Foundations of Intelligence Organisations and Structures:

The Importance of "All-Source Intelligence" -

Assess the advantages and disadvantages of HUMINT, SIGINT, and OSINT [DRAFT]

Joshua Alexander Joseph McManus

(Edited and or reviewed by Microsoft Software)

2401049

BA (Hons) – Security, Intelligence and Cyber

The University of Buckingham (2024-2026)

[Author's Notes: https://archive.org/details/2401049-Dec2024-01]

Table of Contents

Introduction.

What is intelligence? While the exact definition of intelligence remains a debated topic, the major consensus between the different positions on the matter defines intelligence as "Information that, once analysed and processed, provides an actionable insight", usually with strategic implications. This information can come from several different origins and sources. The Intelligence Collection Methodologies - usually referred to as the INTs - are the major groupings of different collection disciplines within the intelligence community, of which the big three are Human Intelligence, Signals Intelligence and Open-Source Intelligence. Once combined, INTs form what is sometimes referred to as All-Source Intelligence.

To explain the process that intelligence analysts and officers undertake, the intelligence community often relies on a circular model called the 'Intelligence Cycle' (Figure 1 | Pg 17)[1]. The US Department of Defence's variant on the Intelligence cycle, as seen within the U.S. Army Human Intelligence Collector Field Manual, outlines a 5-step process: "Plan - Prepare - Collect - Process - Produce" (US DoD; 2014)[2]. While this model does allow for the basics of the intelligence collection and dissemination process to be outlined, it is important to note that the Intelligence Cycle is not a rigid step-by-step plan, but rather a flexible model that allows for adaptation. This essay examines these three major INTs, within the context of the collection stage of the 'Intelligence Cycle' and explains the importance of All-Source Intelligence.

[1] The Pennsylvania State University (2014). *Figure 2: The Intelligence Cycle.* [Webpage Image] *The Learner's Guide to Geospatial Analysis, Intelligence Cycle and Process*. Available at: https://www.e-education.psu.edu/sgam/node/15 [Accessed 18 Feb. 2025].

[2] Department of the Army (2014). U.S. Army Human Intelligence Collector Field Manual. First ed. Rowman & Littlefield.

Section 1: Human Intelligence (HUMINT).

Human Intelligence, the ability to extract information from human sources (voluntary or otherwise), is one of the oldest intelligence collection methodologies. The strategic importance of HUMINT has been recognised to date as far back as recorded history. An example of a historical account of the utility of HUMINT would be 孫子 (Sun Tzu)'s art of war, where it mentions the use of spies to find "the names of the attendants, the aides-de-camp, and door-keepers and sentries of the general in command." (孫子; 4th Century BC)[3] This passage teaches the importance of espionage and human intelligence over 25 centuries ago. Furthermore, HUMINT is particularly valuable, not just for short term tactical operations as the Art of War has demonstrated, but also for long-term intelligence operations, as well-placed sources can provide sustained insights over extended periods.

Traditionally, HUMINT relies on agents and informers to the same extent as spy-craft and espionage. Informants are usually recruited on the basis of receiving a reward, the four main categories for which are "Money, Ideology, Coercion and Ego" (Elmer; 2023)[4]. These 4 'methods of persuasion' gives HUMINT the ability to provide context, offering insights into intentions, emotions, and motivations that cannot be derived from intercepted communications or satellite imagery. While HUMINT provides crucial access to denied areas, intelligence failures (such as the reliance on the Iraqi defector 'curveball'[5] in the lead-

[3] Sun Tzu (2004). The Art of War. Translation by Lionel Giles, M.A.

[4] Ellmer, M. (2023). *A Guide to Human Intelligence (HUMINT)*. [online] Grey Dynamics. Available at: https://greydynamics.com/a-guide-to-human-intelligence-humint/ [Accessed 10 Mar. 2025].

[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 9 Mar. 2025].

up to the 2003 Iraq War) highlight the dangers of relying on unverified sources. To mitigate this, agencies increasingly use multi-source validation, ensuring HUMINT is cross-referenced with other intelligence collection methodologies before being treated as actionable intelligence. This layer of security and verification also allows for increased adaptability as while human assets can respond dynamically to emerging threats and shifting priorities, unlike pre-programmed systems, the intelligence provided may be done so dishonestly.

Despite its strategic value, HUMINT carries significant risks, particularly for Covert Human-Intelligence Sources (CHIS[6]) and their handlers. Operating in high-risk environments[7], these individuals face the constant threat of capture, interrogation and execution, especially considering operations within hostile states or conflict zones, where the ability for an agency to protect their assets is lowered. Beyond physical risks, HUMINT also suffers from reliability issues. Sources may provide false, misleading, or biased information due to coercion, personal agendas, or even deliberate deception as double agents.

Many democratic nations have legal frameworks that regulate the powers of law enforcement and intelligence agencies. In the UK, the Regulation of Investigatory Powers Act (RIPA, 2000)[8], and the Investigatory Powers Act (IPA, 2016) [9] provide the legal basis for

[6] The Home Office (n.d.). *Covert Human Intelligence Sources CODE OF PRACTICE*. St Clements House, 2-16 Colegate, Norwich NR3 1BQ: TSO (The Stationery Office).

[7] Moffett, L., Oxburgh, G.E., Dresser, P., Watson, S.J. and Gabbert, F. (2021). Inside the shadows: a survey of UK human source intelligence (HUMINT) practitioners, examining their considerations when handling a covert human intelligence source (CHIS). *Psychiatry, Psychology and Law*, [online] 29(4), pp.487–505. doi:https://doi.org/10.1080/13218719.2021.1926367.

[8] *Regulation of Investigatory Powers Act (2000)*.Chapter 23 [online] Available at: https://www.legislation.gov.uk/ukpga/2000/23/data.pdf [Accessed 9 Mar. 2025].

[9] *Investigatory Powers Act (2016)*.Chapter 25 [online] Available at: https://www.legislation.gov.uk/ukpga/2016/25/data.pdf [Accessed 9 Mar. 2025].

covert surveillance and intelligence gathering, with oversight mechanisms in place. Additionally, the Joint Committee on Human Rights[10] plays a role in reviewing the balance between security and civil liberties. Some argue that "the UK is far in front of any other country in providing open accounts, either through official history, or via the declassification of documents to unofficial historians." (Aldrich; 2021)[11]

However, this may not be the case, Sophie Duroy investigated how the global Intelligence Community tends to 'distort' legal frameworks, especially with regards to the 'coercive elicitation of information'. In her report, Duroy comes to the following conclusion: "The intelligence community uses international law by putting forward interpretations that will legitimise its preferred outcomes and empower it to pursue its choices of policies." (Duroy; 2025)[12] If the Intelligence community can define the norms by which they are held to, what extent do these legalisations protect human rights? This is a question that remains unsolved in modern geopolitics.

HUMINT operations have a complex ethical dimension to consider. While interrogation and torture are seen as 'undemocratic procedures', nations such as the UK and USA do conduct these forms of operations under the scrutiny of law. One of the most notable

[10] Joint Committee on Human Rights - Section 4. (2006). *Joint Committee On Human Rights - Nineteenth Report*. [online] Parliament.uk. Available at: https://publications.parliament.uk/pa/jt200506/jtselect/jtrights/185/18507.htm [Accessed 18 Feb. 2025].

[11] Aldrich, R.J. (2021). From sigint to cyber: a hundred years of Britain's biggest intelligence agency. *Intelligence and National Security*, [online] 36(6), pp.910–917. doi:https://doi.org/10.1080/02684527.2021.1899636.

[12] Duroy, S. (2025). *The Intelligence Community as a Normative Actor under International Law*. [online] *Social Science Research Network*. Edward Elgar Publishing. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4952054 [Accessed 18 Feb. 2025].

and recent examples of this would be the 'extraordinary rendition' of the alleged terrorist and Al-Qaeda Counter-Intelligence officer, ابو زبيدة (Abu Zubaydah).

Zubaydah, was captured by US operatives in Faisalabad (Punjab province, Pakistan) and moved to Guantanamo Bay detention camp as an 'illegal enemy combatant', where he remains still[13]. Declassified Department of Justice documents have revealed that the interrogation techniques used on Zubaydah included "wailing, physical confinement and waterboarding … in some combination to convince Zubaydah that the only way he can influence his surrounding environment is through co-operation." (US DoJ; 2002)[14] The treatment of Abu Zubaydah was, in the eyes of some, directly contravened the 'Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment'[15] of which the United States signed on the 18th of April 1988[16].

The Zubaydah case underscores the ethical, legal and operational risks that HUMINT poses, particularly in the realm of coercive intelligence gathering. While HUMINT remains an indispensable method for obtaining information that may not be possible elsewhere, its vulnerabilities have led the agencies worldwide to see intelligence through a technological lens. The rise of Signals Intelligence (SIGINT) has transformed intelligence collection,

[13] UN OHCHR (2025). Experts call for release o Abu Zubaydah, arbitrarily detained for over two decades. *Press Releases | Special Procedures*. [online] 8 Jan. Available at: https://www.ohchr.org/en/press-releases/2025/01/experts-call-release-guantanamo-bay-detainee-abu-zubaydah-arbitrarily [Accessed 9 Mar. 2025].

[14] Office of the Assistant Attorney General and US Department of Justice | Office of Legal Counsel (2002). *Memorandum for John Rizzo, Acting General Counsel of the Central Intelligence Agency: Interrogation of al Qaeda Operative*. [online] *US Department of Justice | Justice.Gov*, pp.1–18. Available at: https://www.justice.gov/olc/file/886076/dl?inline [Accessed 9 Mar. 2025].

[15] United Nations (1985). Convention against torture and other cruel, inhuman or degrading treatment or punishment. *Medicine and War*, [online] 1(2), pp.161–161. doi:https://doi.org/10.1080/07488008508408634.

[16] The United States Congress (1990). *Resolution of Ratification - Treaty Document 100-20 - CONVENTION AGAINST TORTURE AND OTHER CRUEL, INHUMAN OR DEGRADING TREATMENT OR PUNISHMENT*. [online] www.congress.gov. Available at: https://www.congress.gov/treaty-document/100th-congress/20/resolution-text [Accessed 9 Mar. 2025].

offering a highly effective means of gathering information through global communications infrastructure to intercept and analyse data in real-time, reducing the reliance on human assets and mitigating many of the ethical dilemmas inherent in espionage.

Section 2: Signals Intelligence (SIGINT).

Signals Intelligence has played a central role in the intelligence field, particularly since the early 20th century, as demonstrated throughout both world wars. A key example of SIGINTs impact can be seen through the interception of the Zimmerman Telegraph, in which Arthur Zimmermann, the German foreign minister planned to offer "United States territory to Mexico in return for joining the German cause." (US National Archives; 2016)[17] The decryption of which, as argued by Peter Matthews of the Foreign Press Association[18], was the "biggest coup that Room 40 had achieved" (Matthews; 2013)[19] marking one of the earliest strategic uses of contemporary SIGINT. Today, with the rise of cyber warfare and mass data interception, SIGINT has become a central pillar of national security. Furthermore, from the breakout of the cold war – to contemporary times, developments within the Technosphere led to SIGINT becoming a key component of national security, providing nations with high levels of cyber knowhow with increased technical warfare capabilities.

One of the primary advantages of SIGINT is the crucial role it provides within the cyber domain. Cyber threats, from ransomware to DDoS attacks, have become a major issue and a focus within the intelligence community, as of recent years – as seen through the

[17] National Archives (2016). The Zimmermann Telegram. [online] National Archives. Available at: https://www.archives.gov/education/lessons/zimmermann#background [Accessed 6 Mar. 2025].

[18] World of Books (n.d.). *About Peter Matthews*. [online] World of Books . Available at: https://www.worldofbooks.com/en-gb/products/sigint-book-peter-matthews-9780750987714 [Accessed 6 Mar. 2025].

[19] Matthews, P. (2013). *SIGINT: The Secret History of Signals Intelligence in the World Wars.* The History Press The Mill, Brimscombe Port Stroud, Gloucestershire, GL5 2QG: The History Press.

publicity of Stuxnet. Stuxnet, attributed by many to the US[20] and Israeli[21] governments (while some speculate further collaboration between commonwealth actors through the Equation Group[22]) was a cyber-attack on the Iranian Natanz uranium enrichment facility, focused on damaging the physical elements of the facility, such as the centrifuges. Although the exact method of Stuxnet's entry remains unknown, it is safe to say the worm induced mechanical stress and degradation while simultaneously feeding false data to monitoring systems to avoid detection[23].

This prolonged damage led to the failure of numerous centrifuges, significantly hindering Iran's nuclear ambitions. Stuxnet represents a paradigm shift in SIGINT, demonstrating how intelligence-gathering capabilities can transition into cyber-offensive operations. By targeting Iran's nuclear program, it illustrated how cyberwarfare can be used as a non-traditional alternative to military strikes, setting a precedent for future intelligence-driven cyber conflicts

One of the other advantages of SIGINT is its role in providing early warnings, allowing for pre-emptive strikes. By intercepting and analysing enemy communications or radar signals, intelligence agencies can detect threats before they materialise. This proactive

[20] Sanger, D.E. (2012). Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times*. [online] 1 Jun. Available at: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=2&_r=1&seid=auto&smid=tw-nytimespolitics&pagewanted=all [Accessed 6 Mar. 2025].

[21] Anderson, N. (2012). *Confirmed: US and Israel created Stuxnet, lost control of it*. [online] Ars Technica. Available at: https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/ [Accessed 6 Mar. 2025].

[22] Council on Foreign Relations (n.d.). *Connect the Dots on State-Sponsored Cyber Incidents - Equation Group*. [online] Council on Foreign Relations. Available at: https://www.cfr.org/cyber-operations/equation-group [Accessed 6 Mar. 2025].

[23] Fildes, J. (2011). Stuxnet virus targets and spread revealed. *BBC News*. [online] 15 Feb. Available at: https://www.bbc.co.uk/news/technology-12465688 [Accessed 10 Mar. 2025].

approach can be instrumental in preventing terrorist attacks, military invasions, or cyber intrusions, giving nations a strategic advantage in warfare and security operations. Unlike traditional Human Intelligence based methodologies, which often require time-consuming human analysis and verification, SIGINT (alongside OSINT) can deliver semi-immediate data on an adversary's movements and intentions. This almost real-time aspect enhances situational awareness for military and intelligence agencies, allowing them to respond swiftly to emerging threats.

Despite these advantages, SIGINT is not without its drawbacks. One of the most significant challenges is the high cost associated with developing and maintaining SIGINT capabilities. Establishing satellite networks, maintaining surveillance aircraft, and funding cyber intelligence programs require substantial financial investment. Additionally, the constant evolution of encryption and communication technologies necessitates continuous updates and research, further driving up costs. The USA's intelligence budget peaked at $73.4 billion in 2025[24], while the UK's single Intelligence Account was £3 billion (2021/22)[25] the "lion's share" (Norton-Taylor; 2021)[26] of which fuels GCHQ. Maintaining cutting-edge SIGINT capabilities demands continuous investment in satellite networks, cybersecurity programs, and AI-driven interception tools.

[24] Federation of American Scientists (2025). *U.S. Intelligence Budget Data*. [online] irp.fas.org. Available at: https://irp.fas.org/budget/ [Accessed 13 Mar. 2025].

[25] Lewis, J. (2022). *Intelligence and Security Committee of Parliament Chairman*. [online] Available at: https://isc.independent.gov.uk/wp-content/uploads/2023/12/ISC-Annual-Report-2022-2023.pdf [Accessed 13 Mar. 2025].

[26] NORTON-TAYLOR, R. (2021). *Whitewashing Britain's largest intelligence agency*. [online] Declassified Media Ltd. Available at: https://www.declassifieduk.org/whitewashing-britains-largest-intelligence-agency/ [Accessed 13 Mar. 2025].

A major limitation of SIGINT is the sheer volume of intercepted communications, often referred to as the 'hosepipe issue.' To address this data saturation, agencies employ AI-driven analysis tools such as XKeyscore, which automates data filtering to identify patterns of interest. XKeyscore has proven to be a controversial and yet incomprehensibly useful tool for the protection of national interests of the United States, The NSA – in a press statement in 2013 – has confirmed how powerful XKeyscore has been to the US, "as of 2008, there were over 300 terrorists captured using intelligence generated from XKEYSCORE." (NSA; 2013)[27] This indicates that while XKeyscore has numerous ethical, officially the benefit to the national security of the US outweighs the cost of personal privacy. However, as the Snowden revelations exposed, this raises concerns over mass surveillance and privacy rights, demonstrating that SIGINT's effectiveness comes at a potential ethical cost.

In an era by which the cyber-realm has become the battlefield, SIGINT's role in hybrid warfare is now indispensable, in fact, John Ferris, in his authorised history of GCHQ, stated that GCHQ's success within the digital era "had reached the highest levels in history, providing much first-rate material on first rate issues." (Ferris; 2020)[28], showcasing the importance of SIGINT within the modern era. As technology continues to evolve, the Intelligence Community must adapt to balance the Advantages and Disadvantages to ensure SIGINT remains effective at the forefront of operations.

[27] National Security Agency (2013). *Press Statement on 30 July 2013*. [online] National Security Agency/Central Security Service. Available at: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/1620989/press-statement-on-30-july-2013/ [Accessed 9 Mar. 2025].

[28] Ferris, J. (2020). Behind the Enigma. Bloomsbury Publishing Ltd.

Section 3: Open-Source Intelligence (OSINT).

Open-source Intelligence, the famous (and yet misunderstood) middle child of the intelligence world, has its roots deeper than one may think. OSINT refers to the collection and analysis of publicly available information from sources such as news reports, social media, academic papers, government records, and public satellite imagery. Often misunderstood as a modern invention, OSINT has deep historical roots. During World War II, intelligence agencies leveraged open sources such as enemy radio broadcasts, propaganda, and press reports to gain insights into adversary strategies.[29] Today, OSINT has evolved into a critical intelligence discipline, fuelled by the digital revolution and the rise of social media, with journalists, analysts, private companies, and intelligence agencies all leveraging its capabilities. Unlike OSINTs more clandestine brothers within the field, OSINT is accessible, cost-effective, and legally available, making it an attractive option for both state and non-state actors.

It plays a crucial role in areas like cybersecurity, geopolitical analysis, and crisis monitoring. However, while OSINT offers valuable insights, it also comes with challenges, including misinformation, data overload, and the difficulty of verifying sources. The reliance on publicly available data means that adversaries can manipulate information or restrict access. Furthermore, it is important to note how uncomprehensible the volume of the data that resides on the internet – everything mentioned earlier with regards to the 'hosepipe issue' is exponentially increase. Unlike intercepted signals, open-source information can be manipulated by adversaries, making verification crucial. The rapid spread of fake news and

[29] Wheatley, B. (2017). British open source intelligence (OSINT) and the Holocaust in the Soviet Union: persecution, extermination and partisan warfare. *Intelligence and National Security*, [online] 33(3), pp.422–438. doi:https://doi.org/10.1080/02684527.2017.1410516.

deepfakes further complicates intelligence analysis, requiring advanced verification techniques such as geolocation analysis, metadata tracing, and AI-driven content authentication.

Despite these limitations, OSINT remains a powerful tool, especially when seen through the eyes of modern asymmetrical warfare. This can be furthered by Netanel Flamer, a specialist in Middle-Eastern studies and Hybrid warfare, "OSINT, like all other disciplines, must adjust itself to the reality of asymmetric warfare in order to fulfil its mission effectively in a new era." (Flamer; 2023)[30] Unlike traditional intelligence, which focuses on state actors, OSINT allows for tracking of decentralized threats such as terrorist networks, insurgent groups, and cybercriminals. The rise of non-state actors exploiting social media for propaganda and recruitment further highlights this.[31]

With the rise in the interconnectedness of the world, OSINT (specifically the Sub-Speciality Social-Media Intelligence / SOCMINT) provides a strong foundation for future information elicitation. One report by the University of Brasília stated that "In addition to providing horizon scanning and strategic alerting capabilities, SOCMINT can make decisive contributions to prevent cybercrime by identifying potential collaborators or perpetrators of cyberthreats." (Macêdo et al; 2023)[32] which allows us to see the potential applications of OSINT that may not instantly come to mind.

[30] Flamer, N. (2023). 'The enemy teaches us how to operate': Palestinian Hamas use of open source intelligence (OSINT) in its intelligence warfare against Israel (1987-2012). *Intelligence and National Security*, [online] 38(7), pp.1–18. doi:https://doi.org/10.1080/02684527.2023.2212556.

[31] Federal Bureau of Investigation (2024). *Terrorism*. [online] Federal Bureau of Investigation. Available at: https://www.fbi.gov/investigate/terrorism [Accessed 13 Mar. 2025].

[32] Macêdo, A., Peotta, L. and Gomes, F. (2023). A Review of the Intersection Techniques on Humint and Osint. *International Journal on Cybernetics & Informatics*, [online] 12(1), pp.1–11. doi:https://doi.org/10.5121/ijci.2023.120105.

However, concerns regarding privacy and the internet are considerable. According to Rønn and Søe, of the Taylor and Francis journal 'Intelligence and National Security', "The Danish Consumer Council called for greater awareness of the non-private nature of social media information and compared information on social media pro les to newspaper articles." (Rønn & Søe; 2019)[33] showcasing how, even with the rise in OSINT within the public lexis, the average person may be ignorant to how consumer data is utilised by companies and individuals.

OSINT's greatest challenge is misinformation, as adversaries can manipulate publicly available data. To counter this, intelligence agencies employ verification techniques such as geolocation analysis, metadata tracing, and AI-driven content authentication. The Centre for Information Resilience, an OSINT investigation and research organisation based in London[34], focuses on Human Rights issues around the world with one of their key projects being a crowdsourced map[35] (Alongside other OSINT groups, such as Bellingcat), documenting and verifying "significant incidents during the conflict in Ukraine" (CIR; 2025)[36]. This highlights how, despite its limitations, OSINT remains a powerful intelligence tool when properly validated.

[33] Rønn, K.V. and Søe, S.O. (2019). Is social media intelligence private? Privacy in public and the nature of social media intelligence. *Intelligence and National Security*, [online] 34(3), pp.362–378. doi:https://doi.org/10.1080/02684527.2019.1553701.

[34] Centre for Information Resilience (2025). *FAQs - Centre for Information Resilience*. [online] Centre for Information Resilience. Available at: https://www.info-res.org/faqs/ [Accessed 9 Mar. 2025].

[35] Centre for Information Resilience (2022). *Eyes on Russia Map*. [online] eyesonrussia.org. Available at: https://eyesonrussia.org [Accessed 9 Mar. 2025].

[36] Strick, B. (2022). *Follow the Russia-Ukraine Monitor Map - bellingcat*. [online] bellingcat. Available at: https://www.bellingcat.com/news/2022/02/27/follow-the-russia-ukraine-monitor-map/ [Accessed 9 Mar. 2025].

Conclusion: The Importance of 'All-Source Intelligence'.

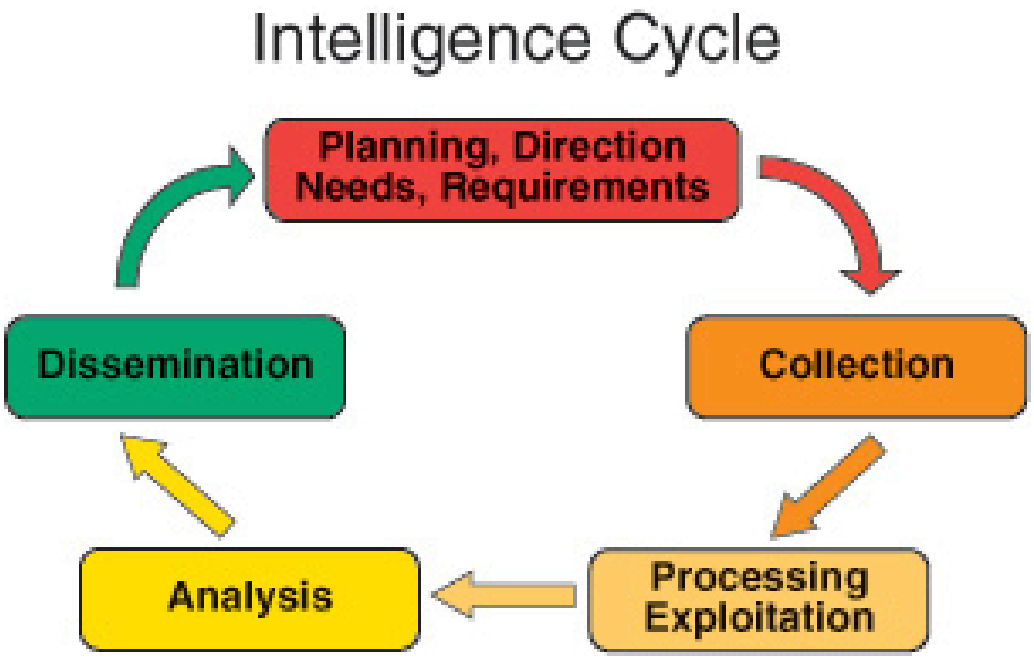
The world is, as it always has been, is in a dangerous state of flux. Similarly to global geopolitics, the field of Intelligence is equally complex and forever evolving, with each of the INTs constantly adapting and changing to match. As demonstrated, HUMINT suffers from reliability concerns, SIGINT faces data overload, and OSINT struggles with both of these issues simultaneously. However, as discussed, intelligence agencies mitigate these weaknesses through an All-Source Intelligence approach. By cross-referencing INTs, analysts can validate sources, prioritise critical threats, and ensure a more accurate intelligence picture. This underscores the necessity of All-Source Intelligence in modern operations, as no single collection method is sufficient in isolation.

To better demonstrate this point, a quote from the fictional Gen. 艾洛 (Ai Lùo) comes to mind. "It is important to draw wisdom from many different places. If we take it from only one place, it becomes rigid and stale." (艾洛, ATLA; 2006)[37] While this creative analogy has been taken from a considerably non-academic source, I believe the principle strongly applies directly to the field of intelligence, where relying solely on one source - whether HUMINT, SIGINT, or OSINT - can lead to blind spots and flawed conclusions. Instead, an All-Source Intelligence approach, ensures a more balanced, accurate, and actionable intelligence picture.

[37] Spaulding, E. DiMartino, M.D. & Konietzko, B. (2006) Avatar: The Last Airbender, Book 2, Episode 9. [TV Series Episode] Nickelodeon, 2 June.

Annex Page.

Annex A | Figure 1:



^

This figure has been taken from The Pennsylvania State University's "*The Learner's Guide to Geospatial Analysis, Intelligence Cycle and Process*.". Footnote № 1, Page № 3.

Reference List.

1. Aid, M.M. (2003). All Glory is Fleeting: Sigint and the Fight Against International Terrorism. *Intelligence and National Security*, [online] 18(4), pp.72–120. doi:https://doi.org/10.1080/02684520310001688880.

2. Aldrich, R.J. (2021). From sigint to cyber: a hundred years of Britain's biggest intelligence agency. *Intelligence and National Security*, [online] 36(6), pp.910–917. doi:https://doi.org/10.1080/02684527.2021.1899636.

3. Anderson, J. (2007). The HUMINT Offensive from Putin's Chekist State. *International Journal of Intelligence and CounterIntelligence*, [online] 20(2), pp.258–316. doi:https://doi.org/10.1080/08850600601079958.

4. Anderson, N. (2012). *Confirmed: US and Israel created Stuxnet, lost control of it*. [online] Ars Technica. Available at: https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/ [Accessed 6 Mar. 2025].

5. Aubrey, C. (1981). *Who's Watching You? Britain's Security Services and the Official Secrets Act.* Penguin Books Ltd, Harmondsworth, Middlesex, England: Penguin Books.

6. Bergien, R., Gerstenberger, D. and Goschler, C. (2022). *Intelligence Agencies, Technology and Knowledge Production*. Routledge.

7. Berkowitz, B. (2002). Book Review: Information warfare. *Issues in Science and Technology*, [online] 18(2). Available at: https://issues.org/br_berkowitz/ [Accessed 18 Feb. 2025].

8. Berkowitz, B. (2008). The R&D Future of Intelligence | Issues in Science and Technology. *Issues in Science and Technology*, [online] 24(3). Available at: https://issues.org/berkowitz-3/ [Accessed 18 Feb. 2025].
9. Boyd, A. (2020). *British Naval Intelligence through the Twentieth Century*. Seaforth Publishing.
10. Centre for Information Resilience (2022). *Eyes on Russia Map*. [online] eyesonrussia.org. Available at: https://eyesonrussia.org [Accessed 9 Mar. 2025].
11. Centre for Information Resilience (2025). *FAQs - Centre for Information Resilience*. [online] Centre for Information Resilience. Available at: https://www.info-res.org/faqs/ [Accessed 9 Mar. 2025].
12. 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 9 Mar. 2025].
13. Council on Foreign Relations (n.d.). *Connect the Dots on State-Sponsored Cyber Incidents - Equation Group*. [online] Council on Foreign Relations. Available at: https://www.cfr.org/cyber-operations/equation-group [Accessed 6 Mar. 2025].
14. Department of the Army (2014). *U.S. Army Human Intelligence Collector Field Manual*. First ed. Rowman & Littlefield.
15. Duroy, S. (2025). *The Intelligence Community as a Normative Actor under International Law*. [online] *Social Science Research Network*. Edward Elgar Publishing. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4952054 [Accessed 18 Feb. 2025].

16. Eldridge, C., Hobbs, C. and Moran, M. (2017). Fusing algorithms and analysts: open-source intelligence in the age of ‘Big Data’. *Intelligence and National Security*, [online] 33(3), pp.391–406. doi:https://doi.org/10.1080/02684527.2017.1406677.
17. Ellmer, M. (2023). *A Guide to Human Intelligence (HUMINT)*. [online] Grey Dynamics. Available at: https://greydynamics.com/a-guide-to-human-intelligence-humint/ [Accessed 10 Mar. 2025].
18. Federal Bureau of Investigation (2024). *Terrorism*. [online] Federal Bureau of Investigation. Available at: https://www.fbi.gov/investigate/terrorism [Accessed 13 Mar. 2025].
19. Federation of American Scientists (2025). *U.S. Intelligence Budget Data*. [online] irp.fas.org. Available at: https://irp.fas.org/budget/ [Accessed 13 Mar. 2025].
20. Ferris, J. (2020). *Behind the Enigma.* Bloomsbury Publishing Ltd.
21. Fildes, J. (2011). Stuxnet virus targets and spread revealed. *BBC News*. [online] 15 Feb. Available at: https://www.bbc.co.uk/news/technology-12465688 [Accessed 10 Mar. 2025].
22. Flamer, N. (2023). ‘The enemy teaches us how to operate’: Palestinian Hamas use of open source intelligence (OSINT) in its intelligence warfare against Israel (1987-2012). *Intelligence and National Security*, [online] 38(7), pp.1–18. doi:https://doi.org/10.1080/02684527.2023.2212556.
23. Hecking, M. (2006). *2006 CCRTS THE STATE OF THE ART AND THE STATE OF THE PRACTICE Content Analysis of HUMINT Reports Content Analysis of HUMINT Reports*. [online] Available at: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ae6c5eb183b02cb69c502d1174272b3c545b7591 [Accessed 17 Feb. 2025].

24. *Investigatory Powers Act (2016)*.Chapter 25 [online] Available at: https://www.legislation.gov.uk/ukpga/2016/25/data.pdf [Accessed 9 Mar. 2025].
25. Joint Committee on Human Rights - Section 4. (2006). *Joint Committee On Human Rights - Nineteenth Report*. [online] Parliament.uk. Available at: https://publications.parliament.uk/pa/jt200506/jtselect/jtrights/185/18507.htm [Accessed 18 Feb. 2025].
26. Juurvee, I. (2017). Birth of Russian SIGINT during World War I on the Baltic Sea. *Intelligence and National Security*, [online] 32(3), pp.300–312. doi:https://doi.org/10.1080/02684527.2016.1270991.
27. Lewis, J. (2022). *Intelligence and Security Committee of Parliament Chairman*. [online] Available at: https://isc.independent.gov.uk/wp-content/uploads/2023/12/ISC-Annual-Report-2022-2023.pdf [Accessed 13 Mar. 2025].
28. Lowenthal, M.M. and Clark, R.M. (2016). *The five disciplines of intelligence collection*. Thousand Oaks, California: Cq Press, An Imprint Of Sage Publications, Inc.
29. Macêdo, A., Peotta, L. and Gomes, F. (2023). A Review of the Intersection Techniques on Humint and Osint. *International Journal on Cybernetics & Informatics*, [online] 12(1), pp.1–11. doi:https://doi.org/10.5121/ijci.2023.120105.
30. Margolis, G. (2013). The Lack of HUMINT: A Recurring Intelligence Problem. *Global Security Studies*, 4(2), p.43.
31. Matthews, P. (2013). *SIGINT: The Secret History of Signals Intelligence in the World Wars.* The History Press The Mill, Brimscombe Port Stroud, Gloucestershire, GL5 2QG: The History Press.

32. Moffett, L., Oxburgh, G.E., Dresser, P., Watson, S.J. and Gabbert, F. (2021). Inside the shadows: a survey of UK human source intelligence (HUMINT) practitioners, examining their considerations when handling a covert human intelligence source (CHIS). *Psychiatry, Psychology and Law*, [online] 29(4), pp.487–505. doi:https://doi.org/10.1080/13218719.2021.1926367.
33. National Archives (2016). *The Zimmermann Telegram*. [online] National Archives. Available at: https://www.archives.gov/education/lessons/zimmermann#background [Accessed 6 Mar. 2025].
34. National Security Agency (2013). *Press Statement on 30 July 2013*. [online] National Security Agency/Central Security Service. Available at: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/1620989/press-statement-on-30-july-2013/ [Accessed 9 Mar. 2025].
35. NORTON-TAYLOR, R. (2021). *Whitewashing Britain's largest intelligence agency*. [online] Declassified Media Ltd. Available at: https://www.declassifieduk.org/whitewashing-britains-largest-intelligence-agency/ [Accessed 13 Mar. 2025].
36. Office of the Assistant Attorney General and US Deparment of Justice | Office of Legal Counsel (2002). *Memorandum for John Rizzo, Acting General Counsel of the Central Intelligence Agency: Interrogation of al Qaeda Operative*. [online] *US Department of Justice | Justice.Gov*, pp.1–18. Available at: https://www.justice.gov/olc/file/886076/dl?inline [Accessed 9 Mar. 2025].
37. Office of the United Nations High Commissioner for Human Rights (2025). Experts call for release of Guantánamo Bay detainee Abu Zubaydah, arbitrarily detained for over two decades. *Press Releases | Special Procedures*. [online] 8

Jan. Available at: https://www.ohchr.org/en/press-releases/2025/01/experts-call-release-guantanamo-bay-detainee-abu-zubaydah-arbitrarily [Accessed 9 Mar. 2025].

38. Rattray, G.J. (2001). *Strategic warfare in cyberspace*. Cambridge (Mass.) ; London: Mit Press.
39. Rayment, S. (2024). *The military's most secretive unit on recruitment drive for undercover operations*. [online] The Telegraph. Available at: https://www.telegraph.co.uk/news/2024/05/18/secretive-army-unit-on-recruitment-drive/?ICID=continue_without_subscribing_reg_first [Accessed 18 Feb. 2025].
40. *Regulation of Investigatory Powers Act (2000)*.Chapter 23 [online] Available at: https://www.legislation.gov.uk/ukpga/2000/23/data.pdf [Accessed 9 Mar. 2025].
41. Rønn, K.V. and Søe, S.O. (2019). Is social media intelligence private? Privacy in public and the nature of social media intelligence. *Intelligence and National Security*, [online] 34(3), pp.362–378. doi:https://doi.org/10.1080/02684527.2019.1553701.
42. Sanger, D.E. (2012). Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times*. [online] 1 Jun. Available at: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=2&_r=1&seid=auto&smid=tw-nytimespolitics&pagewanted=all [Accessed 6 Mar. 2025].
43. Sano, J. (2015). Guide to the Study of Intelligence: The Changing Shape of HUMINT. *Intelligencer: Journal of U.S. Intelligence Studies* , [online] 21(3). Available at: https://www.afio.com/publications/SANO%20John%20on%20The%20Changing

%20Shape%20of%20HUMINT%20Pages%20from%20INTEL_FALLWINTER2015_Vol21_No3_FINAL.pdf [Accessed 17 Feb. 2025].

44. Sebastiaan Rietjens, Sinterniklaas, R. and Coulthart, S. (2024). How intelligence organisations innovate. *Intelligence & National Security*, [online] 40(1), pp.1–20. doi:https://doi.org/10.1080/02684527.2024.2401638.
45. Silverstein, K. (2015). *US Reliance on Too Much SIGINT and Too Little Spycraft Is Dangerous and Expensive*. [online] Observer. Available at: https://observer.com/2015/09/us-reliance-on-too-much-sigint-and-too-little-spycraft-is-dangerous-and-expensive/ [Accessed 18 Feb. 2025].
46. Spaulding, E. DiMartino, M.D. & Konietzko, B. (2006) *Avatar: The Last Airbender*, Book 2, Episode 9. [TV Series Episode] Nickelodeon, 2 June.
47. Stottlemyre, S.A. (2015). HUMINT, OSINT, or Something New? Defining Crowdsourced Intelligence. *International Journal of Intelligence and CounterIntelligence*, [online] 28(3), pp.578–589. doi:https://doi.org/10.1080/08850607.2015.992760.
48. Strick, B. (2022). *Follow the Russia-Ukraine Monitor Map - bellingcat*. [online] bellingcat. Available at: https://www.bellingcat.com/news/2022/02/27/follow-the-russia-ukraine-monitor-map/ [Accessed 9 Mar. 2025].
49. Sun Tzu (2004). *The Art of War*. Translation by Lionel Giles, M.A.
50. The Home Office (n.d.). *Covert Human Intelligence Sources CODE OF PRACTICE*. St Clements House, 2-16 Colegate, Norwich NR3 1BQ: TSO (The Stationery Office).
51. The Pennsylvania State University (2014). *Figure 2: The Intelligence Cycle.* [Webpage Image] *The Learner's Guide to Geospatial Analysis,*

Intelligence Cycle and Process. Available at: https://www.e-education.psu.edu/sgam/node/15 [Accessed 18 Feb. 2025].

52. The United States Congress (1990). *Resolution of Ratification - Treaty Document 100-20 - CONVENTION AGAINST TORTURE AND OTHER CRUEL, INHUMAN OR DEGRADING TREATMENT OR PUNISHMENT*. [online] www.congress.gov. Available at: https://www.congress.gov/treaty-document/100th-congress/20/resolution-text [Accessed 9 Mar. 2025].
53. Thompson, R. (2011). *CRS Report for Congress Governmental Tracking of Cell Phones and Vehicles: The Confluence of Privacy, Technology, and Law*. [online] *www.CRS.Gov*. US Congressional Research Service. Available at: https://sgp.fas.org/crs/intel/R42109.pdf [Accessed 18 Feb. 2025].
54. UK Ministry of Defence (2020). *ROYAL MARINES CAREER HANDBOOK*. [online] *Charlton School*, His Majesty's Naval Service | the Corps of Royal Marines, pp.44–45. Available at: https://www.charlton.uk.com/media/24343/20_0507_rm-career-guide_2020_v1.pdf [Accessed 18 Feb. 2025].
55. United Nations (1985). Convention against torture and other cruel, inhuman or degrading treatment or punishment. *Medicine and War*, [online] 1(2), pp.161–161. doi:https://doi.org/10.1080/07488008508408634.
56. Warner, M. (2012). Reflections on Technology and Intelligence Systems. *Intelligence and National Security*, [online] 27(1), pp.133–153. doi:https://doi.org/10.1080/02684527.2012.621604.
57. Weinbaum, C., Berner, S. and Mcclintock, B. (2015). *Perspective SIGINT for Anyone The Growing Availability of Signals Intelligence in the Public Domain*.

[online] *RAND*. Californa: RAND Corporation. Available at: https://www.rand.org/pubs/perspectives/PE273.html [Accessed 18 Feb. 2025].

58. Wheatley, B. (2017). British open source intelligence (OSINT) and the Holocaust in the Soviet Union: persecution, extermination and partisan warfare. *Intelligence and National Security*, [online] 33(3), pp.422–438. doi:https://doi.org/10.1080/02684527.2017.1410516.
59. Wilson, O. (2020). *Intelligence Gathering: Front Line HUMINT Considerations*.
60. World of Books (n.d.). *About Peter Matthews*. [online] World of Books . Available at: https://www.worldofbooks.com/en-gb/products/sigint-book-peter-matthews-9780750987714 [Accessed 6 Mar. 2025].