INTELLIGENCE AND SECURITY IN THE 21ST CENTURY

THE ROLE OF HUMAN INTELLIGENCE IN THE AGE OF DIGITAL TECHNOLOGY

Domenico FRASCÀ*
Giulia VENTURI*
Maria USTENKO*
Alessandro ZANASI*
Andrew STANIFORTH*
David FORTUNE*

Abstract:
This paper focuses on the role and perspectives of Human Intelligence in the digital era. It explores technological advancements that can be harnessed by Intelligence and Security practitioners in the fields of HUMINT and its associated support activities. The paper considers various technologies, including tools for decision support, deception and information detection, and strategies for mitigating cognitive biases and other limiting factors. The analysis concerns technologies, tools and techniques used in all phases of the Intelligence Cycle, evaluating their utility considering the current challenges posed by them for Intelligence Communities and Law Enforcement Agencies. Recent developments in technologies which support other Intelligence disciplines such as SIGINT, IMINT and OSINT have potentially diminished the standing and priority of HUMINT within the Intelligence Cycle. Moreover, psychology has a crucial role in comprehending HUMINT, as human minds have their imperfections, and psychological processes like cognitive biases can result in unanticipated mistakes and unintentional outcomes within the field of Intelligence. Still, HUMINT sources continue to play a fundamental role in Intelligence Collection, analysis, and interpretation, due to their ability to recall, recognise, contextualise, and establish

* Security researcher at Zanasi & Partners, Modena (Italy), e-mail: info@zanasi-alessandro.eu
* Program manager at Zanasi & Partners, Modena (Italy), e-mail: info@zanasi-alessandro.eu
* Project manager at Zanasi & Partners, Modena (Italy), e-mail: info@zanasi-alessandro.eu
* President of Zanasi & Partners, Modena (Italy), e-mail: info@zanasi-alessandro.eu
* Director of Saher Europe OÜ, Männimäe (Estonia), e-mail: contact@saher-eu.com
* Director of Saher Europe OÜ, Männimäe (Estonia), e-mail: contact@saher-eu.com

connections between different information. HUMINT continues to be a vital element, providing a human touch and insights that can be difficult to reproduce solely through technological methods.

Keywords: *HUMINT, Intelligence, Intelligence Cycle, Security, Technology.*

Introduction

Human Intelligence (HUMINT) is an Intelligence discipline recognised by national security policymakers as the human collection of information through both overt and covert methodologies. The covert, sensitive and secretive nature of HUMINT creates difficulties when it comes to openly and publicly examining, reviewing, or researching the tools, methods, technologies, and skills involved in this confidential Intelligence-gathering field. Recent advancements in technologies supporting other Intelligence disciplines have raised questions about the standing and priority of HUMINT within the Intelligence Cycle. However, it is important to acknowledge that HUMINT sources continue to hold a critical and irreplaceable role in Intelligence collection, analysis, and interpretation. The unique abilities of HUMINT sources, including their capacity to recall, recognise, contextualise, and establish connections among diverse pieces of information, make them invaluable contributors to the Intelligence community. While technology has enhanced various aspects of Intelligence gathering, HUMINT remains an essential component, offering a human element and insights that can be challenging to replicate with technological means alone.

The aim of this paper is to illustrate the current role of HUMINT in light of the latest technological developments, as well as to provide insights to the state-of-the-art of technological advancements exploitable by Intelligence and security practitioners in the fields of HUMINT and support activities. This also encompasses any technology, tools, or methods that are presently considered to be operating beyond the accepted legal, ethical, and cultural standards of security and Intelligence policy practices and procedures in the European Union (EU). The methodology employed involves a thorough analysis of technologies from diverse viewpoints. To achieve this, it was conducted an extensive review of a range of public information sources, including EU-funded projects and related initiatives, primary publications, peer-reviewed

papers, websites, news reports, whitepapers, reference materials detailing best practices and standards, among others. Additionally, have been supplemented the newly identified technology solutions from these sources with other commercial technologies that were documented in the literature and accessible on public websites.

The basic concepts of HUMINT are explored and defined in the first section. The following sections present a review of the latest technological solutions for HUMINT activities and outline their utility considering the Intelligence requirements and security applications. Finally, this paper offers a set of recommendations and relevant discussion topics on the challenges and opportunities of HUMINT technologies for Intelligence organisations and Law Enforcement Agencies (LEAs) within the European framework.

Definition of Human Intelligence

HUMINT is a discipline that refers to Intelligence gathered through means of interpersonal contacts and human sources. Its methodologies can be overt, such as in an interview, or covert, such as through surveillance, and reconnaissance (NATO Allied Command Transformation, 2023). Although associated to the military, the term HUMINT can apply in a variety of civilian sectors, such as LEAs (Clark, 2013). Amongst the rise of other Intelligence disciplines such as Signals Intelligence (SIGINT), Imagery Intelligence (IMINT) and Open-Source Intelligence (OSINT), based on technological advancements, HUMINT remains the oldest method for collecting information, and until the technical revolution of the mid-late 20th century, it was the primary source of Intelligence (US Office of the Director of National Intelligence, 2023). The Official NATO Terminology Database defines HUMINT as "*Intelligence derived from information collected by human operators and primarily provided by human source*" (NATO Standardization Office, 2015). The NATO definition of HUMINT has been adopted and applied in this study as it provides the broadest definition and covers the international dimension of the Intelligence and security practitioners landscape which is essential as it applies to military and defence Intelligence, as well as Intelligence organisations, LEAs, and other security practitioners. Indeed, the NATO definition of HUMINT provides

a description of the discipline that generally encompasses all the definitions provided at the national level by NATO Countries and EU Member States.

For the public, HUMINT is still closely associated with espionage and secretive operations; however, most of HUMINT collection is performed by overt collectors such as strategic debriefers and military attaches (US Office of the Director of National Intelligence, 2023). Although spying and informing on others is described in Intelligence community circles as the oldest Intelligence discipline, HUMINT continues to evolve. Even though the fundamental principles of human espionage remain unchanging, several factors have shaped and redefined the principles and scope of Intelligence over time. It is not only the methods of HUMINT that have evolved but also the reasons and approaches used. Demographics, technology, and cultural expectations all contribute to shaping the modern clandestine service officer or covert HUMINT source of information for Intelligence organisations and LEAs.

HUMINT application

The operational advantages of HUMINT are extensive, and effectively employing this discipline can significantly enhance Intelligence-driven operations and investigations. Intelligence agencies recognise that HUMINT provides a deeper understanding of the context surrounding a potential threat, including the motivations, intentions, and capabilities of the individuals involved. HUMINT also offers a greater degree of flexibity as assets can be directed to focus on pressing security concerns and can be targeted to achieve coverage and reporting on specific intelligence requirements. Moreover, HUMINT offers unique insights to hard to reach areas fo intelligence collection, being able to infiltrate and expose the inner workings and planning of hostile organised crime gangs, extremist groups and terrorist cells.

The operational advantages of HUMINT are not only restricted to the traditional physical elements of intelligence gathering. The contemporary use of HUMINT has observed positive applications in reporting on matters of cyber security. For instance, HUMINT can be used to collect information about potential threats to an organisation's information systems and infrastructure, including insider threats, social

engineering attacks, or various forms of cyber-espionage (CQR Company, 2023). It is this type of information that is instrumental in developing threat Intelligence that aids in identifying and mitigating potential risks which can also be used to examine and explore vulnerabilities in an organisation's physical and digital infrastructure. By gathering information about the organisation's systems, processes, and personnel, HUMINT assists in identifying potential weaknesses that malicious actors could exploit (CQR Company, 2023).

All Intelligence disciplines have their limitations, constraints and disadvantages and HUMINT is no exception. The recruitment, training, nurturing, and ongoing management of HUMINT sources demands substantial resources in the form of time, personnel, and budget to ensure their safety, security, and to generate valuable Intelligence outcomes. Moreover, HUMINT assets need to be handled by highly skilled, professionally trained and dedicated Intelligence personnel who owe a duty of care to the safety, security and well-being of their source. The operational deployment of trained HUMINT assets in the field, being managed by highly proferssional and skilled intelligence operatives, is no gurantee of success. For instance, establishing contacts and handling agents is a time-consuming process, and source reliability and information credibility are often difficult to assess (Pigeon, Beamish, & Zybala, 2002). There are also numerous legal, ethical, and regulatory considerations. The use of HUMINT must adhere to ethical standards and comply with all relevant laws and regulations, which can restrict the scope and scale of operations. Furthermore, there is a persistent risk of exposure and jeopardising the safety and security of those involved. When coupled with the limitations related to scalability and access in high-risk situations, these factors contribute to the complexity of the discipline (CQR Company, 2023). Despite these limiting factors, HUMINT remains a crucial Intelligence discipline that can provide critical information that other Intelligence assets may not be able to deliver.

Acquisition of HUMINT sources

The HUMINT discipline encompasses a diverse set of abilities, spanning from conventional diplomatic communication to techniques involving manipulation and deception. Its central aspect involves the

capability to enlist an individual for the purposes of espionage, information gathering, and infiltration. Evaluating the trustworthiness, motivations, and truthfulness of the human source right from the initial stages of recruitment, and throughout their entire tenure as a human source, is essential for identifying deception, ensuring operational security, and averting the risk of infiltration and various insider threats that could potentially expose State secrets (US Department of the Army, 2020). Additional skill sets in HUMINT encompass counter-Intelligence, surveillance, liaison exploitation, the use of cover, and the implementation of false flag operations.

The process of acquiring an individual for the purpose of espionage and Intelligence-gathering on behalf of a State agency is commonly known as the *Recruitment Cycle*, which involves the ability to identify an individual with access to the required information, identify their vulnerabilities, and assess whether they may be receptive to a recruitment pitch, manipulate those vulnerabilities with the aim of making them more inclined to agree to the recruitment proposal, and finally secure the individual's cooperation. The recruitment of Intelligence sources is an art of its own, where the ability to detect deception is a critical skill for anyone involved in recruiting individuals to carry out specific tasks (Sano, 2015).

The acronym MICE, which stands for Money, Ideology, Compromise, and Excitement, offers a basic explanation of the core motivations and reasons for individuals to become HUMINT sources as follows:

(1) *Money:* the allure of financial gain is a potent motivator for people in general. For a potential Intelligence agent, the right financial incentive can induce them to take significant risks and share sensitive information with a foreign case officer.

(2) *Ideology*. ideologically motivated agents are often seen as particularly dangerous, especially for counter-Intelligence officers tasked with identifying double agents and traitors within their own agencies. Ideology can take various forms, including religious, political, and social affiliations. However, for a case officer, a source driven by ideology can be a potent asset.

(3) *Compromise/coercion*: in contrast to ideology, agents who are coerced or compromised into sharing Intelligence are less desirable.

An agent driven by ideology is rooted in a set of beliefs that go beyond personal interests. On the other hand, a compromised or coerced agent, typically through blackmail, is more susceptible to influence and likely to act to avoid punishment. Because they do not willingly cooperate, they may harbour negative emotions about being an agent, which can pose challenges for a case officer.

(4) *Excitement/ego*: finding ways to stroke or manipulate the human ego and the desire for excitement is a primary approach for a case officer to recruit an asset. While these two traits are often grouped together, they have some distinctions. *Excitement* is a fleeting feeling, whereas if the case officer effectively works on an individual's "ego", it can have a more enduring impact (Burkett, 2013).

Personnel involved in Intelligence, security, and LEAs who are engaged in the development, recruitment, and handling of human sources carry out a diverse array of functions to accomplish the mission of gathering information. These functions encompass both overt and covert methods for Intelligence collection, overseeing the collection and reporting processes, and directing the use of Intelligence to support various operations and investigations. The methodologies and practices employed in HUMINT tradecraft are intricate and encompass a range of tools, techniques, and technologies designed for targeting, recruiting, and utilising HUMINT sources. These practices are inherently sensitive and confidential. Furthermore, different agencies operating in distinct jurisdictions use varying tradecraft techniques, and the disclosure of these methods to the public is safeguarded through rigorous operational security measures, legal non-disclosure agreements, and, in some cases, in compliance with specific national laws and regulations (US Defense Intelligence Agency, 2008).

Technological solutions for HUMINT

Various technology solutions are available to support HUMINT activities, and some of these include tools to detect deception and address cognitive bias challenges within the HUMINT domain.

(1) "iCognative" by Brainwave Science: this technology scientifically identifies whether specific information is stored in the human brain by measuring brainwaves, specifically using the P300 brainwave response

mechanism. Unlike a conventional polygraph that detects emotional stress responses associated with lying, "iCognative" determines only the presence of information within the brain. It boasts a claimed accuracy rate of over 99% (Brainwave Science, 2023).

(2) "Paragon X" by Limestone Technologies: this data acquisition system in the polygraph domain is lauded for its performance, reliability, and innovation, offering features such as high retention USB and dual-channel 32-bit capabilities (Limestone Technologies, 2023).

(3) "CVSA III" by NITV Federal Services: a computer voice stress analyser designed for assessment and lie detection applications, "CVSA III" is known to be highly accurate and has been validated through multiple technical and scientific studies (NITV Federal Services, 2023).

(4) "Palantir Gotham and Palantir Foundry" by Palantir Technologies: this software provides Intelligence organisations and LEAs with the ability to unify and integrate various types of data, regardless of size, source, or format, while maintaining data integrity and source system classifications. It also offers tools for refining and managing high-volume datasets, as well as infrastructure for deploying, training, evaluating, and improving Artificial Intelligence (AI) and Machine Learning (ML) solutions. By enhancing human expertise with technology, it enables analysts to spend more time understanding and engaging with data (Palantir Technologies, 2023).

(5) "EyeDetect+" by Converus: this technology detects deception by monitoring and recording physiological activity, similar to a polygraph, along with involuntary eye behaviour changes during a test. It offers a less intrusive and more impartial alternative to traditional polygraph testing, providing credible assessment experts with reliable testing and valid data analysis (Converus, 2023).

(6) "MX908" by 908 Devices: it enhances the capabilities of emergency responders, bomb disposal units, and the military by enabling rapid detection, identification, and monitoring of explosives and their precursors. It is particularly useful for covert meetings and delivers exceptional selectivity and sensitivity for the identification of explosives and precursors (908 Devices, 2023).

These technology solutions for HUMINT support offer valuable insights into various aspects of the specialised and secretive field of

Intelligence gathering. They cover a wide range of topics, from practical tactics and operational management to the personal characteristics, behaviours, human factors, and cognitive and psychological elements involved in HUMINT operations and investigations. These technologies provide support across the entire HUMINT landscape. It is worth noting that some of these technologies also address physical protective security needs in the HUMINT field, including mobile explosive and precursor detection equipment. This equipment is crucial for ensuring the safe screening of venues where high-value covert HUMINT sources meet with their law enforcement, Intelligence agency, or military Intelligence handlers involved in highly sensitive operations. Furthermore, some of these technologies have applications in other Intelligence disciplines. For instance, they can be used to integrate multiple sources of data to create a more comprehensive Intelligence picture. The identification and inclusion of technologies related to voice stress recognition also have broader security applications within the Intelligence Cycle. Voice stress recognition can be employed to assess and identify stress levels in reports from the public, as well as in interviews with witnesses, criminals, and terrorists. These results can significantly enhance the value of the Intelligence being collected, assessed, analysed, and prioritised.

Deception and disinformation detection

Recognising deceptive information has become increasingly challenging, particularly in light of the uncontrollable spread of disinformation, especially on social media platforms. With news and information being widely shared, it has become increasingly essential in the Intelligence field to distinguish between truthful and deceptive information. Intelligence agencies have long focused on disinformation detection as a critical aspect of their work, as well as engaging in their own misinformation and disinformation operations to shield the true nature and intentions of their covert operations. In the recruitment phase of developing new HUMINT sources, the ability to detect disinformation and deception is a vital skill. This skill is essential for assessing risks and ensuring that recruited individuals do not have

hostile intentions or ulterior motivations that could compromise the integrity of HUMINT sources. Furthermore, ongoing assessment of the integrity of HUMINT sources during their operational deployment is a crucial component of effective source handling and management. Any advancements in deception detection tools, techniques, and technologies are of direct interest to the field of HUMINT, as they can contribute to enhancing the discipline's effectiveness in identifying and mitigating deception and disinformation.

Expert.AI, formerly known as Expert System, has developed a dedicated technique for recognising disinformation based on a technology named "COGITO" (Expert.AI, 2019). This technique combines rule-based semantic engines and ML algorithms, using a hybrid approach. The process involves extracting stylometric features from textual content, which are then used to train ML models. Computational Stylometry is a field in Computational Linguistics that focuses on analysing the literary style of text (Zheng, Li, Chen, & Huang, 2006). It uses techniques to identify various personality traits and characteristics of the author based on their writing style. These characteristics may include sociological factors like age, gender, and education level, as well as psychological factors like personality traits, mental health, and whether the author is a native speaker (Daelemans, 2013). Deceptive texts exhibit specific stylometric features that differentiate them from truthful ones. It is worth noting that stylometric analysis focuses on the unintentional choices made by the writer in their text, as these features are inherent to their writing style and cannot be easily manipulated. This approach allows for the detection of disinformation based on the unique stylometric characteristics of deceptive texts, enabling more accurate identification and mitigation of deceptive content.

Next-generation deception detection for HUMINT is incorporating non-invasive brainwave technology, such as the P300 response, which is being adopted by LEAs around the world. For instance, the Dubai Police Force recently made a significant breakthrough in a murder case by using brainwave science technology to measure the brain waves of suspects, marking a notable use of innovative neuroscience tools in crime investigations (Staniforth, 2021). The origins of P300 technology can be traced back to a discovery in 1965 when scientists observed

distinctive electrical activity in the brain occurring 300 milliseconds after a person saw something familiar during electroencephalogram tests. This response was termed "P300". While the neurological basis of this response remains unclear, P300 has been used as a foundation for Brain Fingerprinting (BF) in neuroscientific research. BF detects concealed information stored in the human brain by measuring brainwaves. P300 responds to words or images relevant to a crime scene or specific knowledge, making it a valuable tool for investigators to detect information stored in the brain, especially related to criminal activities or terrorism. The P300 deception detection technology has demonstrated resilience against deceptive tactics, making it less prone to false positives compared to traditional polygraph deception techniques. This advancement has the potential to bring significant improvements to the criminal justice system, reducing the risk of miscarriages of justice and enhancing the protection of crime victims (Staniforth, 2021).

Technology and cognitive biases in HUMINT

Psychology plays a significant role in understanding HUMINT because human minds are not without their flaws. Psychological mechanisms, such as cognitive biases, can lead to unexpected errors and unintended consequences in the realm of Intelligence. Cognitive biases are described as "patterns of deviation in judgment that occur in particular situations, leading to perceptual distortion, inaccurate judgment, illogical interpretation, or what is broadly called irrationality" (Tversky & Kahneman, 1973) or as "mental errors caused by individuals' simplified information processing strategies" (Heuer, 1999). They can affect the entire Intelligence Cycle, from data collection to processing, analysis, and dissemination: e.g., they can lead to misinterpretation of the significance of data or misattribution of causal relationships between data, they can produce too much trust in Information Technology (IT) tools. In recent years, EU research community has been actively engaged in addressing and countering cognitive biases in the field of Intelligence analysis. In particular, it has examined the relationship between cognitive biases and various phases of the Intelligence Cycle. This includes stages like planning and direction, collection, processing,

analysis, and dissemination. The findings of these studies have indicated that cognitive biases can affect analysts horizontally across all phases of the Intelligence Cycle, highlighting the importance of addressing and countering biases at every stage of the Intelligence process. This involvement is exemplified by projects such as the Law Enforcement Intelligence Learning Applications (LEILA) (European Commision, 2016) and the REduction of COgnitive Biases in Intelligence Analysis (RECOBIA) (European Commission, 2016) These projects have been instrumental in developing strategies and tools to mitigate the impact of cognitive biases on intelligence analysis.

Some examples of the reported cognitive biases include the following.

(1) "Confirmation Bias": the tendency to seek or interpret information in a way that confirms preconceptions.

(2) "Representativeness": the tendency to classify based on partial similarities to something typical or representative.

(3) "Availability Heuristic": the tendency to estimate what is more likely based on what is more available in memory, often biased toward vivid, unusual, or emotionally charged examples.

(4) "Anchoring": the tendency to rely too heavily on past reference points or a single piece of information when making decisions. Additionally, there are biases that impact specific phases of the Intelligence analysis process, such as the "Focusing Effect" and the "Illusionary Correlation": the first is the tendency to place too much importance on one aspect of an event, potentially causing errors in predicting future outcomes; the latter leads to the inaccurate perception or memory of a relationship between two unrelated events. Furthermore, the use of IT tools to process and make sense of available data has introduced significant advantages but has also amplified the effects of cognitive biases or triggered new biases (Pirolli & Card, 2005). For instance, the use of search and filtering technologies can lead to biases by assuming that collected data genuinely reflect reality or perceiving a data set as complete, which may lead to a cessation of further investigation.

To mitigate the impact of cognitive biases, a variety of software tools and technological solutions are at the disposal of analysts. Some of

these technologies automatically display large volumes of information in various formats, allowing analysts to efficiently explore and examine data. Additionally, visualisation tools aid analysts in making more rapid and accurate inferences by revealing patterns and connections in the data. Other tools are adept at uncovering relationships between events across time and space, as well as identifying interconnections among various entities, such as individuals, organisations, locations, and dates. This category encompasses a wide range of tools, including those supporting structured analytical techniques, Decision Support Systems (DSS), Group Support Systems (GSS), collaborative analysis tools, serious games, data mining tools, statistical software, text mining tools, and risk analysis software. Collectively, all these tools and solutions play a critical role in minimising the impact of cognitive biases in the field of Intelligence analysis, enabling analysts to provide more objective and well-informed assessments.

The role of HUMINT in the digital era: discussion and recommendations

The landscape of the Intelligence gathering has indeed seen significant transformations due to technological advancements, which have raised questions about the standing and priority of HUMINT in the Intelligence Cycle. These advancements have the potential to diminish the value of HUMINT, particularly in an age of high-tech surveillance and widespread use of social media for instant mass communication. New AI-powered surveillance platforms, combined with emerging bio and facial recognition technologies, have created a challenging environment for covert HUMINT sources operating in public spaces. The proliferation of private security and advanced Closed-Circuit Television (CCTV) digital systems further increases the risk of source compromise, making the collection of HUMINT more challenging. Technology is now not only used for surveillance but also for counter-surveillance of potential targets and HUMINT sources. This includes monitoring online activities, tracking movements through Global Positioning System (GPS), and other forms of electronic surveillance. As a result, the gathering of HUMINT has become increasingly digital and

virtual. HUMINT handlers are adopting new developments in encrypted digital communications to mitigate these risks.

Technology facilitates communication between human sources and Intelligence operators, regardless of their physical locations. This includes the use of encrypted messaging, email, video conferencing, and other forms of online communication. While technology has presented challenges to traditional HUMINT, it also offers opportunities for more secure and efficient communication between sources and Intelligence personnel.

The use of new technology for surveillance may initially frustrate HUMINT operations by potentiailly compromising the identity of the informant or the location of covert meetings, but the Intelligence community responds by introducing, implementing, and integrating tools, techniques, and technologies to counter these challenges. Technological advancements have a profound impact on both HUMINT and the broader Intelligence Cycle. For instance, technology is instrumental in analysing vast volumes of data, which includes information collected through HUMINT operations. Advanced analytical techniques, such as ML, are employed to identify patterns and anomalies that might signify potential security threats. Furthermore, technology is used to collect, store, and manage HUMINT data, encompassing digital records, images, and various types of information. Secure databases and other information management systems are used to uphold the confidentiality and integrity of this data. In addition, technology is applied for biometric identification of individuals, including facial recognition and fingerprint scanning, to support the identification of potential targets and threat actors. The continuous integration of technology enhances the capabilities of Intelligence agencies and their ability to respond to evolving security challenges.

HUMINT indeed holds substantial value in the realm of information security, with a particular focus on threat Intelligence, incident response, and cybercrime investigations. It provides critical information and insights that may not be accessible through technical means alone, contributing to enhanced effectiveness and efficiency in information security efforts. As cyber threats grow in sophistication and

complexity, the need for HUMINT to complement technical measures is likely to become even more crucial. In essence, the utilisation of HUMINT in information security, whether for public authority services or private sector businesses, is expected to maintain its significance. Moreover, as AI and automation continue to expand their roles in information security, the discipline of HUMINT may become even more valuable in identifying and mitigating emerging threats. A well-balanced integration of technical capabilities and human resources is essential for effectively utilising HUMINT in information security. By harnessing the strengths of both approaches, security organisations, Intelligence agencies, and LEAs can enhance their ability to safeguard themselves and their stakeholders from the ever-evolving threats in the digital landscape.

Conclusions

The increased digitisation of the Intelligence gathering discipline has raised concerns among some national security policymakers. They have criticised defence, Intelligence organisations, and LEAs for appearing to deprioritise, under-resource, or neglect HUMINT in favour of more readily accessible sources of information. In the past decade, the proliferation of affordable, sophisticated high-tech surveillance technology has expanded globally, particularly in the realms of audio and video surveillance. Consequently, there has been a perception that the value and contribution of HUMINT to the overall Intelligence landscape have been diminished. To some extent, the widespread availability and decreasing cost of surveillance and public monitoring technology have led to increased investment and reliance on remote Intelligence collection through modern technological disciplines like SIGINT and IMINT. Additionally, the growth of OSINT, which involves Intelligence derived from publicly available information, has enriched the capabilities of LEAs. OSINT provides access to actionable Intelligence, enhancing decision-making, tasking, and coordination activities. The concerns raised by national security policymakers underscore the evolving nature of Intelligence gathering and the need for a balanced approach that leverages both traditional HUMINT methods and contemporary

technological Intelligence disciplines to address the complex and multifaceted challenges in the digital age.

The relentless pursuit of Intelligence to understand new and emerging threats has fuelled the growth of OSINT as a vital intelligence discipline in the digital age. However, the increasing availability of publicly accessible information should not diminish the value, standing, and investment in HUMINT. To effectively prevent various contemporary security threats, avoid strategic surprises, and unveil what hostile actors seek to keep hidden, security operations must remain Intelligence-led and include HUMINT as an integral component. In light of this, HUMINT retains a crucial role in informing the Intelligence Cycle. While recent advancements in ubiquitous surveillance have presented new challenges, there is a need to ensure that HUMINT remains relevant and effective in the digital age. One important step is to review current HUMINT doctrine to align it with the strategic Intelligence requirements of government agencies, ensuring the safety and security of EU Member States. Balancing HUMINT with other Intelligence disciplines is also essential for addressing the evolving threat landscape comprehensively.

Acknowledgement: This work was supported by the NOTIONES (iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and acadEmia actorS) project, that has received funding from the European Unions' Horizon 2020 research and innovation programme under grant agreement No. 101021853. The objective of the NOTIONES project is to build a pan-European network of practitioners from the security and Intelligence services, from the industry – including SMEs – and from the Academia, with the objective to enhance their interaction and identify specific technology and innovation requirements, needs, expectations and gaps.

References:

1. 908 Devices. (2023). MX908. Retrieved September 12, 2023, from 908 Devices, https://908devices.com/products/mx908/.

2. Brainwave Science. (2023). iCognitive. Retrieved September 12, 2023, from Brainwave Science, https://brainwavescience.com/icognative/.

3. Burkett, R. (2013, March). "Rethinking an Old Approach. An alternative Framework for Agent Recruitment: From MICE to RASCLS." *Studies in Intelligence*, 57(1), 7-17. Retrieved September 4, 2023, from https://www.cia.gov/static/Alt-Framework-Agent-Recruitment.pdf.

4. Clark, R. (2013). *Intelligence Collection*. Washington, D.C., USA: CQ Press.

5. Converus. (2023). *The World's First Automated Polygraph: EyeDetect+.* Retrieved September 12, 2023, from Converus, https://converus.com/eyedetectplus/.

6. CQR Company. (2023, February 14). *HUMINT*. Retrieved September 5, 2023, from CQR Company, https://cqr.company/pentesting-process/humint/.

7. Daelemans, W. (2013). "Explanation in Computational Stylometry." In International Conference on Intelligent Text Processing and Computational Linguistics (pp. 451-462). Springer. Retrieved September 10, 2023.

8. European Commision. (2016, December 5). *Law Enforcement Intelligence Learning Application*. Retrieved September 6, 2023, from European Commission, https://cordis.europa.eu/project/id/608303.

9. European Commission. (2016, February 18). *REduction of COgnitive BIAses in Intelligence Analysis*. Retrieved September 6, 2023, from European Commission, https://cordis.europa.eu/project/id/285010#:~:text=Objective,affect%20the%20practice%20of%20intelligence&text=%2D%20organization.

10. Expert.AI. (2019, March 19). *Expert System Annuncia la Nuova Versione della Piattaforma di Intelligenza Artificiale COGITO*. Retrieved September 10, 2023, from Expert.AI, https://www.expert.ai/it/expert-system-annuncia-la-nuova-versione-della-piattaforma-di-intelligenza-artificiale-cogito/.

11. Heuer, R. (1999). *Pyschology of Intelligence Analysis.* Retrieved September 5, 2023, from Central Intelligence Agency, https://www.cia.gov/static/Pyschology-of-Intelligence-Analysis.pdf.

12. Limestone Technologies. (2023). *Polygraph Pro Suite Products.* Retrieved September 12, 2023, from Limestone Technologies, https://limestonetech.com/polygraph-pro-suite-products/.

13. NATO Allied Command Transformation. (2023, July 10). *NATO Centres of Excellence – Human Intelligence.* Retrieved September 4, 2023, from NATO

Allied Command Transformation, https://www.act.nato.int/article/nato-coes-humint/.

14. NATO Standardization Office. (2015, August 20). *HUMINT.* Retrieved September 4, 2023, from Official NATO Terminology Database, https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en.

15. NITV Federal Services. (2023). *CVSA III*. Retrieved September 12, 2023, from NITV Federal Services, https://www.cvsa1.com/products.htm.

16. Palantir Technologies. (2023). *Intelligence*. Retrieved September 12, 2023, from Palantir Technologies, https://www.palantir.com/offerings/intelligence/.

17. Pigeon, L., Beamish, C., & Zybala, M. (2002, September). Pigeon, L., Beamish, C.J., & Zybala, M. (2002). *HUMINT Communication Information Systems for Complex Warfare.* Retrieved September 12, 2023, from 7th International Command and Control Research and Technology Symposium (ICCRTS 2002), https://apps.dtic.mil/sti/pdfs/ADA467646.pdf.

18. Pirolli, P., & Card, S. (2005, May). "The Sensemaking Process and Leverage Points for Analyst Technology as Identified Through Cognitive Task Analysis." Proceedings of International Conference on Intelligence Analysis, 5(1), 2-4. Retrieved September 5, 2023.

19. Sano, J. (2015, Fall/Winter). "The Changing Shape of HUMINT Guide to the Study of Intelligence." *AFIO Intelligencer Journal*, 21(3), 77-80. Retrieved September 4, 2023, from https://www.afio.com/publications/SANO%20John%20on%20The%20Changing%20Shape%20of%20HUMINT%20Pages%20from%20INTEL_FALLWINTER2015_Vol21_No3_FINAL.pdf.

20. Staniforth, A. (2021, March 25). *Murder Investigation: The Police Application of Brainwave Technology*. Retrieved September 12, 2023, from Policing Insight, https://policinginsight.com/features/innovation/murder-investigation-the-police-application-of-brainwave-technology/.

21. Tversky, A., & Kahneman, D. (1973, September). "Availability: A Heuristic for Judging Frequency and Probability." *Cognitive Psychology*, 5(2), 207-232. Retrieved September 5, 2023.

22. US Defense Intelligence Agency. (2008, March). *A Tradecraft Primer: Basic Structured Analytic Techniques*. Retrieved September 5, 2023, from US Defense Intelligence Agency, https://www.dia.mil/FOIA/FOIA-Electronic-Reading-Room/FileId/161442/.

23. US Department of the Army. (2020, January). *Intelligence Analysis (ATP 2-33.4).* Retrieved September 5, 2023, from Federation of American Scientists: Intelligence Resource Program, https://irp.fas.org/doddir/army/atp2-33-4.pdf.

24. US Office of the Director of National Intelligence. (2023). *What Is Intelligence?* Retrieved September 4, 2023, from US Office of the Director of National Intelligence, https://www.dni.gov/index.php/what-we-do/what-is-intelligence.

25. Zheng, R., Li, J., Chen, H., & Huang, Z. (2006). "A Framework for Authorship Identification of Online Messages: Writing-Style Features and Classification Techniques." *Journal of the American Society for Information Science and Technology*, 57(3), 378-393. Retrieved September 10, 2023.