THE INSTITUTE FOR THE RESEARCH OF THE METHODOLOGY OF INTELLIGENCE
ISRAEL INTELLIGENCE HERITAGE & COMMEMORATION CENTER (IICC)

Open Intelligence: A new framework for relations between intelligence organizations and the civilian Sphere

Ofer Guterman[1]

March 17, 2023

Tear down the walls see the world,
Is there something we have missed
Turn from ourselves, look beyond
There's so much more than this
(Tear Down the Walls, Joel Houston and Matt Crocker)

Overview

Intelligence organizations around the world are undergoing significant changes, shifting in accordance with the sea changes in the environment in which they operate, and one of the most important changes concerns the unprecedented openness to the civilian shpere. However, this paradigmatic change lacks a systematic and holistic presence in professional and academic writing on intelligence.

The objective of this article is to propose an integrative conceptual framework for what can be called "open intelligence." It has five interactive components: intelligence dealing with issues of national security that concerns global civilian threats which go beyond the security-military sphere (such as climate change and public health); intelligence-civilian partnerships in collection activities, analysis and operations conducted in the digital realm, necessitated by the OSINT (Open Source Intelligence) revolution (prominently displayed in the war in Ukraine); need for intelligence organizations to embed themselves within the civilian STEM-ecosystem in order to preserve technological superiority; obligation to share information and intelligence assessments with the public in an era of fake news and truth decay; and movement towards human-capital strategies more symbiotic with the public sector and the private labor market.

The process of opening up to the civilian sphere must continue and deepen to provide a vital growth engine for intelligence organizations, but to succeed it must cope with its inherent challenges: developing a more sophisticated secrecy culture and moving the needle in sources and methods risk management; internalizing the loss of monopoly on intelligence and the need to turn to external partnerships to maintain relevance; managing possible tension with the political decision makers, who are liable to view intelligence sharing with the public as a violation of their monopoly on the consumption of intelligence information; clarifying ethical and democratic dilemmas arising from relations with the civilian sphere; and coping with the possible reservations of civilian parties regarding working with the intelligence organizations.

[1] Ofer Guterman (PhD) is a senior research fellow at the Israeli Institute for the Research of the Methodology of Intelligence.

Introduction

The 21st century marks humanity's entry into the fourth Industrial Revolution,[2] the digital information revolution, characterized by a series of technological sub-revolutions in fields such as artificial intelligence and machine learning, the Internet of things, automation and robotics, cyber and Cloud services, 3D printing, biotechnology, nanotechnology and quantum computing. Such dramatic technological revolutions lead to equally dramatic changes in many other areas of life, from the economic structure to the social and political order, to the most basic aspects of identity, values and human culture.

The intelligence organizations are in the eye of the storm of this historical revolution: first, because intelligence work processes are inherently tied to information and technology, and second, because intelligence operates within the wider world – its subjects of interest and the objects of its operation and analysis are the same world that is changing before our very eyes.

It is therefore clear that the intelligence establishments cannot avoid the changes experienced by the world around them. Rather, they have to spearhead the understanding of the directions humanity is taking, both to better describe them for intelligence consumers and decision makers, and to enable intelligence organizations to carry out internal transformations and adapt to the changing world.

Western intelligence organizations recognize the aforementioned processes, and in recent decades have begun making significant changes. Public statements by senior intelligence officials reflect the understanding that change cannot be confined to the technological dimension, but rather requires **a rethinking of the entire intelligence value chain** – the consumers served by intelligence organizations, their missions, the sources, tools and methods that will enable them to meet their tasks, and the people who carry them out.[3]

Moreover, it follows that the central change intelligence organizations have to make, relates to their relations with the external civilian sphere. The trajectory of the change has to be opening up and creating mutual ties with civil society and the business sector in a way that is unprecedented and revolutionary vis-à-vis the intelligence culture of seclusion and secrecy.

---

[2] Klaus Schwab (December 12, 2015), The Fourth Industrial Revolution: What it means and how to respond, *Foreign Affairs*; Sam Trendall (December 5, 2018), MI6 chief calls for tech-enabled 'fourth-generation espionage', *CSW*.

[3] Matt Alderton (April 24, 2022), CIA Deputy Director for Digital Innovation: 'Innovate or Perish', *Trajectory*. Jeanne Chirop (June 23, 2015), NGA director challenges partners to join in 'new power' of GEOINT, *NGA*.

The foregoing is evident in a number of fields: the intelligence organizations' partnering with the private sector, especially with regard to technology; the rising importance of OSINT created by civilians for civilians; the increase in intelligence organizations' involvement in civilian issues which are important for national security, especially the COVID-19 pandemic and climate change; the worsening foreign and local threats of misinformation and disinformation in recent years, which gave rise to the question of whether, as part of its struggle for the truth, the intelligence community has a commitment to share intelligence information and assessments with the public.

However, professional and academic writing on intelligence lacks a systematic and holistic reference to the issue of the interrelationships between intelligence organizations and the civilian sphere. Thus, the objective of this article is to connect the dots and propose a framework for what can be called ***open intelligence*****, a term to illustrate the intelligence establishment's need to change the paradigm of how it relates to the civilian** sphere.

The integrative framework proposed here has **five interrelated components**: civilian Priority Intelligence Information (PIR); partnerships in collection activities, analysis and operations in the digital dimension; a rising obligation to share intelligence assessments with the public; partnerships in technological power building; and the management of human capital through more flexible boundaries with the civilian sphere.

Expanding the scope of national security and its implication for national intelligence

Priority Intelligence Information (PIR) define the topics of collection and research for intelligence organizations. Historically, PIR was focused on military and political issues. In modern times, the intelligence organizations which developed during the World Wars served the wartime objectives of the countries in conflict. Later, PIR expanded to include issues of diplomatic and foreign affairs (for example, waging the Cold War). During the past decades, pir expanded beyond the classic realm of war to deal with asymmetrical threats, especially the threat of terrorism, and later with cyber threats. Yet still, the changes occurred within the paradigm that regards intelligence as serving national security in its narrower sense.

Thus, for example, *national security*, according to the *IDF Dictionary of Terms*, means: "(1) A situation which assures a national capability to deal effectively (in all possible circumstances) with a threat to national existence and interests. It is manifested by the following: a clear military advantage over any

foreign entity, the assurance of the capability to deal with foreign entities which threaten (or potentially threaten) the nation, the state or national interests; a sufficiently strong position in the international arena, comprehensive security capability that can successfully deal with any internal or external overt, covert, hostile or destructive activity; (2) The government's comprehensive national-political effort undertaken with the participation and oversight of the Knesset, to create a situation of sufficient national security." [4] The Israeli National Security Council Law defines its role as "the council for the prime minister and government for foreign affairs and the security of the State of Israel."[5] The American idea that led to the establishment of the National Security Council (NSC) also conceived of national security in terms of foreign affairs and security.[5]

Today, **the time has come to recognize that military threats to national security are a central but only one component of a wide spectrum of significant threats**.[6] An expression of this can be found in the American NSC's current definition of national security: "Today's challenges demand a new and broader understanding of national security – one that facilitates coordination between domestic and foreign policy as well as among traditional national security, economic security, health security, and environmental security."[7]

Therefore, national intelligence PIR in the service of national security has to include significant work on global and civilian issues which influence national security. That argument, which only a few years ago would have seemed revolutionary and radical, has today become more acceptable in the wake of the COVID-19 crisis and the outbreak of natural disasters and other consequences of global climate change. These threats are expected to increase in the coming years, and intelligence organizations are examining how to join national efforts to meet them.[8]

The rise in civilian PIR may cause genuine dilemmas for the intelligence community's borders and architecture. Do intelligence communities need to accept responsibility for civilian PIR, which do not deal with enemies and are based on information which is overt and readily available? Are intelligence

---

[4] IDF (1980), *Glossary of IDF terms*.
[5] Government of Israel, *National Security Council Law*, 2008
[6] Eilon Avra'am (1980), National Security, *Monthly review* number 3-4, pp 6-22.
[6] Ofer Guterman (2020), Israel's Need for Information and Knowledge in Civilian Areas of Interest, *Intelligence in theory and in practice*, No. 5 (National-Civilian Intelligence – Approaches and Ideas for Implementation in Israel).
[7] National Security Council, *The White House homepage* (ret. 27.12.2022).
[8] Jessica Shannon, Catherine Jones & Ingrid Carlson (n.d.), Rethinking national security in the wake of COVID-19, *PWC*; Scott Gottlieb (September 17, 2021), Intelligence agencies can help stop future pandemics. Here's how; *The Washington Post*; Miriam Matejova & Robert Weiss (March 17, 2022). Disaster intelligence: developing strategic warning for national security, *Intelligence and National Security*; Michael Birnbaum (January 2, 2023), Why the US is enlisting a spy agency during hurricanes, *Stars and Stripes*; Anthony Albanese to order intelligence chief to examine security threats posed by climate crisis, *The Guardian*.

agencies capable, from the point of view of their organizational culture and resources, of dramatically changing and expanding to enter new, broader fields of responsibility? Will they be able to navigate between dealing with those topics and preserving the quality of the response to traditional security PIR? Or should the intelligence communities reject calls and pressure to deal with civilian PIR and hone their unique capabilities in the military-security field, leaving civilian PIR to the country's other apparatuses and mechanisms? Or perhaps the right direction to take would be to develop a national ecosystem approach for national security intelligence, one that is more flexible and open, within which intelligence organizations would manage different levels of cooperation and interaction with other agencies in the government sector and civilian society, and deal jointly with interests common to both.

A telling test-case was the COVID-19 crisis in Israel, during which the various intelligence organizations, each according to its unique capabilities, joined forces in a national effort to combat the pandemic. At the height of the pandemic, Israel's Military Intelligence Directorate established The National Center for Information and Knowledge to Combat COVID-19 to provide an immediate response to bridge information gaps and the needs of the ministry of health. IDF intelligence analysts, with their methods of collecting and analyzing data (and using their mass of personnel), worked together with ministry of health experts, providing insights and giving recommendations for a national policy to combat the disease. Today, with the crisis over, and after the public health system has assimilated the need for such an information enterprise and the principles for operating it, the ministry of health is working to replace the Intelligence Directorate's center with a permanent civilian one.[10]

It seems that solutions to the dilemma will vary from country to country according to political and intelligence cultures. They will have to face different challenges, from the concern in democratic countries regarding the involvement of intelligence organizations in civilian matters, to a concern regarding damage to the focus and quality of the intelligence organizations' response to its traditional military PIR. One way or another, the new problem necessitates a new national mindset for how the traditional intelligence establishment, fashioned in the 20th century, relates to the issues of national security in the 21st.

[10] Ido Efrati (July 14'th, 2022), IDI's Center for Information and Knowledge to Combat COVID-19 will be closed, its tasks will be transferred to the Ministry of Health, *Ha'aretz.*

Leveraging the OSINT revolution for open digital intelligence-civilian cooperation

The extent and availability of OSINT (open-source intelligence) are growing exponentially and have revolutionized its importance to intelligence. From a source whose reliability was regarded by intelligence analysts as marginal and problematic it became a source so important that intelligence organizations keep trying to find ways to use it to its full capacity.[11] Not every intelligence community has internalized the degree of change or is equally uncertain as to how to cope with the change, but all are far from exploiting its full potential.

OSINT's increasing importance for intelligence organizations is linked not only to exogenic reasons of increase in its extent and availability, but also to endogenic reasons of the rise in the importance of civilian PIR, since OSINT is the dominant, if not the only source capable of meeting the relevant information needs.

However, OSINT also creates new answers to old intelligence questions. Today, for their own reasons, media outlets, NGOs and business intelligence companies conduct investigations of armies, militias, terrorist and criminal organizations at a level often equal to and sometimes higher than those of the established intelligence organizations. The civilian investigators know (and usually better than intelligence organizations) how to extract, fuse and analyze relevant open data and information from databases, social networks, unencrypted CCTVs, Geo-locate portable devices (such as smartphones and watches), and other open sources.[12]

The war in Ukraine is a watershed moment for the intelligence organizations' internalizing the revolution in OSINT's importance and power and the need to transform the way they relate to it.[13] The war illustrates the unprecedented, massive use of OSINT in a variety of classic military intelligence ways, such as building a Common Intelligence Picture (CIP), identifying changes in enemy deployment, supporting the kill chain, exposing war crimes, spreading disinformation and waging information warfare. All are carried out using near-real time information from the extensive

[11] Heather J. Williams & Ilana Blum (2018), Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise, *RAND*.

[12] Bellingcat (December 14, 2020), Hunting the Hunters: How We Identified Navalny's FSB Stalkers; Bellingcat (July 18, 2022), Donbas Doubles: The Search for Girkin and Plotnitsky's Cover Identities; Bellingcat (February 23, 2022), Documenting and Debunking Dubious Footage from Ukraine's Frontlines.

[13] General Sir Jim Hockenhull, Commander Strategic Command (Dec. 2022), How open-source intelligence has shaped the Russia-Ukraine war, speech at a *RUSI* Members Webinar, Delivered on 7 November 2022, Published 9 December 2022; Amy Zegart (Jan./Feb. 2023), Open Secrets: Ukraine and the Next Intelligence Revolution, *Foreign Affairs*.

documentation from civilians on the ground[9] and commercial satellites,[10] along with the ability to use archived Internet databases, making it possible to cross-refence and locate current and previous relevant information.

As part of the intelligence personnel's perplexity regarding the OSINT revolution, statements such as "the end of secrets" are beginning to appear in the professional intelligence literature.[11] There are two main reasons why such a discourse does not contribute to understanding the change. One, even if classified information is trending downward as a percentage of information relevant for intelligence organizations, its singular added values remain high in intelligence domains where OSINT cannot replace it (for example, intimate information about leadership's decision-making process, or certain tactical information for operations and targeting).

Two, and more importantly, **the dichotomy behind the argument about the superiority of OSINT or classified information ignores the fact that the distinction between them is becoming blurred**. That is particularly salient in the worlds of cyber security and in data extracted from civilian sensors, from commercial satellites with powerful, state-like capabilities and from personal sensors such as smartphones and wearable equipment (the Internet of Bodies - IoB).

Therefore, the argument about the balance of power between classified information and open-source information should be exchanged for more productive discussions dealing with the common areas of open-source information which either exist or should be created between intelligence organizations and the civilian world. **That would make it possible to map, with higher resolution, the areas and ways in which OSINT should serve as the most important source** (as opposed to areas where extolling its virtues is nothing more than rationalizing faulty and missing covert collection), and to brainstorm ways to utilize OSINT and integrate it as an equal partner within the concept of All Source Intelligence.

Moreover, those sorts of deliberations will be able to transcend the idea of open-source information merely as a source, and **develop the open digital dimension as a space of civilian-intelligence**

[9] New York Times (December 25, 2022), How Citizen Spies Foiled Putin's Grand Plan for One Ukrainian City.
[10] Sandra Erwin (September 7, 2022), GAO: Defense, intelligence agencies need a better plan to buy commercial satellite imagery, *SpaceNews*; Christopher Miller, Mark Scott & Bryan Bender (June 8, 2022), UkraineX: How Elon Musk's space satellites changed the war on the ground, *Politico*.
[11] Zachery Tyson Brown and Carmen A. Medin (March 9, 2021), The Declining Market for Secrets: U.S. Spy Agencies Must Adapt to an Open-Source World, *Foreign Affairs*.

partnerships, in collection, assessment and operations. To that end, I propose four models:

- **Model A: The unidirectional flow of information and knowledge from the civilian world to the intelligence world**. To extract OSINT information, intelligence organizations cannot merely rely on assimilating Web Intelligence (WEBINT) tools and capabilities. They have to transform how they relate to OSINT, integrate it into their hybrid (on-prem and cloud) IT architecture, develop AI applications to extract unstructured open-source Big Data and turn it into processed intelligence information, know how to fuse it with classified databases and assimilate the new capabilities in intelligence processes by making the necessary structural, organizational and work-related changes.[12]
- **Model B: The unidirectional flow of information and knowledge from the intelligence community to the civilian world**. For example, the release of information for waging economic, legal and political warfare, or for cyber security. In this instance as well, the war in Ukraine provides a foundation for accelerating the public use of intelligence, illustrated by US and UK IC's publication of a large amount of information and its strategic use for waging the battle for hearts and minds against Russia, refuting Russian claims and enlisting the international community against it.[13] The challenge of this model is in the development of mechanisms for using classified information in unsterile areas and transferring it to civilian entities. The challenge comes from both the practical aspect of managing the risks of keeping secrets and the challenge of overcoming the intelligence organizations' culture of secrecy.
- **Model C: Elevating the civilian sphere as a source of new information and knowledge**. Some of the information is collected through Crowdsourced Intelligence,[14] as was recently illustrated by the extensive, proactive use made by the Ukrainian army of civilian reports as a primary source of important information regarding the movements of Russian troops. An older but equally interesting example of mass intelligence was the Hootenanny Project launched by the American National Geospatial-Intelligence Agency (NGA) in the middle of the last decade, which included the use of open architecture for uploading images from satellites and aerial photographs to the

[12] Emily Harding (January 19, 2022), Move Over JARVIS, Meet OSCAR: Open-Source, Cloud-Based, AI-Enabled Reporting for the Intelligence Community, CSIS

[13] Dylan, H., & Maguire, T. J. (2022). Secret Intelligence and Public Diplomacy in the Ukraine War. Survival, 64(4), 33-74.

[14] Shay Herskovitz (April, 2018), CROSINT – Crowdsourced Intelligence: Using the wisdom of the crowd for Intelligence needs, *The Institute for the Research of Methodology of Intelligence;* ODNI (February 8, 2017), IARPA launches "CREATE" Program to improve reasoning through Crowdsourcing; Sharon Weinberger (November 18, 2014), US intelligence agencies hope the "wisdom of the crowd" can help them predict the future.

Internet. The NGA's objective was to turn the commercialization of satellite imagery from a threat to an opportunity, and to enable scaling up Geospatial Intelligence (GEOINT) by using a platform that would allow raw material to be uploaded by various sources, enabling large numbers of civilians to quickly join the efforts to interpret it.[15]

The National Intelligence Council (NIC), which conducts research and long-term assessments for the American intelligence community, presents a different example for public cooperation in collecting information and developing knowledge, based on expert-sourced (rather than crowdsourced) intelligence. Besides the participation of academic scholars and private sector figures as members of the council, it also uses various methods (such as questionnaires and in-depth interviews), to obtain insights from civil factors such as students and NGOs around the world, as part of building its assessment of global trends for the coming decades.[16]

- **Model D: Joint operational activity in the digital dimension on common PIR**. This model surpasses the previous models and is not limited merely for transmitting information from one side to another. An outstanding example is the cooperation between governmental cyber bodies and civilian bodies and private businesses in the worlds of information and cyber security.[17] Like the cooperative mechanisms created over the past years for cyber security, it is worthwhile to examine the development of joint mechanisms between intelligence organizations and bodies in the public and private sectors and civilian society in other areas. Examples would be the entrance of GCHQ (the UK's SIGINT agency) to combat Internet crime,[18] and combatting disinformation.

A need to join the civilian STEM ecosystem to preserve technological superiority

In the past, the military-security establishment, and within it the intelligence community, was at the forefront of technology, and its internally-developed technological capabilities later trickled into civilian applications and permeated the private business sector (from the Internet to microwave

[15] Maurice Power, Brian Chiou, Norman Abrahamson, Yousef Bozorgnia, Thomas Shantz & Clifford Roblee (February 2008), An overview of the NGA project, *ResearchGate*; NGA (September 2006), Geospatial Intelligence (GEOINT) Basic Doctrine.

[16] Ofer Guterman (2021), Publications of the American intelligence community regarding threats and long-term trends - methodological insights, *The Institute for the Research of Methodology of Intelligence*; National Intelligence Council (January 2023), Join The Conversation – Tumbler Page.

[17] Sergei Boeke, Caitríona Heinl & Matthijs Veenendaal (2015), civil-Military relations and International Military cooperation in cyber Security: common challenges & State Practices Across Asia and Europe, 7th International Conference on Cyber Conflict; Cybersecurity and Infrastructure Security Agency (January 2023), Joint Cyber Defense Collaborative.

[18] GCHQ (February 24, 2021), GCHQ to use AI to tackle child sex abuse, disinformation and trafficking.

ovens). Today the scales have turned and the civilian sphere is at the cutting edge of technological development.[19] It is a historic sea change, related to the economic and political structure of capitalist societies (globalization and the growing advantage of the private sector over the public sector in financial and human capital), and to the transition to a data-oriented economy and technology, the overwhelming majority of which exists in the civilian domain.

The change is one of the most dramatic disruptions the security establishment has undergone in modern history, and to a great extent, if not entirely, it is relevant to every aspect of the information technology used by the intelligence community: sensors, accumulating and storing data, computing and processing capabilities, algorithms and applications.

In this brave new world, intelligence organizations are forced to pursue the private market and use different kinds of mechanisms for cooperation and public-private sharing to keep up with changes and preserve relevance:

1. **Import**: One of the mechanisms is to import civilian R&D activities and capabilities, to be carried out in-house, behind the intelligence walls. For example, IARPA (The Intelligence Advanced Research Projects Activity, subordinate to the DNI) bases many of its fundamental R&D activities on civilian hi-tech workers and technology, some of whom are recruited to IARPA for periods of some years.[20]
2. **Investment**: Another mechanism is the intelligence organizations' investment in capabilities developed by the hi-tech industry and civilian startups. The CIA set up In-Q-Tel,[21] a government-sponsored venture capital firm, which locates relevant civilian startups for the intelligence community, primarily for the Agency. Government funding makes it possible for the intelligence organizations to promote the development of high-risk high-payoff technologies for which it would be difficult to find funding from private investors. In recent years, inspired by In-Q-Tel, Israeli initiatives were established, such as the Mossad's Libertad Ventures[22] and the Israeli Security Agency's XCELERATOR.[23]
3. **Migration**: Other measures go further afield, physically and paradigmatically, and **create a permanent presence of intelligence organizations within civilian STEM** (Science Technology

[19] The Cipher Brief (December 2, 2021), CIA Deputy for Digital Innovation Talks Mission, Partnerships and Espionage Challenges.
[20] ODNI (May 9, 2017), IARPA Project; Chelsea Seeber (June 24, 2022) Professor receives grant as part of $14 million industry collaboration to improve secure communications, Virginia Tech.
[21] InQTel Homepage
[22] Libertad Ventures Homepage
[23] The XCELERATOR Homepage

Engineering and Mathematics) **ecosystems.** The objective is to create physical spaces for shared work and encourage joint ventures between intelligence organizations on the one hand, and the university system and the hi-tech industry on the other. Good examples of this are NGA2West project, under which the second headquarter of the NGA is being built in St. Louis, situated nearer to hi-tech, startup and academic GEOINT centers); the FBI campus in Huntsville, Alabama (established near academic and industrial defense and space centers, and expected to employ thousands of Bureau personnel), or the GCHQ's Heron House in Manchester (whose objective is to be near the talents working in the local hi-tech complex). The new facilities also include unclassified work areas to enable shared intramural work with civilians.[24]

Commitment to share intelligence information and assessments with the public

According to the original and most prevalent concept, the intelligence community works first and foremost for the decision makers in the executive and legislative branches. Today that concept is insufficient. Western intelligence agencies should regard the civilian public as an important client who must be informed of intelligence assessments, at least on some issues, and needless to say within the limitation of source protection. Previously, that was necessary because of the growing demand in some countries for the civilian transparency of intelligence, following the war on global terrorism and the criticism in its wake of the violation of human rights and individual freedoms. However, the demand for transparency is still essentially passive regarding civilian involvement in practical intelligence matters, and is limited to satisfying the public demand to ensure that intelligence organizations' work methods operate properly and do not deviate from the ethical and democratic limitations that apply to them.

Today, however, the public has to be regarded as an intelligence consumer and receive intelligence products. Given the enormous power of the social networks, which are not bound by national security considerations and regulating them is still in its infancy,[25] the public in the West is a primary target for systematic attacks of disinformation and influence campaigns from foreign countries, as well as from politicians, lobbies and even simply chaos agents working on their own from inside the country itself. Those attacks have a significant negative influence on the nation's democratic fabric

[24] Ofer Guterman (April 2021), Intelligence organizations' integration in local ecosystems of innovation, The Institute for the Research of Methodology of Intelligence; NGA (November 21, 2019), NGA breaks ground on new facility in north St. Louis; FBI (n.d.) The FBI at Redstone; GCHQ (n.d.) Locations-Manchester.

[25] Israeli Ministry of Communications, (December 14, 2022), After the European Union, the State of Israel also intends to apply regulation to social media; Jonathan Wareham, (February 10, 2020) Should Social Media Platforms Be Regulated?, Forbes.

and resilience because of the decline of trust in national institutions, political polarity and the fomenting of rifts and arguments, the difficulty in reaching an agreed-upon, factual basis for reality, and the weakness of social solidarity.[26]

Given the circumstances, intelligence organizations no longer have the privilege of hiding behind walls of secrecy, or of allowing the justified concern of involvement in political discourse to silence them. Public perception has become one of today's most important battlefields, and intelligence is a vital, central weapon. Therefore, intelligence organizations should play an active role not only in directly preventing efforts to negatively influence the public, but to broker their professional truth in the fields of national security to combat false narratives that weaken national resolve (in addition to their role in the battle for the hearts and minds of external target audiences.)[27]

In effect, the commitment to the public should be expressed through **the public dissemination in systematic, orderly fashion, both verbally and in writing**, of intelligence products and assessments (needless to say, without classified information). In Israel today intelligence assessments reach the eyes and ears of the public through the briefings and interviews given by senior intelligence figures, leading to a situation in which the media rather than the intelligence organizations control the message, and therefore the result is often partial, superficial and on occasion, incorrect.[28]

Sharing intelligence assessment with the public should take place after a thorough, rigorous clarification of ethical and democratic aspects, considerations of secrecy and the protection of sources, and an intelligent risk-management of possible sensitivity vis-à-vis the political echelon, which may feel slighted by losing its monopoly on intelligence assessment vis-à-vis the electorate.

Therefore, the intelligence organizations should play a proactive role in exposing and neutralizing disinformation and misinformation campaigns. Since the civilian area of activity is a complex venue, the intelligence organizations will not be able to operate in it independently and isolated from other forces already active in the arena. That again increases the importance of integrating intelligence forces with those of relevant interests in the government ministries and additional public bodies,

---

[26] Josh A. Goldstein & Shelby Grossman (July 4, 2021), How disinformation evolved in 2020, Brookings; Chris Tenove (May 25, 2020), Protecting Democracy from Disinformation: Normative Threats and Policy Responses, The International Journal of Press/Politics; Merten Reglitz (July 27, 2022), 'Fake news' poses corrosive existential threat to democracy - study, University of Birmingham.

[27] Dan Sabbagh (December 29, 2022), GCHQ chief: western spy agencies must 'pre-bunk' disinformation, The Guardian; Capt Tom (March 18, 2022), How the West is starting to win the disinformation war, Wavell Room.

[28] Yossi Kuperwasser, Major A., Dodi Siman Tov (June 2020), The commitment of the intelligence community to a national assessment to the public, the Institute for the Research of the Methodology of Intelligence.

civilian actors involved in the field, foreign intelligence organizations and like-minded groups.[29]

Adopting human capital strategies which are more open to the public sector and the private market

Intelligence organizations, like other organizations around the globe, are preoccupied with the dramatic changes in the labor market caused by the entrance of generations of workers with different sociological orientations, digital transformations and changing cultural trends that affect workplaces. By their nature, many of the changes push for greater interrelationships between intelligence organizations and the civilian sphere, such as the need for social and environmental responsibility. In addition, young workers who have reservations regarding the old, stable model of working in the same organization until retirement require more diverse and flexible models, including transitions between intelligence organizations and civilian work places (in the public and private sectors).[30]

In addition, the required changes in human capital strategies in intelligence organizations also have unique characteristics. First, as the intelligence organizations move towards increasing their dealings with civilian issues or issues with civilian dimensions, they would do well to acquire knowledge about civilian areas of endeavor and points of view. Those should be acquired not only through outsourcing and cooperation with civilian sources, but also by assimilating capabilities and points of view from within the organizations themselves through a growing integration of civilians in the ranks of the intelligence organizations.

The American intelligence community, which has dealt with the issue at great length in recent years, reflects the growing challenge to recruit and retain the talent from the public sector because of the difficulty in competing with the private market, where salaries are higher and the work is more flexible. For the American intelligence community, the challenge begins at the recruiting stage since there is no compulsory military service, as there is in Israel, therefore some of the early American

[29] Dodi Siman Tov and Liav Sela (November 2020), The role of intelligence vis-a-vis foreign influence on democratic processes: an in-depth study, the Institute for the Research of the Methodology of Intelligence.
[30] Aliya Sternstein (January 27, 2016), Look Who's Worried About the NSA's 96 Percent Retention Rate, DefenseOne; The Economist (March 3, 2018), America's intelligence agencies find creative ways to compete for talent; Yasmin Tadjdeh (February 26, 2018), Cyber talent wanted: Military, Intelligence Community Strive to Retain Cyber Workforces, National Defense.

solutions are related to simplifying and shortening the recruitment process of civilians, many of them from the ranks of university graduates with relevant degrees.[31]

Another challenge, one more relevant to Israel, is the preservation of existing human capital. One American strategy is to strengthen the connection between intelligence personnel and the civilian sphere by transitioning between intelligence roles and civilian stations on their career courses. For example, a study carried out for the American Department of Defense by MIT in 2019 to "provide insights and recommendations for how laboratories in the Defense Laboratory Enterprise can meet their dual purpose: to serve the national defense interest through innovation and, simultaneously, to play a role in supporting their regional innovation economies," included recommending the appointment of a Director of Engagement who would work with local interests, incentivize holding meetings between individuals from both worlds, including providing funds for "entrepreneurial sabbaticals." The rationale was that sabbaticals would strengthen the Department's technologists and engineers who were interested in entrepreneurial ventures, as well as relations between the Department and the entrepreneurial communities, and develop companies that would contribute to the local region.[32] In similar fashion, the integral transitioning in the career course of intelligence personnel who are not technologists into the ranks of academia, government ministries and the private sector can be considered.

Open intelligence – barriers and the way forward

Relations are beginning to be forged between the intelligence establishment and the civilian world in ever-increasing fields and with unprecedented strength, which accumulate into a paradigmatic change in the way intelligence is done. This is as true in the aspects of capabilities-building as it is in the aspects of the exercise of intelligence activities along the entire length of the intelligence value chain. **To preserve relevance, the intelligence community has to continue gradually forming open and more symbiotic relations with the civilian world,** and even to integrate into civilian ecosystems. This is a vital growth engine for the intelligence community and in fact for the national security

[31] WSJ Noted (February 4, 2021) Here's How the CIA Is Trying to Attract More Diverse Millennial and Gen-Z Talent; David Stebbins, Sina Beaghley, Ashley L. Rhoades, Sunny D. Bhatt (2019), Literature on Personnel Vetting Processes and Procedures, RAND.
[32] Kathryn Person, Dylan Cohen, Jonathan Miller, Fiona Murray (May, 2019), NSWC Crane Innovation Analysis: Contributing to Regional Innovation Ecosystems, MIT Innovation Center.

of countries, and ignoring it will, over time, erode the ability of intelligence organizations to fulfill their missions.

Today, some of the intelligence organizations move along this path in a conscious, strategic and pro-active manner, while others advance at a slower and more tactical pace, and promote cooperation with civilian entities only where it is necessary. The differences also stem in part from the lack of an overall conceptual framework for the new relations with the civilian sphere, but also due to four major barriers that stand in the way of the intelligence organizations seeking to open up to the civilian world.

The first barrier is **the culture of secrecy and self-reliance**. The intelligence organizations' DNA is programmed for covert activity in the dark, away from the eyes of anyone who is not in the circle of secret-keepers, and even more so away from the eyes of the public. Intelligence activities, in the classical view, are none of their concern. Every contact with civilians is fraught with risk to sources, who are the core assets of intelligence, as well as to the unique tools and methods of the intelligence organizations. However, nowadays, where the open sources have become a central source of importance, and the technology responsible for the production of the intelligence's operational capabilities is to be found mainly in private industry, the culture of secrets has to be thoroughly revised to adapt it to the new global situation.[33]

The second barrier concerns the intelligence organizations' ability to **internalize the loss of monopoly in the intelligence market**, and the resulting need to turn to external partnerships to maintain relevance. It is by no means certain that all intelligence communities realize to what degree they are in competition with the media, civilian intelligence, think tanks and NGOs, all of which construct good intelligence information, interpretations and assessments, and shape the intelligence perceptions of political decision-makers and the general public.

The third barrier is related to **possible tension between intelligence and the decision makers at the political level**, as the intelligence organizations internalize their obligation to provide the public with information and intelligence assessments in a broad, systematic manner. Familiarity with information material gives the decision makers an inherent advantage, and no less important, the image of an inherent advantage, over the general public. Exposing the intelligence to the public can deprive politicians of one of the elements they use to yield public support for their policy on foreign and security

[33] Matilda Head (December 29, 2022), Spies need to be less secretive, says head of GCHQ, The Telegraph; Dan Sabbagh (December 29, 2022).

issues. The tension will be especially acute in cases where the intelligence assessments do not match the intelligence picture of the decision makers, or in cases where intelligence information has personal implications for the decision makers, as could be argued in several events in recent years in various countries.

The fourth barrier is related to the **reluctance of elements in civil society and the business sector to cooperate with the state, and especially with security and intelligence services**. The deep reluctance of many in Silicon Valley to work with and for the intelligence community is a mirror image of the blurring of the boundaries between the Chinese state and the private sector in terms of security and intelligence. Israel has a third and more balanced model (although not without its problems), of the private high-tech industry with the security establishment and within it the intelligence organizations, which function as distinct entities but with many interrelations between them.

To overcome the aforementioned barriers and enable the formation of strong connections and brave partnerships with the civilian sphere, intelligence organizations need to formulate new strategies and the willingness to challenge the basic premises rooted in traditional intelligence culture. **The strategies will need clear, thorough-going processes regarding civilian national security issues** whose treatment of intelligence is planning to share, extensive processes of learning the civilian sphere and the full realization of the potential of cooperation with it, moving the needle of sources and information risk management, and creating a joint technological work environment (Cloud based).

During the past two decades, intelligence organizations around the globe carried out significant processes of internal jointness, which broke barriers and created bridges between different parts of the same intelligence organization, within organizations of the same intelligence community, and between different intelligence communities. The intelligence establishment is currently facing another challenge of breaking down walls and creating bridges, this time with the civilian sphere within which and for which it operates. That is a more complex challenge than its predecessors, but it is just as important and essential to ensuring the ability of the intelligence organizations to fulfill their important role in the defense of national security.