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

How Tech is Transforming the Intelligence Industry

Shay Hershkovitz

At a conference on the future challenges of intelligence organizations held in 2018, former Director of National Intelligence Dan Coats argued that he transformation of the American intelligence community must be a revolution rather than an evolution. The community must be innovative and flexible, capable of rapidly adopting innovative technologies wherever they may arise.

Intelligence communities across the Western world are now at a crossroads: The growing proliferation of technologies, including artificial intelligence, Big Data, robotics, the Internet of Things, and blockchain, changes the rules of the game. The proliferation of these technologies – most of which are civilian, could create data breaches and lead to backdoor threats for intelligence agencies. Furthermore, since they are affordable and ubiquitous, they could be used for malicious purposes.

The technological breakthroughs of recent years have led intelligence organizations to challenge the accepted truths that have historically shaped their endeavors. The hierarchical, compartmentalized, industrial structure of these organizations is now changing, revolving primarily around the integration of new technologies with traditional intelligence work and the redefinition of the role of the humans in the intelligence process.

Take for example Open-Source Intelligence (OSINT) – a concept created by the intelligence community to describe information that is unclassified and accessible to the general public. Traditionally, this kind of information was inferior compared to classified information; and as a result, the investments in OSINT technologies were substantially lower compared to other types of technologies and sources. This is changing now; agencies are now realizing that OSINT is easy to acquire and more beneficial, compared to other – more challenging – types of information.

Yet, this understanding trickle down solely, as the use of OSINT by intelligence organizations still involves cumbersome processes, including slow and complex integration of unclassified and classified IT environments. It isn't surprising therefore that intelligence executives – for example the Head of State Department's Intelligence Arm or the nominee to become the Director of the National Reconnaissance Office – recently argued that one of the community's grandest challenges is the quick and efficient integration of OSINT in its operations.

Indeed, technological innovations have always been central to the intelligence profession. But when it came to processing, analyzing, interpreting, and acting on intelligence, however, human ability – with all its limitations – has always been considered unquestionably superior. That the proliferation of data and data sources are necessitating a better system of prioritization and analysis, is not questionable. But who should have a supremacy? Humans or machines?

Big data comes for the spy business

The discourse is tempestuous. Intelligence veterans claim that there is no substitute for human judgment. They argue that artificial intelligence will never be capable of comprehending the full spectrum of considerations in strategic decision-making, and that it cannot evaluate abstract issues in the interpretation of human behavior. Machines can collect data and perhaps identify patterns, but they will never succeed in interpreting reality as do humans. Others also warn of the ethical implications of relying on machines for life-or-death situations, such as a decision to go to war.

In contrast, techno-optimists claim that human superiority, which defined intelligence activities over the last century, is already bowing to technological superiority. While humans are still significant, their role is no longer exclusive, and perhaps not even the most important in the process. How can the average intelligence officer cope with the ceaseless volumes of information that the modern world produces?

From 1995 to 2016, the amount of reading required of an average US intelligence researcher, covering a low-priority country, grew from 20,000 to 200,000 words per day. And that is just the beginning. According to forecasts, the volume of digital data that humanity will produce in 2025 will be ten times greater than is produced today. Some argue this volume can only be processed – and even analyzed – by computers.

Of course, the most ardent advocates for integration of machines into intelligence work are not removing human involvement entirely; even the most skeptical do not doubt the need to integrate artificial intelligence into

intelligence activities. The debate centers on the question of who will help whom: machines in aid of humans or humans in aid of machines.

Most insiders agree that the key to moving intelligence communities into the 21st century lies in breaking down inter- and intra-organizational walls, including betweenthe services within the national security establishment; between the public sector, the private sector, and academia; and between intelligence services of different countries.

It isn't surprising therefore that the push toward technological innovation is a part of the current intelligence revolution. The national security establishment already recognizes that the private sector and academia are the main drivers of technological innovation.

Private services and national intelligence

In the United States there is dynamic cooperation between these bodies and the security community, including venture capital funds jointly owned by the government and private companies.

Take In-Q-Tel – a venture capital fund established 20 years ago to identify and invest in companies that develop innovative technology which serves the national security of the United States, thus positioning the American intelligence community at the forefront of technological development. The fund is an independent corporation, which is not subordinate to any government agency, but it maintains constant coordination with the CIA, and the US government is the main investor.

It's most successful endeavor, which has grown to become a multi-billion company though somewhat controversial, is Palantir, a data-integration and knowledge management provider. But there are copious other startups and more established companies, ranging from sophisticated chemical detection (e.g. 908devices), automated language translations (e.g. Lilt), and digital imagery (e.g. Immersive Wisdom) to sensor technology (e.g. Echodyne), predictive analytics (e.g. Tamr) and cyber security (e.g. Interset).

Actually, a significant part of intelligence work is already being done by such companies, small and big. Companies like Hexagon, Nice, Splunk, Cisco and NEC offer intelligence and law enforcement agencies a full suite of platforms and services, including various analytical solutions such as video analytics, identity analytics, and social media analytics . These platforms help agencies to obtain insights and make predictions from the collected and historic data, by using real-time data stream analytics and machine learning. A one-stop-intelligence-shop if you will.

Another example of government and non-government collaboration is the Intelligence Advanced Research Projects Activity (IARPA) – a nonprofit organization which reports to the Director of National Intelligence (DNI). Established in 2006, IARPA finances advanced research relevant to the American intelligence community, with a focus on cooperation between academic institutions and the private sector, in a broad range of technological and social sciences fields. With a relatively small annual operational budget of around $3bn, the fund gives priority to multi-year development projects that meet the concrete needs of the intelligence community. The majority of the

studies supported by the fund are unclassified and open to public scrutiny, at least until the stage of implementation by intelligence agencies.

Challenging government hegemony in the intelligence industry

These are all exciting opportunities; however, the future holds several challenges for intelligence agencies:

First, intelligence communities lose their primacy over collecting, processing and disseminating data. Until recently, the organizations Raison D'etre was, first and foremost, to obtain information about the enemy, before said enemy could disguise that information.

Today, however, a lot of information is available, and a plethora of off-the-shelf tools (some of which are free) allow all parties, including individuals, to collect, process and analyze vast amounts of data. Just look at IBM's i2 Analyst's Notebook, which gives analysts, for just few thousand dollars, multidimensional visual analysis capabilities so they can quickly uncover hidden connections and patterns in data. Such capacities belonged, just until recently, only to governmental organizations.

A second challenge for intelligence organizations lies in the nature of the information itself and its many different formats, as well as in the collection and processing systems, which are usually separate and lacking standardization. As a result, it is difficult to merge all of the available information into a single product. For this reason, intelligence organizations are developing concepts and structures which emphasize cooperation and decentralization.

The private market offers a variety of tools for merging information; ranging from simple off-the-shelf solutions, to sophisticated tools that enable complex organizational processes. Some of the tools can be purchased and quickly implemented – for example, data and knowledge sharing and management platforms – while others are developed by the organizations themselves to meet their specific needs.

The third challenge relates to the change in the principle of intelligence prioritization. In the past, the collection of information about a given target required a specific decision to do so and dedicated resources to be allocated for that purpose, generally at the expense of allocation of resources to a different target. But in this era of infinite quantities of information, almost unlimited access to information, advanced data storage capabilities and the ability to manipulate data, intelligence organizations can now collect and store information on a massive scale, without the need to immediately process it – rather, it may be processed as required.

This development leads to other challenges, including: the need to pinpoint the relevant information when required; to process the information quickly; to identify patterns and draw conclusions from mountains of data; and to make the knowledge produced accessible to the consumer. It is therefore not surprising that most of the technological advancements in the intelligence field respond to these challenges, bringing together technologies such as big data with artificial intelligence, advanced information storage capabilities and advanced graphical presentation of information, usually in real time.

Lastly, intelligence organizations are built and operate according to concepts developed at the peak of the industrial era, which championed the principle of the assembly line, which are both linear and cyclical. The linear model of the intelligence cycle – collection, processing, research, distribution and feedback from the consumer – has become less relevant. In this new era, the boundaries between the various intelligence functions and between the intelligence organizations and their eco-system are increasingly blurred.

The brave new world of intelligence

A new order of intelligence work is therefore required, and therefore intelligence organizations are currently in the midst of a redefinition process. Traditional divisions – e.g. between collection and research; internal security organizations and positive intelligence; and public and private sectors – all become obsolete. This is not another attempt to carry out structural reforms: there is a sense of epistemological rupture which requires a redefinition of the discipline, the relationships that intelligence organizations have with their environments – from decision makers to the general public – and the development of new structures and conceptions.

And of course, there are even wider concerns; legislators need to create a legal framework that accurately incorporates the assessments based on data in a way that takes the predictive aspects of these technologies into account and still protects the privacy and security rights of individual citizens in nation states that have a respect for those concepts.

Despite the recognition of the profound changes taking place around them, today's intelligence institutions are still built and operate in the spirit of Cold

War conceptions. In a sense, intelligence organizations have not internalized the complexity that characterizes the present time – a complexity which requires abandoning the dichotomous (within and outside) perception of the intelligence establishment, as well as the understanding of the intelligence enterprise and government bodies as having a monopoly on knowledge; concepts that have become obsolete in an age of decentralization, networking and increasing prosperity.

Although some doubt the ability of intelligence organizations to transform and adapt themselves to the challenges of the future, there is no doubt that they must do so in this era in which speed and relevance will determine who prevails.

Dr. **Shay Hershkovitz** is a senior research fellow at the Intelligence Methodology Research Center in Israel. He has over 20 years of experience in the Strategy and Research industry space; including in the Israeli intelligence community, the private sector and academia. is co-author of AMAN Comes to Light: Israeli Military Intelligence in the 1950s, and the author of dozens of academic articles. He writes regularly in U.S. media such as Wired, TechCrunch, and TheHill.com, and speaks to a variety of audiences.