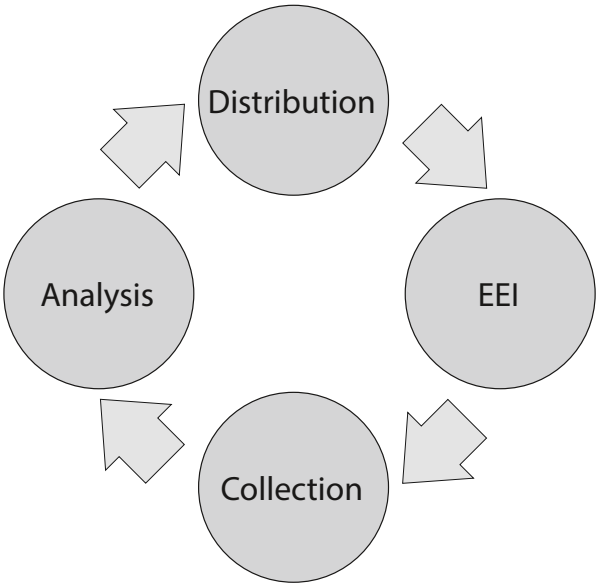
This essay examines the changes that have occurred in the production of intelligence and presents several problems that the intelligence community currently faces. The main argument of the essay is that it is possible to improve intelligence capabilities significantly and move them into the twenty-first century if a new approach to intelligence making is adopted, one that draws its inspiration primarily from the Web 2.0 phenomenon.[1]

The Intelligence Cycle as an Organizational Principle

The intelligence cycle was the major organizational principle on which intelligence institutions were constructed and around which they operated after World War II. In Israel's case, this cycle was preceded by activity carried out by individuals without an organization, without any particular method, without a hierarchy, and without any distinction between collection and analysis. Chaim Herzog, the third head of Israel Military Intelligence and the head of the intelligence department at the IDF's Operations Branch, described the situation as follows:

> At the start, there were primitive beginnings... small empires with small generals who maintained direct relations with Ben-Gurion, every one of whom ran to him with his intelligence....There were some good people [but] they lacked a military infrastructure, concepts, an analytical approach, research and working methods – collection, classification, analysis, and dissemination in a scientific manner. In other words, turning information into intelligence is a science in and of itself. We brought working methods from the [British] army and built military intelligence.[2]

The concept of the intelligence cycle identified several clear and separate stages, all of which together comprise the intelligence process: information collection, information processing (analysis), and distribution of the resulting intelligence to the various consumers. Furthermore, the process involves the commanding officer or leader extracting the so-called



essential elements of information (EEI). These steps become part of a cyclical recursive process (figure 1).[3]

Figure 1. The Intelligence Cycle

The concept of the intelligence cycle was applied with the founding of Israel's military intelligence establishment in the form of the IDF's Intelligence Branch (Military Intelligence, or MI). There, the intelligence enterprise was divided into two groups: collection agencies and analysis agencies. The collection branch (and later, the collection department) mediated between the two types of agencies with a great deal of success by providing overall direction from above while making use of the EEI, which included a limited number of carefully crafted questions. It remained for the analysts, accordingly, simply to receive the "ready-made" information; they had virtually no involvement in the work of information collection.

The rationale behind the intelligence cycle was to organize intelligence production according to clear guidelines. Compartmentalization, one of its leading principles, was not only the result of security concerns but also the result of a particular conceptualization of the work. It was meant to ensure that "everyone would do his job" and not "interfere" with the jobs of the other system components or become biased through contact with them.

Another norm stemming from the organizational principle of the intelligence cycle was the one-way flow of information: the analysts sent the EEI questions to the collectors, and the collectors sent the answers

to the analysts. There was little room for either side's involvement in the daily workings of the other.

Yet another key principle upon which the intelligence cycle rested was the so-called "value chain," which holds that the more progress is made along the intelligence process, the greater the value of the intelligence product, that is, from raw data to distilled intelligence, and from there to an intelligence assessment expressed in an analytical research document.

The intelligence cycle did not have – and did not need – any form of shared discourse or space to develop knowledge, because each of the different components of the system had its own separate and distinct job, and because the operating assumption was that every component of the system could and should do its job independently.

The separation among the intelligence system's components grew even more pronounced starting in the 1970s as a result of the Yom Kippur intelligence failure and the Agranat Commission's report, which led, inter alia, to the concept of intelligence pluralism being incorporated as a formative principle designed "to ensure the effective functioning of all members of the intelligence community to provide warning." The Agranat Commission's full report, declassified in recent years, stated that, "it is necessary to institute wide-ranging changes in the structure of IMI that will allow the expression of opposing views by analysis department personnel."[4]

Cracks in the Intelligence Cycle

In the 1960s, sectors of the Israeli intelligence community began to challenge the validity of the intelligence cycle as the exclusive organizing principle of the intelligence enterprise. For example, direct contact between surveillance bodies and operations bodies such as the Air Force and the Navy, which began in the 1960s, serve as evidence of an understanding that, at least with regard to certain threats, it was necessary to create "short cycles" between collectors and analysts. Another example was the involvement of analysts in the development and debriefing of human intelligence sources (HUMINT). But these were still the exceptions to the rule, and most of the intelligence enterprise was conducted in accordance with the division of labor described above. By contrast, in recent years, many in the intelligence community have concluded that the intelligence cycle is no longer valid as the exclusive organizational principle. Additionally, in the American

intelligence discourse there are now voices calling for the intelligence cycle to be "killed."[5] Why are these voices becoming more prevalent?

There are many causes and reasons, but an examination of the most fundamental influences reveals two historic revolutions that started at the end of the previous century. The first is the transition from the industrial age to the digital information age, manifested in the appearance of cyberspace, including the invention of the computer and the internet, which have profoundly changed human conduct. The second is the Revolution in Military Affairs in which the focus has shifted from confrontations between nations and armies to a growing range of nonconventional, non-state conflicts of a dynamic, hybrid, networked nature.

To deal with the shifting challenges of warfare, joint teams consisting of intelligence bodies and operations bodies were established as early as the 1970s (for example, the Air Force's Operations Intelligence Teams), but for many years these remained few and far between. Currently, given the frequency of asymmetrical conflicts in which the enemy can vanish into the surrounding population, the reduced window of opportunity for counteraction (a matter of minutes in some cases), and the ever-increasing challenge of minimizing harm to non-combatants, the concept of a war room that integrates all the relevant components of intelligence and operational systems – in order to complete the intelligence and operations cycle in real time – has become the standard way of thinking. This type of adjustment proves that it is possible to break organizational patterns given urgent operational needs.

On the basis of the same rationale – but in the context of intelligence challenges of a long term or infrastructural nature – a new form of intelligence structure has developed, one in which task-driven intelligence teams are built, combining all the relevant functions and capabilities (all types of collection and analysis) in order to deal with an intelligence issue in a holistic manner. Like joint attack cells, this structure also breaks organizational molds, but because these bodies operate over time rather than only during a specific operation, they pose a much greater threat to the classical organizational culture, which sanctifies compartmentalization.

Another development that has challenged the validity of the intelligence cycle is the creation of a networked log shared by all parties, which in wartime allows all participants to provide and receive updates in real time. The utility of such a log is obvious: all collectors know with great precision,

and in an unmediated form, what the EEIs are and provide immediate responses; they understand in real time the problems of concern to the analysts or operational bodies and contribute as much as they can to their resolution. At the same time, analysts receive the information they need in a timely fashion and with unprecedented exposure to the work of collection, with none of the filters or limitations typical of the principle of the intelligence cycle. The challenge to the entire concept of the intelligence cycle lies not only in doing away with the compartmentalization but also *in breaking the principle of the value chain*. The networked log is an embodiment of the understanding that, at least when time is of the essence, collected material that has not undergone organized processing and classification but arrives in real time has much greater intelligence value than canonical intelligence data that the collection unit has officially approved as fit for dissemination.

We have provided examples of tools and organizational structures already in place in the Israeli intelligence community that are recognized as being an integral and necessary part of the intelligence enterprise. These are not yet used widely enough, however, and there are still arguments over the potential for transforming them from isolated instances of shared space to a dominant facet of the overall work of intelligence.

Another fundamental reason for challenging the intelligence cycle paradigm is the information age. More concretely, one may speak of the emergence of cyberspace as the catalyst accelerating the change in two senses: one is the focus on information flow, information variety, and accessibility of information for both analysts and collectors, and the second expresses the new ways and approaches in the development and preservation of knowledge. The transition of the center of gravity in the world of information and knowledge away from institutions and into the hands of the masses (Wikipedia being a perfect example) and the appearance of blogs and social media, which as we will show later on are part of the Web 2.0 revolution, are a major factor in destabilizing the traditional method of intelligence production. They increase the tension between the way in which civilian information develops, flows, and is stored, and the outdated nature of the intelligence cycle. The new approach of information sharing and knowledge development is trickling into the intelligence community, to a great extent via the influence of the younger generation that brings to the world of intelligence the culture of information

sharing and knowledge development to which it is exposed during leisure time.

Furthermore, the nature of information collection in the cyberspace era is changing and is based more on textual information and databases than on telephone conversations using jargon intelligible only to collectors. In light of the complexity and scope of information available in this world, collection can no longer handle the raw materials at its disposal by itself; *a much stronger, richer and more profound connection is needed between collection and analysis*, with a focus on joint study and action in order to cope with the ever-growing challenge.

Similarly, technological and economic issues that surface in intelligence material underscore the advantage of having analysts who specialize in these fields and the need for their assistance in fully extracting potential information. At any rate, given the enormous volumes of information, collection efforts will flounder unless they incorporate analysis in order to separate the critical from the peripheral.

In short, the clear line between collection and analysis is blurring. Slowly but surely all participants in the intelligence system are becoming partners in the same task. It should be strongly emphasized, however, that the lines between the intelligence system's components have not disappeared altogether. Each side must retain its professional uniqueness in order to bring its added value to the overall endeavor. But each side must devote more time to getting to know the other side – its partner in the intelligence system. Analysts must become better acquainted with the uncertainties and capabilities of collectors, while collectors must become better acquainted with the uncertainties and needs of analysts.

With the emergence of cyberspace, new tools and methods were quickly integrated into intelligence production. Nonetheless, it appears that the intelligence cycle has not yet been broken and, in fact, continues to serve as the main organizational principle. For example, information items and reviews started circulating through automated systems such as email rather than being disseminated as hard copy, as had previously been the case, so as to shorten dissemination time, expand the list of recipients, and improve the ability to preserve information and retrieve it later. Yet the concept of unidirectional transmission of information from one component to another remains entrenched, and does not allow for the creation of a shared space to preserve and develop intelligence knowledge.

Another major difficulty is the inability to connect information systems of different organizations. These systems were built as closed loops, as there was almost no need for integration connectivity between them. The unfortunate result is that while connectivity within units has improved, connections among them are still minimal. The attempt over a decade ago to establish an intelligence network at IMI was not very successful; this network was secondary at best; it was not the main workspace, nor does any intelligence information develop on it.

Starting in the early 2000s, an attempt was made in the IDF to apply tools and methods of information management and development. In hindsight, these may now be called Web 1.0, and they included organizational and topical portals, various forums, and working rooms. The goal of the new tools and patterns was to manage intelligence information and create intelligence information communities, but almost every such attempt ended in failure: the portals that multiplied like mushrooms after the rain were closed one by one, becoming virtual tombstones. The intelligence forums and working rooms remained desolate and static. No new knowledge was produced in them, and before long they did not even serve to preserve current information. MI's attempt to adopt new tools for information management and preservation failed. The gap between the impressive vision of the project in its early years – "the creation of intelligence communities producing information and knowledge" – and reality was woefully large.

Among the causes of this failure is presumably the lack of any conceptual change in advance of the technological initiative. If no unit deems it is necessary to operate in a networked way with other units on a daily basis, then communities of knowledge, which are essentially the connections among different bodies, are unlikely to emerge. Furthermore, no attempt was made to translate or interpret the external tools that had been brought into the unique and truly distinctive world of intelligence.

Notably, difficulties in integrating and the failure to integrate civilian information systems and applications from the world of Web 1.0 into organizations are not unique to the intelligence community. In an essay analyzing the failure of portals in other organizations, the author argues that among other reasons one may point to organizations' failure to give heed to the social network of the workplace and to organizations' creation of a unidirectional platform of communications that ignored the

opportunity for consumers – namely, the employees in the workplace – to contribute contents of their own to the portal. In addition, many of the failed portals were constructed uniformly, not allowing users to create a homepage based on their personal needs and desires.[6]

Web 2.0: Cultural and Conceptual Innovations

Web 2.0 is a technological and socio-cultural phenomenon referring to the second generation of internet products and services. While the first generation, or Web 1.0, focused on websites whose contents were created by webmasters and where the flow of information was unidirectional, from the producer to the consumer, the second generation refers to websites as an infrastructure for the joint creation of contents relying on information sharing and user creation. The revolution within this phenomenon is more cultural than technological, whereby the ordinary user is transformed from a passive consumer of information to an agent of its creation. Control is no longer in the exclusive hands of the media and institutions but has been handed over to the people, creating a hitherto unknown democratization of knowledge. It was absolutely fitting that the *TIME Magazine* voted the internet user as its Person of the Year in 2006.[7]

Thus, *Web 2.0 is the technological infrastructure for sharing and creating contents by the users themselves amongst one another using the social media*. Web 2.0 expresses the idea of the "prosumer" (producer + consumer), a term coined by Alvin and Heidi Toffler.[8] It represents the rise of the new economic element: consumers who are involved in the production of the services and products they consume. It also expresses the notion of the "wisdom of the crowd" via technology and a collaborative approach by which individual contributions add up to the development of knowledge of a scale and quality that could never have been created otherwise. A salient manifestation of this phenomenon is Wikipedia, which is not merely an online encyclopedia but rather the collaborative effort of users who create its contents.

Another concept relevant to the Web 2.0 revolution and manifesting its inherent social changes is the Y Generation, the current generation born into the internet revolution and experiencing the rapid changes it entails. This generation is characterized by the ability to adapt to rapid technological changes, work as a team, multitask, and make extensive use of social networks as a primary means of making contacts and transmitting

contents. Unlike the previous generation, which made do with email as an alternative to traditional mail, members of Generation Y prefer Facebook as the platform for transmitting messages in various ways.

Web 2.0 is also characterized by a rich and varied user experience, with laptops, smartphones, tablets, and the like, alongside new and continuously changing ways of transmitting messages, from blogs to Twitter, which allows yet another form of contact based on followers. Add to all of these the concept of serendipity, which the internet facilitates and fosters. Often internet surfers receive unsolicited friend requests from people likely to interest them, or their attention is directed to items likely to be of value to them without actively having looked for them. This is radically different from the question-and-answer approach embodied by the intelligence cycle.

Intelligence 2.0

The Principles of the Intelligence Net

This section will describe how a relevant interpretation and implementation of Web 2.0 can provide a response to the problems currently afflicting intelligence. Clearly there is no magic remedy, and the approach suggested here does not stand on its own. Rather, we propose an examination of its application to the world of intelligence, while offering an interpretation that will tailor our suggested approach to the uniqueness of that world.

The first adaptation necessary is the prerequisite of applying the Web 2.0 concept differently in the two working environments of intelligence – the internal intelligence environment and the external environment in which intelligence is a central participant. The intelligence environment includes many different knowledge communities. Some deal with a specific enemy (such as Hizbollah or Iran), some deal with a specific sector (such as Lebanon and its power players), and some deal with weapons threats or technological threats and the like. The internal intelligence environment comprises several partners – the collectors and analysts at MI and the intelligence community, including the Mossad and Israel's Internal Security Service. By contrast, the external environment includes a long and varied list of planning and operations bodies in the IDF and the political system (such as the National Security Council staff and government ministries) as well as certain civilian research institutes. Within the internal environment, intelligence is mainly focused on obtaining information and developing

knowledge about "the other," on the basis of an understanding of the needs of the external environment. In the external environment, intelligence aids the processes of formulation, planning, and execution, by means of the information it obtains and the knowledge it develops.

The organizational principle at the core of the Intelligence 2.0 concept is that of a shared, networked space of intelligence. Instead of a hierarchic, compartmentalized division of labor, we suggest adopting a shared, networked intelligence space and dynamic, evolving intelligence communities of knowledge. This is a shared space on several levels: a shared space for analysts and collectors working together to develop knowledge about the enemy, a shared space among various research units in order to enhance their understandings using a single infrastructure, and a shared space for the intelligence community and the communities using the intelligence (the intelligence "consumers," the technological knowledge community serving intelligence, and more). In the new shared space, the sharp distinction between producer and consumer blurs. All sides – analysts and collectors, the intelligence producers and the intelligence consumers – become partners within new communities of knowledge that share a single goal: the development of applicable knowledge for the benefit of political and military endeavors, without attempting to displace one another and while retaining all professionalism and discipline-specific expertise.

Suggesting a shared networked space as a new foundation for intelligence production does not conflict with the creation of shared physical spaces for intelligence units, whether in ad hoc locations for a specific operation (a shared command center for analysts, collectors, and operatives) or in shared production and research rooms for analysts and collectors to deal with a designated mission or for routine work. In this essay we do not discuss the possibility of shared physical spaces, which is worth exploring further as another significant factor affecting the work of intelligence.

Calls for the creation of a shared intelligence space are gaining ground in the current discourse. But it seems that in the context of this discourse, one fact is being overlooked: shared spaces, by virtue of their very nature, blur the lines between the various participants, especially among the various research bodies, thereby undermining the pluralism principle. Should the pluralism principle be put to the test of time, we will likely

find it has not made any significant contribution to intelligence or to the prevention of errors and surprises; on the contrary, it has contributed only to isolationism and unhealthy competitiveness in the Israeli intelligence community.[9] Moreover, given the mass quantity and complexity of the challenges currently facing intelligence, the constraining paucity of resources, and above all the complex, hybrid, networked nature of many of the threats (global jihad is a good example), one must reject the pluralism principle and prefer unification of all intelligence efforts.

It is not necessarily the case that the networked approach to intelligence would abolish the pluralism principle; in fact, it may endow it with a new interpretation as well as better and more meaningful applicability. The recommendations of the Agranat Commission about the need for a multiplicity of opinions and transparency of information can be implemented through shared networked spaces. These spaces would reflect all intelligence information and provide better opportunities to express and present divergent opinions among intelligence personnel within the same organization or among intelligence personnel in different organizations representing different perspectives. Consequently, the proposed approach of a shared knowledge space would enhance the intelligence discourse and easily accommodate a platform for dissenting voices, intelligence debates, conflicting theses, and different stances and interpretations, while reducing the current duplication of work by fellow analyst groups.

Another key idea at the core of the new space is discourse, that is, the willingness of members of the knowledge communities to participate and share their insights. To a great extent, discourse is an alternative to the EEI paradigm, which for many years has not been serving its purpose. Discourse platforms created by Web 2.0 are likely to allow analysts and collectors to hold intimate discussions of their work, in real time *and* on a continuous basis. An analyst receiving a new report from a collector would be able to refer to it or ask for clarifications in close to real time. The collector would learn if the information provided to the community was helpful or not and would be able to supplement it with additional information that could not be included in the official framework of canonical intelligence data as currently disseminated by collectors' units.

A sequence of such responses − the transition from EEI to discourse − is an important foundation for examining the success of the knowledge community. A state in which community members do not feel comfortable

being exposed and do not respond to one another's input would signify a possible failure in the way the discourse was constructed in that space, and the discussion leaders would have to take steps to solve the problem. It is essential that there be leaders of the knowledge community responsible for advancing the processes of knowledge development.

By implementing the idea of Intelligence 2.0, a fundamental change would occur in the retention of organizational knowledge and in the creation of an organizational memory. At present, knowledge that does not make it into official documents is lost. Most of the informal discourse is carried out through email, but it is not systematically stored and its potential to serve as an organizational asset is simply wiped out. Personnel who have held important positions over many years in the organizations are focal points of organizational knowledge. When they leave, the information in their heads and the materials accumulated and developed on their computers, simply vanish. These are organizational assets of the highest order, but they are not defined as such, and there is currently no attempt or means to preserve them. In the new approach we propose, the great emphasis placed on processes of internal discourse would allow the system to distill, reveal, and make accessible all the informal knowledge contained in the minds of intelligence personnel who are themselves knowledge focal points. They would be offered an opportunity to share personal insights and databases that they stored on their personal computers in a systematic, regular manner, as a matter of routine organizational activity.

Key Tools in Implementing the Approach

Having examined some of the major conceptual aspects that could characterize the Intelligence 2.0 approach, we will now present some of the essential tools of the world of Web 2.0 and examine the adaptation they would require for the world of intelligence.[10]

Within the shared intelligence space, it is possible to create an "Intelligence Wikipedia" accessible to all members of the intelligence community, who would also be partners in its constant revisions and updates. In this Wikipedia it would be possible to post updated analytical entries about the enemy as well as organizational information about intelligence doctrines and philosophies of use, various working plans, and intelligence projects.

Clearly this endeavor would require the formulation of rules that differ from those used in the civilian sector, where the wisdom of the crowd provides the foundation for Wikipedia's existence. By contrast, the wisdom of experts (individuals or small groups) would serve as the Intelligence Wikipedia's foundation. But the few experts in each field would be able to learn from one another and present the information and knowledge they have in the same Intelligence Wikipedia entry so as to create the fullest picture possible of the subject instead of competing with one another. Unlike Wikipedia, updates in the Intelligence Wikipedia would not be a voluntary or optional exercise, but would be incorporated into the guidelines and new job descriptions of the organization and would constitute a key obligation of the authorized editors. Another salient principle of the internet that is unsuited to the intelligence environment is the principle of anonymity, because in the intelligence environment great importance is attached to knowing who is responsible for a particular insight in order to enable clarifications and updates from the same individual.

Parts of this Intelligence Wikipedia would be available within the space that is shared by the world of intelligence and consumers outside of this world, but within that space it would not be possible to change the entries. That is to say, the Intelligence Wikipedia would be able to serve as a generic, accessible knowledge base serving members of the intelligence community as they prepare intelligence products, and these intelligence products could in turn serve as a knowledge base and could be updated via Intelligence Wikipedia entries. The updating of finished products as entries in the Intelligence Wikipedia could also enhance the timeliness of intelligence knowledge. That is, unlike the present situation, in which some of the information within an intelligence review quickly becomes outdated (but not to the extent that the entire review requires updating), the Intelligence Wikipedia would allow the review to be kept current because any corrections or updates could take place in real time.

In the shared space, blogs would serve as a central tool that some participants could use to record their personal insights in a continuous, timely manner. But unlike the situation in the civilian internet, it would be inappropriate to allow anyone in the intelligence community to start a blog without restrictions, guidance, or oversight. It might be necessary initially to limit the organization's network of blogs to include only the organization's knowledge focal points and senior personnel. Some of the

veteran intelligence personnel have a great deal of unique knowledge – musings on methodological issues, insights regarding intelligence issues resulting from many years of service, personal experiences of intelligence events with doctrinal value, and more – that has no room for expression in the usual official products. Similarly, there are senior personnel who would like to be able to transmit, frequently and informally, their perspectives on processes in the organizations for which they are responsible and suggest directions for continued action. Blogs could serve as an ideal platform for these people and allow them to put their insights into writing.

One of the most important and promising directions that the Web 2.0 era can offer intelligence is the establishment of a social intelligence network,[11] which in the future would serve as an advanced alternative to organizational email. Organizational email, adopted as a main working tool in the IDF and MI in the early 2000s, was designed to transmit messages amid an organization's personnel. It was not meant to be a technological platform for the construction of knowledge, but in the world of intelligence it became one nonetheless, because of the great need for such a tool and the lack of an alternative. The use of organizational email for sharing and developing knowledge is rife with problems and drawbacks: for technical reasons and because of issues of compartmentalization, it is impossible to transmit a message to all appropriate addressees; it is impossible to carry out discussions over time (the shelf-life of an email discussion is short); email messages do not appear in a user's inbox according to any rational order of classification by intelligence issues, but rather in a uniform, undifferentiated list (alongside a great deal of junk mail); and, worst of all, it is impossible to save email messages systematically, meaning that the knowledge developed through them is lost.

The broad integration of social media would mark a profound revolution in connectivity among individuals in an organization and create living, dynamic knowledge communities that would serve as critical infrastructure for any future intelligence organization. Thus, instead of providing only the members' names, telephone numbers, and job descriptions (the current situation in non-social organizational networks), the social network would allow one to become acquainted with the organization's individuals the way Facebook allows one to form acquaintances in the civilian sector. Every individual would be able to define the relevant colleagues ("friends") and follow them and any new contents they may post to the network.

Moreover, the profile of every user would automatically, as well as through manual input, include areas of expertise and interest (as a consequence, for example, of jobs held and academic, military, and intelligence training) and official and unofficial publications and writings. By assessing these criteria, the system would be able to suggest appropriate contents as well as invite individuals to participate in certain online discussions and knowledge communities likely to be of interest, which they would not otherwise have discovered. Similarly, using the same criteria, other friends on the network would be able to locate this individual and request assistance, whether through a proactive search or through the system's capacity for suggesting introductions and sharing profile contents.

Another fundamental change inherent in Intelligence 2.0 would be the ability, which does not exist today, to hold asynchronous discussions, that is, long-term, discontinuous discussions of an issue. A culture of debate that does not require everyone to be available at the same time is a good approach to adopt not in order to replace physical meetings but as a necessary complement that provides added value. For example, embassy staff in the United States or India would be able to participate in a discussion about the country in which they are serving, and members of the intelligence knowledge communities located at opposite ends of a country would be able to meet. Individuals would also be able to contribute to a discussion that took place several months earlier but is still relevant.

One can develop this idea further and propose that discussion groups on the social network (knowledge communities) be officially designated as the primary organizational configuration for joint intelligence mission teams. At present, the notion of joint mission teams is suspended between two alternatives, neither of which is ideal for classical intelligence organizations. On the one hand, there is the model of a joint mission team functioning on a part time, limited basis, with members who participate while also fulfilling a host of other functions. Consequently, the joint mission team holds team member meetings only once every few weeks or months, and the processes of learning, sharing, and knowledge development take place in a very limited way because of time and information systems constraints. On the other hand, there is the alternative of the joint mission team whose mandate constitutes the only mission for its members, who work together in a shared physical space.

Conclusion

In this era, competition over learning is becoming a central battlefield, and intelligence organizations must become institutions that can quickly learn and adapt to changes occurring in their sphere of activity. Incorporating the concept of Web 2.0 into the intelligence enterprise, with relevant interpretations and modifications for the intelligence environment, has the power to generate a revolution that could fundamentally change the relationships among the various intelligence organizations, and between them and their consumers. This approach can endow working processes with the interconnectivity, synergy, flexibility, and speed that are critical in confronting the dynamic challenges and hybrid enemies of the current era.

Implementing the new approach entails serious difficulties and challenges for a variety of reasons. First, the approach would seem to contradict the intelligence traditions of secrecy and compartmentalization, on the one hand, and of competitiveness and pluralism, on the other. A culture in which "knowledge is power" and where sources and information are only revealed on a strict need-to-know basis will find it difficult to change abruptly and work according to the new guiding principle that "sharing is power" and sources and information should be disseminated on a need-to-share basis.[12]

Another significant difficulty, an offshoot of the above, is the lack of technological connectivity among intelligence organizations, not to mention between them and their consumers. The reality is one of network isolationism, the result of a long tradition of compartmentalization, differentiation, and competition among the components of the intelligence community, stemming in part from the guiding rationale of the intelligence cycle. The connectivity sought refers not merely to email (which also does not always exist), but rather to the creation of a shared network space that would allow the development of shared knowledge and a knowledge base to which everyone is a partner.

A further problem that sometimes prevents organizations in general, and intelligence organizations in particular, from adopting social media into their organizational midst is the organizations' fear of the creation of a new type of knowledge. This fear stems from veteran personnel's concerns regarding the new technology and the philosophy it represents and from concerns that communication through a social medium will distract the individuals in the organization from their tasks. Indeed, it should be

underscored that implementation of a social network in the intelligence world is liable to generate tension between the chaotic nature typical of civilian internet surfing and the need for focus and mission-driven action in the intelligence world. How can one optimize the use of a social intelligence network in order to take full advantage of its unique features while also circumventing the problems that these very features pose for the mission-driven nature of intelligence?

Yet another significant challenge, illustrated by the American experience,[13] is the possibility that the new tools for creating contacts and transmitting messages among members of the intelligence communities, and the tools for saving and developing intelligence knowledge, will turn into additional secondary tools among the organizations' information systems. If that happens, not only will the new tools fail to serve the development of intelligence knowledge, they will in fact create duplication and prevent the social intelligence network from becoming the primary space in which organizational knowledge is kept and developed.

Meeting these challenges consists of several steps. Most importantly, it is critical to define the social intelligence network as the organization's primary operational working environment. This is the tool the intelligence community must use to communicate better internally and with external agencies that could, to a limited extent, be incorporated into it. Thus, an intelligence version of Facebook would serve, inter alia, as the workspace of mission-driven teams, and the Intelligence Wikipedia would be the place for retaining knowledge in the system. Processes of preparation and authorization of intelligence products would also occur in the new shared space.

A networked space based on the Web 2.0 concept must be effective and offer value-added elements for information management. To this end, it is necessary to make sure that all of the organization's information sources and knowledge assets be concentrated and available in this space, while giving more advanced options both to preservation of information and knowledge and to access to them (integrating and incorporating contents, document and file sharing, connections to external systems, access to databases, robust retrieval services). As groundwork, a true revolution in the field of inter-organizational information systems and connectivity is needed. The creation of shared spaces will be possible only

if standardization occurs so that different systems can communicate with one another.

Beyond this, there is a need for a profound cultural and conceptual change, similar to the understanding that developed in the American discourse. Incorporating new technological tools is not enough. The change must also entail training and the institutionalization of new professions. Furthermore, there must be a doctrinal review of the development of intelligence knowledge, leading to a revamping of outmoded organizational processes and an end to patterns that only serve to reinforce inter-organizational isolation and competition.

There are several proposals in the current American discourse for pulling the intelligence wagon out of the rut in which it is stuck. Especially noteworthy is the "Living Intelligence" approach developed by the National Geospatial-Intelligence Agency (NGA), which calls for changing the old culture, habits, and patterns of intelligence production.[14] The innovation of this approach is its call for viewing social media as the primary working environment of the intelligence community. In other words, the approach is chiefly concerned with intelligence products and suggests making intelligence products, their production processes, and their manner of presentation networked and social. The approach also calls for creating integrated intelligence products, thereby significantly reducing the overlap and duplication currently typical of intelligence organizations.

Another component critical for increasing the likelihood of success of such a transformation is a command model that differs from the classical, hierarchic model that views the change as a process to be initiated primarily from above. The new model must also allow for managed chaos, while adopting and embracing the younger generation joining the intelligence community as leaders of change. Members of this generation started communicating on social networks long before their recruitment. They need only be allowed to maintain their habits of sharing their environment, to be reinforced without becoming entrenched, and to be granted the tools to which they are accustomed for the sake of sharing and creating knowledge. All of this must, of course, occur in the context of a dialogue between the networked command model and the classical model, in order to find the golden mean between the need for innovation from below and the necessity of segregating those areas of production where the allocation

of responsibility and authorization of intelligence products are essential principles.

The organizational and institutional fear of incorporating social media as a way of communicating and creating knowledge is understandable, but it is liable to be the major hindrance to creating networked, cross-organizational intelligence communities. Efforts to limit the ways in which individuals in the community can contact one another will not succeed; individuals will simply turn to the civilian social media to do so, and the intelligence network will remain secondary at best and duplicate processes at worst. Importing social media into the intelligence community will generate the Intelligence 2.0 revolution and enable the entire intelligence endeavor to take a giant stride forward.

Notes

1 This essay was first written and distributed within IDF Military Intelligence in 2012. Since then, as part of a fundamental organizational and conceptual change spearheaded by the head of IMI, some of the core concepts articulated herein have already been applied. The authors would like to thank Gur A. and Tal G. for their significant contribution to the learning process that was the framework for this essay.

2 Chaim Herzog, cited by Zehava Ostfeld, *An Army Is Born* (Tel Aviv: Ministry of Defense Publishing House, 1994), p. 333.

3 Israel Military Intelligence, *The Process of Intelligence Work*, IDF Archives, 1956. A copy of the booklet is preserved at the Institute for the Study of Intelligence at MI and kept at Training Base 15.

4 See the full report of the Agranat Commission investigating the Yom Kippur War at the IDF Archives site, pp. 160 and 168, http://www.archives.mod.gov.il/.

5 Kristian J. Wheaton. "Let's Kill the Intelligence Cycle," *Sources and Methods*, May 20, 2011, http://sourcesandmethods.blogspot.com/2011/05/lets-kill-intelligence-cycle-original.html.

6 Shani Avnet, "Empowering Information Portals through User Experience," Netwise Ltd. The PowerPoint presentation is available at http://api.ning.com/files/x6R-TdDcUc0aH8798ORM5OWlq3G5G-1lnmXkOaf1WI8dFFg7BwS1RyyeiOuO7tCvYtSUlTTqOn2M-kjH8EJ5cGbX6OI1A2rt/file.pdf.

7 *TIME Magazine*, December 25, 2006, http://www.time.com/time/magazine/article/0,9171,1570810,00.html.

8 Alvin Toffler, *The Third Wave* (William Morrow, 1980); see also Alvin and Heidi Toffler, *Revolutionary Wealth* (New York: Doubleday, 2006).

9 Shmuel Even and Amos Granit, *The Israeli Intelligence Community: Where To?* Memorandum No. 97 (Tel Aviv: Institute for National Security Studies, 2009), p. 47.

10 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.

11 A social intelligence network was constructed in MI about two years ago and is being used by thousands of intelligence personnel – collectors and analysts – as a central system for intelligence production.

12 David Schroeder, "Efficacy and Adoption of Central Web 2.0 and Social Software Tools in the U.S. Intelligence Community," American Public University System, March 2011, http://www.academia.edu/1443504/Efficacy_and_Adoption_of_Central_Web_2.0_and_Social_Software_Tools_in_the_U.S._Intelligence_Community.

13 Ibid., p. 2.

14 Chris Rasmussen, "Toward Living Intelligence," Gov 2.0 Expo Showcase, Washington D.C., September 8, 2009, http://www.gov2expo.com/gov2expo2009/public/schedule/detail/10599. See also the YouTube video at http://www.youtube.com/watch?v=XdQPuTVDOH4.