HUMINT in the Cybernetic Era: Gaming in Two Worlds

Avi Tal and David Siman-Tov

The cyber era has caused enormous changes in intelligence and intelligence gathering. This article discusses whether the profession of human intelligence (HUMINT) is currently still relevant when cyberspace constitutes the main scene for intelligence gathering and action. If so, what missions should it assume, and are new opportunities being created for new operational methods in the cyber era? The article examines the substance of the HUMINT discipline and the challenges that cyberspace poses to this discipline. It also addresses the potential contribution of HUMINT in the cybernetic era, and raises the question whether it constitutes a new intelligence discipline. The first part of this article presents the HUMINT up until the cyber era. The second part discusses HUMINT in the cybernetic era, with an emphasis on its opportunities and risks, its changes, and presents a proposal for a new concept of the HUMINT profession in the cybernetic era.

Keywords: human intelligence, intelligence, intelligence gathering, cyber, intelligence community, cybernetic human intelligence, avatar

Introduction

Cyberspace has transformed the world into a global village. Cyberspace provides instant access to colleagues and rivals, friend and enemies, while transcending borders and languages. Public, open source information, as well as classified and encoded, all pass through cyberspace, which is also a key platform for command and control of systems and weapons. The social networks, blogosphere, and the new media have become the main mass platform for discourse and action in all spheres of life.[1] Almost everyone

David Siman-Tov is an intelligence researcher at the Institute for National Security Studies. Avi Tal is a former senior officer in the Arab Section of the Israel Security Agency.

now has a personal homepage on the Internet, and almost everyone uses the Internet to express their beliefs and desires regarding personal and professional matters. At the same time, cyberspace has led to the creation of threats of cybernetic attacks, which can sometimes have kinetic effects. The social networks have become an important platform for organizational efforts, as we saw with the "Arab Spring," as well as for incitement, as we have seen in the campaign that has led to current wave of knife attacks in Israel. The amount of public information is enormous and continually growing; at the same time, some cybernetic areas are difficult to penetrate.[2]

The cyber era has generated prodigious changes in intelligence and gathering of intelligence. These changes have led to questions about whether human intelligence (HUMINT) is still relevant when cyberspace is an important scene of action, and if so, whether opportunities for new modes of action are being created. The purpose of this article is to consider the nature of HUMINT in the cybernetic era, with an emphasis on the changes that have taken place in its concepts and methods of operation in comparison to the classic profession of HUMINT. The first part of the article presents HUMINT up until the cyber era. The second part discusses HUMINT in the cybernetic era, with an emphasis on its opportunities and risks, and the changes encountered. Finally, we present a proposal for a new concept of the HUMINT profession in the cyber era.

Classic HUMINT

From the dawn of history until the beginning of the twentieth century, intelligence agencies relied exclusively on information from human sources. Sun Tzu, a Chinese general from the sixth century BCE, wrote about spies and their importance in war.[3] Some regard the classic HUMINT profession as an art because it requires its practitioners to have great skills in interpersonal communications, broad general knowledge, familiarity with the psychological-philosophical study of human behavior, as well as the ability to be a jack-of-all-trades, and to be able to persuade, convince, and motivate people.

There are three key stages in the HUMINT profession. The first is locating and selecting the people needed on the basis of personal talents and qualifications, motives (existing and potential), and accessibility (for recruitment and being handled). The second stage is the actual recruitment of the people, for which various and diverse methods can be used: planned recruitment, direct recruitment, indirect recruitment through an undercover collaborator, chance recruitment, and recruitment of volunteers.[4] The third stage is handling and operations. A physical clandestine meeting is very important in creating trust and a personal affinity with the agent, and the related operational aspects of handling the agent (a test of courage, providing weapons, special teaching and training, and so forth).

Classic HUMINT was originally a simple human activity.[5] Recruiting and handling were based mainly on physical meetings, due to an almost complete absence of remote access. The process of locating people relied on limited and relatively inadequate intelligence, while the ability of the recruiters to select good agents was limited. In this physical world, the recruiting and handling required undercover action vis-à-vis the recruit and the surroundings while the system had to completely adapt to the recruit and his environs according to his cover story. These had to meet the physical test: the handler, the support players (including security), the location, lighting, language, and so forth. This situation created many risks for the security of the operation, the agent handlers, and also the agent. Equipping the agent with tools for covert actions increased the risk and constituted an incriminating signature.

The status of HUMINT in the western intelligence community faded from the 1970s onward,[6] as a result of the technological developments and the massive shift by people and armies to using electromagnetic space. This shift caused the rise of technological intelligence gathering; an increase in the contribution of geospatial intelligence through the use of satellites and cyberspace; and an enormous surge in the quantity of open source intelligence (OSINT). The conclusions of the investigatory committees that probed the September 11, 2001 terrorist attacks in the United States and the failure of US intelligence in Iraq were a turning point in the American intelligence community. These conclusions cited a lack of precise information about the al-Qaeda organization – the kind of intimate knowledge that HUMINT is designed to provide. As a result, it was understood that HUMINT had to resume its central role in the US intelligence efforts. One example of an effective and recent contribution by HUMINT to American intelligence gathering was in the hunt for al-Qaeda leader Osama bin Laden. The CIA recruited a Pakistani doctor who administered a vaccination to bin Laden's family members in their compound so that he might be able to obtain a DNA sample from Bin Laden to confirm his presence.

HUMINT in the Cybernetic Era

In the discourse on intelligence gathering in the cybernetic age, one approach is that the intelligence community should not rely only upon cyberspace for intelligence gathering. There is no substitute for HUMINT if the intelligence picture is to be comprehended as a whole, especially for organizations like ISIS and Hamas, which have a low cyber signature; total reliance on technological intelligence in obtaining accurate information about them is inadequate and questionable.[7] One approach holds that only when the extent to which intelligence gathering has penetrated into all aspects of life becomes apparent, then countries and organizations should seek to reduce the level of their intelligence signatures through messengers and work meetings.

In the theoretical discourse on HUMINT in the cybernetic age, some have proposed to broaden the HUMINT concept by combining it with the concept of "social engineering." This would mean creating a false identity for the purpose of recruiting human sources in order to influence them to act in a desired way. The combining of HUMINT and social engineering could fail to achieve HUMINT's existing advantages by channeling it into a single field, that of information security, in addition to losing the inherent potential of offensive cybernetic HUMINT.

The development of cybernetic HUMINT began in the middle of the preceding decade as agents turned to cybernetic tools; first and foremost, they turned to the Internet, and mainly to online forums where they operated under their own names or under aliases. The next stage of cybernetic HUMINT was the creation of fake identities and assumed names, led by a team of people from different disciplines. The team directed these personas to various forums, penetrating areas where existing agents were unlikely to operate. This stage was the result of accelerated technological development in recent years, which has made it possible to create identifies without limitations. In the Israeli context, this method makes it possible to move away from monitoring and foiling "knife terrorism" – currently being practiced and whose effectiveness is questionable – to actively and proactively reducing the incitement that leads to this type of terrorism and influences public opinion.

An internal contradiction exists ostensibly between the classic HUMINT manner of handling agents and that based on handling agents in cyberspace. Classic HUMINT includes holding personal meetings to create trust and personal affinity; developing close, intimate, and long-term relationships;

and hierarchical relations similar to employer-employee relations, including material and non-material remuneration. This is in addition to developing the handling from a long-term perspective, conducting reliability checks, providing training and weapons, and so forth. Cybernetic HUMINT, on the other hand, is based on relations that are not necessarily permanent, with a lower degree of commitment and loyalty, while the connections between the handler and his sources are not deep nor based on direct human connection.

Classic HUMINT involves intimate personal contact facilitating a direct emotional language that creates a connection and closeness beyond shared interests. In cybernetic HUMINT, handling is based on a convergence of interests. As a result, the level of commitment in classic HUMINT is higher, and the agent is more likely to take actions that will endanger him. In cybernetic handling, on the other hand, the level of risk to the agent is much lower. Furthermore, the direct physical meeting with agents is a critical element in creating a personal affinity, important in almost every aspect of handling and operations. The physical contact, the eating and drinking together, and so forth create a special connection that contributes to the agent’s motivation. Cyberspace, on the other hand, makes it possible to conduct a virtual meeting that has some similarities to a physical meeting. All that a virtual meeting requires is that it be conducted with minimum risk and without incriminating signatures.

In the cybernetic HUMINT era, the candidates for recruitment are diverse and almost unlimited. Intelligence required for locating them can be obtained quickly, the selection is broad, and access is easy. Furthermore, cyberspace makes it possible to conduct the recruitment and handling stages with relatively little risk, at almost no cost, and with almost no effort, with the help of impersonation or anonymity, including multimedia meetings. Connecting with individuals and groups can be done easily, without any physical danger. Cybernetic HUMINT is groundbreaking and significantly improves the ability of HUMINT personnel to reach remote target audiences that are difficult to recruit. Cyberspace also gives the investigative personnel additional tools to verify the reliability of agents and double check the interrogation of suspects. For example, checking the reliability of a person being interrogated can be done using the information he shared on Facebook. The problem of anonymous sources who are unknown to the handler seems insignificant when the information is intended for research and understanding social currents. On the other hand, this question is acutely significant when the information is needed for counteraction or another operation liable to endanger human life.

The cyber era makes it possible to vanish into the vast sea of information and under assumed identities and roles, thereby substantially ensuring safe communications with agents. Given the varied capabilities for transmitting information through cyberspace and the ability to rapidly transmit large volumes of information, cyberspace has improved the possibilities of communication between agents and collaborators. In the past, agents had to fill cases, luggage, or boxes with material and deliver it to their handlers, at great risk to both parties. Today, a USB drive is enough to enable agents to transfer large amounts of multimedia information of even higher quality. Although cyberspace has reduced the need for face-to-face meetings, thereby diminishing the risk to both parties, at the same time, active intelligence activity in cyberspace has a signature that is liable to constitute a threat in the short or long term. Indirect risks are also increasing as supervision, monitoring, and discovery actions in cyberspace are being stepped up.

Cybernetic HUMINT can penetrate the enemy's cyberspace, such as open or closed forums, and join them passively or actively – in order to extract information. Cybernetic agents can actively exert their influence by recruiting the enemy's agents for the purpose of gathering information; directing agents to act in the physical world; or by affecting public opinion, such as by forging opinions against the delegitimization of Israel (BDS) in relevant forums. Cyberspace can also be utilized to create false rumors about a person in order to attack him – a kind of "cybernetic shaming." In addition, the potential of cybernetic HUMINT for influencing and shaping the enemy's cyberspace is vast, as a result of the open and civilian character of the cyber era. It is important to stress in this context that many intelligence organizations are already operating in the cybernetic sphere, and that the cybernetic personas of these organizations can be located. This makes it possible to engage in cooperative efforts and forge mutual synergy with foreign intelligence organizations that share common interests. At the same time, it should be taken into account that hostile groups or enemies will manipulate cyberspace by using "cybernetic double agents" who will feed false information to intelligence agencies.

In the civilian cyberspace, the "avatar" image – a representation of a user in cyberspace through an imaginary graphic icon, like an actor in a play or a movie, is prevalent. By using avatars, a person could have an unlimited number of identities, and could rapidly create an image and assumed identity for almost any scenario and without complicated operations that require many resources. American intelligence has warned about the use of digital avatars for terrorist purposes, such as Osama Bin Laden's avatar for mass recruitment of terrorists.[8] *Washington Post* reporter Robert O'Harrow wrote about making the spies' battlefield a virtual one, citing as an example a businessman's avatar in the field of games. He notes that intelligence sources understand the potential of the avatar for purposes of terrorism and crime.[9] The handling of avatars of various types and volumes plays a key role in cybernetic HUMINT, including the use of avatars developed in civilian companies, such as an avatar agent for verification testing,[10] a voice-based verification testing device,[11] and polygraph applications[12] used to assist in interrogations and reliability tests.

Actions for Consideration by the Intelligence Community

The field of cybernetic HUMINT integrates the handling characteristics of HUMINT and cyberspace. This combination gives rise to new groundbreaking opportunities that the traditional HUMINT had reserved only for itself. It is too early to tell whether a new discipline has emerged, but the combination of the two, with new concepts and practical features requires an innovative synergy between the clandestine environment and the civilian-commercial environment. This has great potential, both for obtaining intelligence from new communities more quickly and on a larger scale, as well as for influencing the adversaries' social networks and cyberspace.

In the cyber era, HUMINT has experienced substantial changes, led by the introduction of a new sub-profession, which we have referred to as "cybernetic HUMINT." In addition to the need for principles similar to those of traditional HUMINT, cybernetic HUMINT has new features, and does not require direct contact with the sources. This understanding requires organization of all the aspects of building the intelligence force, with an emphasis on training intelligence personnel; in addition to human sensitivity, intelligence personnel need to acquire social sensitivity.

The principles of the HUMINT profession from the period before the cybernetic era form the classic intelligence-gathering profession. The development of this profession in the cyber age emphasizes the change and innovation of this era. The question of the ostensible contradiction between the two types of HUMINT professions – the classic and the cybernetic – was examined, and a number of differences between them can be pointed out:

1. Classic HUMINT requires proximity and direct meeting with the source. In contrast, in cybernetic HUMINT sources can be handled without the handlers knowing their identity, at least up to a certain point.
2. The ability to cross borders is limited in classic HUMINT. In cybernetic HUMINT, borders can be crossed and sources can be handled in remote areas as well.
3. Classic HUMINT focuses on gathering information. In cybernetic HUMINT, the public opinion of the adversary can also be influenced through psychological warfare.
4. In classic HUMINT, the search for agents is limited, and it is difficult to obtain information about the candidates for recruitment. In cybernetic HUMINT, the search for agents is virtually unlimited, with most of those recruited volunteering information and revealing themselves on their own free will.
5. In classic HUMINT, handling incurs great risk for both the handler and the agent being handled. Cybernetic handling, on the other hand, is ostensibly safer, and does not incur risk, although cybernetic handling leaves signatures.
6. In classic handling, the enemy's physical space is given. In cybernetic handling, on the other hand, the enemy's cyberspace can be influenced and shaped.
7. Classic HUMINT is based on human sources and human handlers. In addition to human handling, cybernetic HUMINT is also based on the imaginary personas on both sides, and on computer-generated personas.

In the cyber era, the cooperation between intelligence-gathering disciplines has become stronger. Cyber intelligence and Signals Intelligence (SIGINT) provide intelligence for HUMINT for locating and recruiting, accessing and handling, and gaining operational opportunities, in addition to providing an umbrella of security for its activity. HUMINT provides SIGINT and cyberspace intelligence with leads, which enable them to intercept and monitor intelligence and gain access to information channels, databases, and end-user equipment that is not provided by Internet and by the new type of agents.

It is important for the HUMINT discipline in the intelligence community to monitor the achievements of the civilian industries and companies engaged in cybernetic research, development, and the operational field,[13] and to adapt the HUMINT profession to the challenges of the new era. In addition, the intelligence community should conduct a continuous dialogue with civilian industries and companies in this area as significant HUMINT technologies and capabilities have been created by the private sector from which the defense establishment can and should learn, rather than trying to develop the tools and methods itself. Such a dialogue will significantly augment HUMINT capabilities for coping with the challenges ahead.

Notes

[1] Andrew Shapiro, "Is the Net Democratic? Yes – and No," World Media Forum, Berkman Center for Internet and Society at Harvard University, http://cyber.law.harvard.edu/shapiroworld.html.

[2] Amit Steinhart, "The Future is behind us? The Human Factor in Cyber Intelligence: Interplay between Cyber-HUMINT, Hackers and Social Engineering," *Cyber Guard*, 2014, http://diplomacy.bg./archives/1190?lang=en.

[3] Sun Tzu, *The Art of War*, vol. 13, *The Use of Spies*. Trans. Lionel Giles, http://classics.mit.edu/Tzu/artwar.html.

[4] Volunteers constitute both a risk and an opportunity, because the character is unknown and their intentions have not been verified. They can be swindlers and charlatans, acting out of real and varied motives, or as enemy agents planning to penetrate intelligence ranks as double agents. They can become the best agents, and can also lead us to the brink of disaster. An article by researcher Katherine Herbig analyzes the changes in the methods of espionage in the United States during 1947-2007. See Katherine L. Herbig, *Changes in Espionage by Americans: 1947-2007* (Defense Personnel Security Research Center, March 2008), https://www.fas.org/sgp/library/changes.pdf.

[5] Yehoshafat Harkabi, *The Intelligence as a National Institute (*Tel Aviv: IDF Publishing House and Israel Intelligence Heritage and Commemoration Center, 2015), p. 173, http://www.terrorism-info.org.il/Data/articles/Art_20896/arkabi_1008526679.pdf.

[6] Julien Babanoury, "Where Does HUMINT Fit in with the 21st Century Intelligence Community?" September 8, 2014, http://www.secuinsight.fr/2014/03/03/where-does-humint-fit-in-with-the-21st-century-intelligence-community-by-julien-babanoury-ceis/.

[7] Gabi Siboni, "Cyber Tools are not a Substitute for Human Intelligence," *Haaretz,* July 2, 2014, http://www.haaretz.com/opinion/.premium-1.602413.

[8] Sara Malm, "A Threat for the Digital Age – An Avatar Osama Bin Laden: U.S. Intelligence Warned Terrorists Could Create Virtual Jihadist To Preach and Issue Fatwas for Hundreds of Years," *MailOnline*, January 9, 2014, http://www.dailymail.co.uk/news/article-2536440/A-threat-digital-age-avatar-Osama-bin-Laden-U-S-intelligence-warned-terrorists-create-virtual-jihadist-preach-issue-fatwas-hundreds-years.html; David Kravets, "US Intel: Bin Laden Avatar Could Recruit Terrorists for Hundreds of Years," *Wired*,

January 9, 2014, http://www.wired.co.uk/news/archive/2014-01/09/osama-bin-laden-avatar.

9 Robert O'Harrow Jr., "Spies' Battleground Turns Virtual," *Washington Post*, February 6, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/02/05/AR2008020503144.html.

10 AVATAR – Automated Virtual Agent for Truth Assessments in Real-Time, University of Arizona, 2015, http://borders.arizona.edu/cms/projects/avatar-automated-virtual-agent-truth-assessments-real-time.

11 Amir Liberman, The LVA (Layered Voice Analysis) Technology, nemesysco, http://www.nemesysco.com/technology-lvavoiceanalysis.html.

12 Android apk Polygraph Lie Detector Version 1.0 Free Download, 2014, http://appdownload.m5f.net/apk/com.ciberdroix.polygraph.html.

13 For example, an Israel cyber intelligence company operating an avatar: https://www.sensecy.com.