Media, Society, Security, and Cyberspace:
Is there a need for HUMINT in the age of digital intelligence?

2401049

Joshua.A.J.McManus

The University of Buckingham

BA (Hons) Security, Intelligence, and Cyber

Table of Contents

SECTION 1:

MAIN BODY

Introduction

In the contemporary era, the digital world has grown beyond its own restraints. In reference to the question of whether or not it has grown beyond the need for Human Intelligence (HUMINT), we must first define some key words. Data is that of facts and numbers, pieces of objectivity in a subjective world. Information is that of data in context, providing a means to make those facts readable. Intelligence stands out of these three as 'information actionable', key insights that allow for the tides to turn. Intelligence is often categorised by its nature, for example Open Source Intelligence (OSINT) is that of insights gathered from publicly available (sometimes by obfuscated and obscured means) information, while Signals Intelligence (SIGINT) comes from decrypting electronic signals and communications, digital and analogue alike, to better understand an adversary's intentions.

With the increase in the importance of technology and the growth of social media, OSINT operations have become an invaluable tool for not only the global intelligence community, but for private trans-national corporations (TNCs) alike, allowing for a rapidly growing private sector to develop an estimated global market worth over $18 Billion (USD)[1]. However, while the digital era has fundamentally shifted the scale of data collection, it has not altered the fundamental nature of human intent. This essay will outline the critical role Human Intelligence (HUMINT) plays as the psychological anchor, by examining the limitations of digital-only approaches and the necessity of access to the most sensitive of places, hypothesising that HUMINT remains an indispensable and necessary component of a robust All Source Intelligence framework, especially in the digital age.

[1] Mordor Intelligence (2025). Open Source Intelligence (OSINT) Market Size, Report & Share Analysis 2030. [online] Mordorintelligence.com. Available at: https://www.mordorintelligence.com/industry-reports/open-source-intelligence-market [Accessed 13 Mar. 2026].

The value of HUMINT

Historically, Human Intelligence has served as the quintessential methodology for providing contextual depth, validation, and nuanced insight into conflict dynamics. While the instruments of statecraft have evolved, the fundamental necessity of comprehending the human dimension remains constant. As the Song Dynasty military historian Zhang Yu observed in his commentary on Sun Tzu, "knowing the enemy enables you to take the offensive; knowing yourself enables you to stand on the defensive"[2]. This ancient principle illuminates a profoundly modern reality: whereas digital collection methodologies can effectively map the 'what' and the 'where' of adversarial activity, HUMINT possesses the unique capacity to access what might be termed the 'inner space' of human motivation, intentionality, and deception.

The critical significance of this 'human gap' finds its most instructive illustration in the catastrophic intelligence failure concerning Iraq's alleged Weapons of Mass Destruction programmes. In this instance, the intelligence community possessed an abundance of technical data: high-resolution satellite imagery and extensive intercepted communications traffic. Yet the conspicuous absence of reliable human sources embedded within the Iraqi regime's inner circles meant there existed no mechanism to confirm or authoritatively refute the actual strategic intent underpinning Saddam Hussein's actions. The resulting misinterpretation demonstrates that technical intelligence, when divorced from human validation, remains peculiarly susceptible to catastrophic analytic failure[3].

A detailed examination of the Iraq WMD case reveals something more nuanced than simple 'absence' of HUMINT. The intelligence community did possess human sources, but their reporting was often second-hand, unreliable, or simply misinterpreted. The Butler Review[4] later highlighted how reporting from a source codenamed 'Curveball' (a defector whose claims about weapons factories were later discredited)[5] was fed into the intelligence machine without adequate human validation from alternative sources. This suggests that the problem was not merely the presence of HUMINT, but the quality of its handling and the

---

[2] 孫子 (500BC). 孫子兵法 (The Art of War) - Chapter III, Attack By Stratagem. [online] Available at: https://www.mv.helsinki.fi/home/jetsu/suntzu.pdf [Accessed 19 Mar. 2026].

[3] Pike, J. (2026). REPORT ON THE U.S. INTELLIGENCE COMMUNITY'S PREWAR INTELLIGENCE ASSESSMENTS ON IRAQ. [online] Globalsecurity.org. Available at: https://www.globalsecurity.org/intell/library/congress/2004_rpt/iraq-wmd-intell_toc.htm [Accessed 19 Mar. 2026].

[4] The Rt Hon Butler, F. (2004). Review Of Intelligence On Weapons Of Mass Destruction: Implementation Of Its Conclusions. [online] Available at: https://assets.publishing.service.gov.uk/media/5a79e18ded915d042206bb61/wmdreview.pdf [Accessed 19 Mar. 2026].

[5] Chulov, M. and Pidd, H. (2011). Curveball: How US was duped by Iraqi fantasist looking to topple Saddam. [online] the Guardian. Available at: https://www.theguardian.com/world/2011/feb/15/curveball-iraqi-fantasist-cia-saddam [Accessed 19 Mar. 2026].

analytical frameworks applied to it. The Iraq case study raises an uncomfortable question for HUMINT: is human intelligence inherently valuable, or does its value depend entirely on the capability to recruit and assess the right sources? This creates a challenge to the assumption that 'more' human intelligence automatically equates to 'better' strategic understanding.

Beyond the battlefield, the insider threat remains a domain where digital monitoring frequently proves inadequate. Figures such as Edward Snowden[6] or John Kiriakou[7] exemplify cases where unauthorised disclosures present a threat greater than or equal to the information disclosed. Identifying the subtle behavioural indicators that precede such disclosures requires precisely the nuanced understanding that only human vetting and sustained interpersonal relationships can provide. A 2024 Romanian Intelligence Studies Review states, "HUMINT sources continue to play a fundamental role in Intelligence Collection, analysis, and interpretation, due to their ability to recall, recognise, contextualise, and establish connections between different information"[8]. This is a recognition that human beings remain the only collection discipline capable of accessing the interior world of intent, as digital systems are completely void on this environment.

Yet even this argument requires exploration. Critics might counter that psychological profiling and AI-driven behavioural analysis are rapidly advancing, potentially offering windows into intent that does not require risky human source recruitment. However to counter this, these tools require training data derived from human behaviour and, in high-stakes national security contexts, the behavioural baselines of hostile actors are precisely what intelligence agencies lack. AI can identify patterns in known data; it cannot, without human cueing, know what it does not know. Furthermore, The Intelligence Review also states that "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"[9]. The very biases that complicate human judgment also constitute the terrain that only human sources can navigate.

---

[6] Ray, M. (2019). National Security Agency | History, Role, & Surveillance Programs. In: Encyclopædia Britannica. [online] Available at: https://www.britannica.com/topic/National-Security-Agency [Accessed 19 Mar. 2026].

[7] WhistleBlower (n.d.). John Kiriakou, A Biography. [online] Government Accountability Project. Available at: https://whistleblower.org/bio-john-kiriakou/ [Accessed 19 Mar. 2026].

[8] Frascà, D. and others (2024). The Role of Human Intelligence in the Age of Digital Technologies. Romanian Intelligence Studies Review, (1(31)), pp.5–24.

[9] Ibidem (Footnote № 8)

The rise of Digital Intelligence

The most compelling argument for the diminished relevance of HUMINT resides in the rapidly increasing successes of digital collection methodologies. In a society where human interaction is increasingly mediated through digital interfaces, the secrets once closely held by individuals are now frequently accessible through systematic exploitation of cyberspace. Proponents of a digital-first intelligence doctrine argue persuasively that OSINT and SOCMINT offer safer, more cost-effective, and more comprehensive alternatives to the inherently high-risk enterprise of recruiting and managing human assets.

The extraordinary scale of this capability was notably highlighted by disclosures surrounding the National Security Agency's bulk metadata programmes. Systems such as XKeyscore[10] demonstrated an unprecedented capacity to synthesise vast quantities of internet traffic, email records, and telephony metadata, constructing intricate social network maps with remarkable precision. Such technical reach enables intelligence services to identify associational patterns and behavioural routines without exposing agents to physical risks in hostile operational environments. Furthermore, in 'denied areas' such as North Korea or Iran, where operational conditions prove restrictive for traditional espionage, technical disciplines including Geospatial and Signals Intelligence provide persistent surveillance capabilities that human sources cannot reliably guarantee.

Sir David Omand, a pivotal figure in the conceptualisation of Social Media Intelligence (SOCMINT)[11], argued as early as 2012 that the 'digital footprint' has fundamentally reconfigured the intelligence requirement. Omand suggested that the state assumes a positive duty to utilise these "new signals"[12] for public protection, suggesting that sophisticated social media analysis can provide real-time insights into societal trends and emerging threat vectors. The 2011 UK riots demonstrated that police had failed to appreciate the opportunities provided by social media used by members of the public who wanted to alert authorities. This is not an argument for more surveillance, but for a reconceptualisation of intelligence as something that could emerge organically from the digital public sphere.

Yet this strategic pivot toward the digital domain introduces significant challenges that warrant careful examination. The first is the 'floodgate issue' (Also referred to as

[10] Greenwald, G. (2013). XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. [online] the Guardian. Available at: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data [Accessed 19 Mar. 2026].

[11] Norton-Taylor, R. (2012). Former spy chief calls for laws on online snooping. [online] the Guardian. Available at: https://www.theguardian.com/technology/2012/apr/24/former-spy-chief-laws-snooping?newsfeed=true [Accessed 19 Mar. 2026].

[12] Omand, D., Bartlett, J. and Miller, C. (2012). Introducing Social Media Intelligence (SOCMINT). Intelligence and National Security, 27(6), pp.801–823. doi:https://doi.org/10.1080/02684527.2012.716965.

Information Overload), an over-reliance on digital collection risks overwhelming analytical capacity with a 'tsunami' of data, substantial portions of which are either irrelevant to intelligence requirements or intentionally deceptive[13]. As Mattermost's analysis of the modern intelligence environment notes, "OSINT thrives on speed and accessibility, but its credibility depends on validation. HUMINT requires time and discretion, shaped by trust and context. SIGINT delivers technical precision, but at the cost of overwhelming volume"[14]. This data saturation paradoxically impedes rather than enhances the intelligence production process.

The second challenge is the critical distinction between data and intelligence that technical collection alone cannot bridge. While a technical intercept may successfully record communications between two high-interest targets, it frequently fails to capture the essential 'why' underpinning that interaction. Without the contextual nuance that human perspective provides, technical data suffers from what may be termed the 'so-what?' problem: the inability to translate observation into strategic significance. Digital metadata might identify an associational connection, but it requires the interpretative framework of HUMINT to determine whether that connection represents benign coincidence or significant security concern. These challenges showcase that while the age of digital intelligence brings about new opportunities, these opportunities must be exploited and enhanced by other forms of intelligence in order to ensure authenticity and applicability.

---

[13] Bouher, K. (2026). Information overload - Digital Threat Digest. [online] PGI. Available at: https://www.pgitl.com/insights/information-overload-digital-threat-digest [Accessed 20 Mar. 2026].

[14] Brown, C. (2025). Signals in Sync: OSINT, HUMINT, SIGINT, GEOINT in the Modern Intelligence Environment. [online] Mattermost.com. Available at: https://mattermost.com/blog/signals-in-sync-modern-intelligence-environment/ [Accessed 19 Mar. 2026].

All Source Intelligence

The debate concerning the rivalry between digital and human intelligence methodologies frequently rests upon a fundamentally false dichotomy. In practice, the intelligence sector is not defined by the replacement of HUMINT in favour of technology based approaches, but rather by the complex synthesis of intelligence collection methods creating what is known as 'All Source Intelligence'. The requirement for an integrated framework is rooted in the relationship between technical breadth and human depth, but this symbiosis is far more contested and difficult than is often acknowledged.

The success of this approach is most clearly demonstrated through the idea that digital intelligence provides human operations with key insights, and therefore both are equally important and necessary. An example of the value of All Source intelligence, in a digital era, can be seen through AI-driven analysis of financial transaction patterns and communication metadata, which can identify anomalies that highlight previously unknown facilitators within hostile networks. This digital lead enables an intelligence officer to focus efforts on a specific targets with enhanced confidence. However, this apparently seamless sequence conceals significant friction. According to research completed by the US Airforce Institute of Technology (AFIT) intelligence analysts face profound challenges in "quantitatively representing uncertainty in text-based intelligence reporting (i.e., HUMINT, OSINT, SIGINT)"[15]. The very act of integrating different intelligence disciplines requires analytical frameworks that can weigh and compare sources with fundamentally different natures. How does one weigh a SIGINT intercept with 95% technical confidence against a HUMINT report from a source of uncertain reliability? As there is no objective answer, the judgement remains human.

Conversely, HUMINT frequently serves as the essential 'cueing' mechanism that directs and focuses technical sensors. A report from a Covert Human Intelligence Source (CHIS) regarding a high-level meeting in a specific location provides the necessary targeting data to task assets or activate SIGINT capabilities. Without this initial human insight, the vast technical apparatus of the state would remain fundamentally undirected, and yet even this relationship is fraught. As NV5's analysis of cross-domain orchestration notes, "the word 'stovepipes' has long described one of the greatest barriers to speed and clarity. Each intelligence discipline has traditionally operated in isolation. Valuable insights too often remain locked within their respective domains"[16]. The institutional challenge of breaking down these stovepipes, creating workflows where HUMINT cues SIGINT and SIGINT validates HUMINT in real time, remains as significant as the technical challenge.

---

[15] Nesmith, A.D. (2023). Quantitative Modeling of Text-Based Intelligence Source Uncertainty. [online] AFIT Scholar. Available at: https://scholar.afit.edu/etd/7327/ [Accessed 22 Mar. 2026].

[16] NV5 Global Incorporated (2025). Orchestrating Intelligence Across Domains for a Unified Multi-Int Enterprise. Available at: https://www.nv5.com/news/orchestrating-intelligence/ [Accessed 22 Mar. 2026].

Showcasing this is the operation to locate Osama bin Laden[17], which serves as the definitive case study of All Source synthesis. While often treated as the cornerstone of All Source, it also reveals the tensions inherent in integration. The intelligence thread began with HUMINT, specifically the interrogation of detainees who identified a key courier within the bin Laden network. This human-derived lead was then meticulously expanded through SIGINT (tracking communications patterns) and GEOINT (Geographical Intelligence - analysing the distinctive characteristics of the Abbottabad compound)[18]. Yet this was not a frictionless process as analysts debated whether the courier lead was credible, dragging the process on for several months if not years. Furthermore, Different intelligence agencies prioritised different sources. The final mission represented a hard-won victory, because of the struggle to integrate them all the forms of intelligence gathered on Osama bin laden. Neither element alone would have sufficed, but together the synthesis was achieved through persistence and the willingness to take risks.

Looking toward the future, the reliance upon HUMINT appears unlikely to diminish, primarily because the fundamental nature of the threat remains persistently human-centric. Even in the modern age, the most fundamentally vulnerable component in any cybersecurity operation is always that of the human user. The prevalence of social engineering and phishing attacks underscores that the most effective method of breaching a digital network is to exploit the psychological vulnerabilities of the person operating it. Understanding these vulnerabilities requires precisely the nuanced grasp of human behaviour that only HUMINT can provide. This is not an argument of HUMINT over SIGINT, but rather it is an argument for ensuring that intelligence backs up intelligence. All Source intelligence is a recognition that different intelligence disciplines answer different questions, and that the relationship between them is not a settled hierarchy. As technology evolves, it will undoubtedly provide new techniques for collection, but it cannot justify the abandonment of the human element. Instead, the evolution of cyberspace will continue to feed a cycle wherein technology enables traditional intelligence to flourish, even as it transforms the very meaning of ‘human intelligence’.

---

[17] DAHL, E.J. (2014). Finding Bin Laden: Lessons for a New American Way of Intelligence. Political Science Quarterly, [online] 129(2), pp.179–210. Available at: https://www.jstor.org/stable/43828649.

[18] Boyle, A. (2011). How satellites helped get Osama. [online] NBC News. Available at: https://www.nbcnews.com/science/cosmic-log/how-satellites-helped-get-osama-flna6c10403193 [Accessed 20 Mar. 2026].

Conclusion

As stated, the debate on whether there is a need for HUMINT in the age of digital intelligence is fundamentally flawed, as it requires a complete separate of intelligence collection methods (the 'INTs) resulting in a false dichotomy. While digital intelligence (as the technology required to analyse it) has advanced to the point where the term OSINT has entered the everyday vocabulary[19], it has yet to become a powerful enough tool to make Human Intelligence redundant. This essay, via exploring case studies (such as the hunt for Osama bin Laden and the Iraq WMD case study) as well as commentary from experts in the field, showcases the value of HUMINT and its irreplaceable nature even in the face of the modern era's reliance on digital systems.

The digital era has expanded the 'how' and the 'what' of intelligence collection to an almost infinite scale, but it has not provided a technological substitute for the interpretative 'why', the understanding of human motivation that prevents strategic surprise. By combining the best of both digital and more 'analogue' HUMINT methods, the production of an All Source intelligence approach allows for neither side to run dry or to overpower the other, and thus it can be stated that HUMINT remains an indispensable and necessary component of a robust All Source Intelligence framework, especially in the digital age.

THE END.

[19] Google Trends (2026). Search Term; OSINT. [online] Google.com. Available at: https://trends.google.com/explore?q=OSINT&date=all&geo=Worldwide [Accessed 22 Mar. 2026].

SECTION 2:

Accreditation.

Sources Used

1. Bouher, K. (2026). *Information overload - Digital Threat Digest*. [online] PGI. Available at: https://www.pgitl.com/insights/information-overload-digital-threat-digest [Accessed 20 Mar. 2026].
2. Boyle, A. (2011). *How satellites helped get Osama*. [online] NBC News. Available at: https://www.nbcnews.com/science/cosmic-log/how-satellites-helped-get-osama-flna6c10403193 [Accessed 20 Mar. 2026].
3. Brown, C. (2025). *Signals in Sync: OSINT, HUMINT, SIGINT, GEOINT in the Modern Intelligence Environment*. [online] Mattermost.com. Available at: https://mattermost.com/blog/signals-in-sync-modern-intelligence-environment/ [Accessed 19 Mar. 2026].
4. Chulov, M. and Pidd, H. (2011). *Curveball: How US was duped by Iraqi fantasist looking to topple Saddam*. [online] the Guardian. Available at: https://www.theguardian.com/world/2011/feb/15/curveball-iraqi-fantasist-cia-saddam [Accessed 19 Mar. 2026].
5. DAHL, E.J. (2014). Finding Bin Laden: Lessons for a New American Way of Intelligence. *Political Science Quarterly*, [online] 129(2), pp.179–210. Available at: https://www.jstor.org/stable/43828649.
6. Frascà, D. and others (2024). The Role of Human Intelligence in the Age of Digital Technologies. *Romanian Intelligence Studies Review*, (1(31)), pp.5–24.
7. Google Trends (2026). *Search Term; OSINT*. [online] Google.com. Available at: https://trends.google.com/explore?q=OSINT&date=all&geo=Worldwide [Accessed 22 Mar. 2026].
8. Greenwald, G. (2013). *XKeyscore: NSA tool collects 'nearly everything a user does on the internet'*. [online] the Guardian. Available at: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data [Accessed 19 Mar. 2026].
9. Mordor Intelligence (2025). *Open Source Intelligence (OSINT) Market Size, Report & Share Analysis 2030*. [online] Mordorintelligence.com. Available at: https://www.mordorintelligence.com/industry-reports/open-source-intelligence-market [Accessed 13 Mar. 2026].
10. Nesmith, A.D. (2023). *Quantitative Modeling of Text-Based Intelligence Source Uncertainty*. [online] AFIT Scholar. Available at: https://scholar.afit.edu/etd/7327/ [Accessed 22 Mar. 2026].
11. Norton-Taylor, R. (2012). *Former spy chief calls for laws on online snooping*. [online] the Guardian. Available at: https://www.theguardian.com/technology/2012/apr/24/former-spy-chief-laws-snooping?newsfeed=true [Accessed 19 Mar. 2026].

12. NV5 Global Incorporated (2025). Orchestrating Intelligence Across Domains for a Unified Multi-Int Enterprise. Available at: https://www.nv5.com/news/orchestrating-intelligence/ [Accessed 22 Mar. 2026].
13. Omand, D., Bartlett, J. and Miller, C. (2012). Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security*, 27(6), pp.801–823. doi:https://doi.org/10.1080/02684527.2012.716965.
14. Pike, J. (2026). *REPORT ON THE U.S. INTELLIGENCE COMMUNITY'S PREWAR INTELLIGENCE ASSESSMENTS ON IRAQ*. [online] Globalsecurity.org. Available at: https://www.globalsecurity.org/intell/library/congress/2004_rpt/iraq-wmd-intell_toc.htm [Accessed 19 Mar. 2026].
15. Ray, M. (2019). National Security Agency | History, Role, & Surveillance Programs. In: *Encyclopædia Britannica*. [online] Available at: https://www.britannica.com/topic/National-Security-Agency [Accessed 19 Mar. 2026].
16. 孫子 (500BC). *孫子兵法 (The Art of War) - Chapter III, Attack By Stratagem.* [online] Available at: https://www.mv.helsinki.fi/home/jetsu/suntzu.pdf [Accessed 19 Mar. 2026].
17. The Rt Hon Butler, F. (2004). *Review Of Intelligence On Weapons Of Mass Destruction: Implementation Of Its Conclusions*. [online] Available at: https://assets.publishing.service.gov.uk/media/5a79e18ded915d042206bb61/wmdreview.pdf [Accessed 19 Mar. 2026].
18. WhistleBlower (n.d.). *John Kiriakou, A Biography.* [online] Government Accountability Project. Available at: https://whistleblower.org/bio-john-kiriakou/ [Accessed 19 Mar. 2026].

Media, Society, Security, and Cyberspace:
Is there a need for HUMINT in the age of digital intelligence?

2401049
Joshua.A.J.McManus
The University of Buckingham
BA (Hons) Security, Intelligence, and Cyber