CENTRE FOR SECURITY STUDIES | ISSUE BRIEF

JANUARY 2024

BALANCING THE SCALES: NAVIGATING THE INTERPLAY BETWEEN TECHNOLOGY AND HUMINT

Divyashree Jha

Edited by: Guneet Sahni

About the Author

Divyashree Jha is an undergraduate student at the Jindal School of International Affairs (JSIA) and is an Editor at the Centre for Security Studies, JSIA.

About the Centre for Security Studies

The Centre for Security Studies (CSS) was established in 2020 as the Jindal School of International Affairs' first student-run research centre under the aegis of Prof. Dr. Pankaj K. Jha. Researchers at CSS explore both regional and thematic topics in the broader field of international security studies to write issue briefs, policy briefs, defence white papers, and dialogue session reports on contemporary issues. The concept of international security has been expanded to reflect not merely the study of state security, but also include topics like ethnic, sectarian, and religious conflict; civil wars and state failure; cyber and space warfare; resource-related security issues; the proliferation of weapons of mass destruction; defence economics and the role of ethics or morality in the formulation of security policies. The complexity of these matters is what the Centre for Security Studies attempts to unfold. Please refer to www.cssjsia.com for further details, and follow the Centre's social media platforms for critical news and research updates:


www.linkedin.com/company/jindal-centre-for-security-studies/


www.instagram.com/css_jsia/


https://twitter.com/Css_Jsia

Get in touch with us through email: css@jgu.edu.in

Important disclaimer

All views expressed in this publication belong to the author and do not reflect the opinions or positions of the Centre for Security Studies. While researchers and editors at CSS strive towards innovation, CSS as an organisation does not take any responsibility for any instance of plagiarism committed by the authors. The onus to ensure plagiarism-free work lies with the authors themselves.

IB2401004

Introduction

Human Intelligence (HUMINT) has long been a cornerstone of intelligence gathering, relying on the intricate understanding of human behaviour and interactions to source data. However, with the rapid advancement of technology over the last few decades and the evolution of cyberspace and AI, concepts like cybernetic HUMINT are on the rise. This evolution represents the fusion of traditional human intelligence methodologies with cutting-edge technological capabilities. It also adds a new chapter to the years-long HUMINT versus TECHINT debate, creating new challenges and implications for the policy sphere amidst the growing need for multi-dimensional intelligence strategies.

This paper delves into the transformative impact that rapid technological development has had on the landscape of HUMINT, exploring how their synergy has not only enhanced information gathering but also presented new challenges. Additionally, it scrutinizes the position of cybernetic HUMINT and the use of AI within the broader discourse encompassing traditional HUMINT and TECHINT.

Historical Context

Human Intelligence, as officially defined by NATO, encompasses the collection of information through human sources, employing a wide range of interpersonal skills to acquire insights, assessments, and knowledge vital for decision-making[1]. Traditionally rooted in human interactions, HUMINT has been a linchpin in intelligence efforts, providing a nuanced understanding of various geopolitical landscapes. Human Intelligence operations manifest in various forms, encompassing both overt and covert missions. Overt activities, such as interrogations or interviews, are conducted openly, while covert operations, such as espionage for surveillance, involve discreet and secretive measures.

[1] *NATO Review - A new era for NATO intelligence*. (2019, October 29). NATO Review. https://www.nato.int/docu/review/articles/2019/10/29/a-new-era-for-nato-intelligence/index.html

The roots of HUMINT trace back to ancient civilizations, where emissaries and spies played pivotal roles in gathering information for military and political purposes. Evidence of the use of cryptography, i.e. codes and ciphers to protect information can be found on clay tablets dating as early as 1500BC from Mesopotamia.[2] By 500 BC, coded messages and communications have been observed in Greece and Rome, along with the use of human agents as spies and informants.[3] The medieval times saw the sophistication of cyphers and rampant employment of emissaries and undercover envoys for intelligence gathering in the politically strained feudal systems of Europe.[4] Notably, Chanakya's magnum opus, the "Arthashastra," delves into the intricacies of espionage, elucidating its crucial role in building and dismantling empires. The treatise not only underscores the significance of missions to other kingdoms but also provides insights into the clandestine operations within royal courts and among the local populace.[5] Additionally, Chanakya's work elucidates tactics for effective counter-espionage, emphasizing the perpetual cat-and-mouse game inherent in the world of intelligence.[6]

The role of HUMINT can also be observed in the process of colonisation of regions in Asia, Africa and America by European powers, with massive deployments for mapping territories, gathering intelligence on local populations and monitoring rival colonial powers.[7] It was during the world wars, however, that technological advancements like telegraph and radio systems began being

[2] Kahn, D. (1996). *The Codebreakers*. Simon and Schuster.

[3] *History of Encryption | SANS Institute*. (n.d.). Www.sans.org. https://www.sans.org/white-papers/730/

[4] Beechy, T. (2023). *Aesthetics and the Incarnation in Early Medieval Britain*. University of Notre Dame Press.

[5] Kautilya, & Rangarajan, L. N. (1992). *The Arthashastra*. Penguin Books India.

[6] Ibid

[7] Assayag, J. (1998). [Review of *Empire and Information. Intelligence Gathering and Social Communication in India, 1780-1870*, by C. A. Bayly]. *L'Homme*, *146*, 289–293. http://www.jstor.org/stable/25133332

utilised in intelligence operations. HUMINT also gained prominence with the use of spies and covert agents in trench warfare. Espionage networks became crucial for both the Allied and Central Powers.[8] By the Second World War, Special Operations Executive (SOE) and other intelligence agencies were heavily relying on HUMINT for gathering information behind enemy lines.[9] The Double Cross System is a notable success in British counterintelligence.[10] Advancements in cryptography, radar technology, and the use of the Enigma machine by Axis powers significantly impacted intelligence operations.[11] The Cold War era furthered the rise of satellite technology for surveillance, the use of spy planes such as the American U-2, and the development of intelligence agencies like the CIA and the KGB. The Cuban Missile Crisis in 1962 was a notable event where intelligence played a critical role. This era also saw the advent of computers and the internet, with the use of early computing systems for codebreaking and signal intelligence (SIGINT). The end of the Cold War prompted a shift in focus to non-state actors and asymmetric threats. The advent of the internet and digital communication also introduced new challenges and opportunities for intelligence gathering and began increasing the weightage of TECHINT alongside HUMINT in operations.

The 9/11 attacks prompted a renewed focus on HUMINT by Western intelligence agencies to understand and counter-terrorist networks. Intelligence agencies prioritized the recruitment of human assets in regions of heightened strategic interest. However, reliance on signals intelligence (SIGINT), geospatial intelligence (GEOINT), and the development of data mining and analysis tools also became prevalent. A good example of this multifaceted intelligence operation was the pursuit to locate Osama Bin Laden, and the satellite imageries as well as on-ground agents involved

[8] Newton-Matza, M. (2017). *The Espionage and Sedition Acts : World War I and the image of civil liberties*. Routledge.

[9] Duckett, R. (2017). *The Special Operations Executive (SOE) in Burma*. Bloomsbury Publishing.

[10] Masterman, J. C. (2011). *Double-Cross System*. Rowman & Littlefield.

[11] Alvarez, D. (2013). *Allied and Axis Signals Intelligence in World War II*. Routledge.

in making the mission a success.[12] The Global War on Terror also emphasized the need for intelligence collaboration and information sharing among nations.

As intelligence practices evolved, the integration of cyber technology into traditional HUMINT became imperative. The 21st century witnessed a paradigm shift, where intelligence agencies harnessed the power of cyber capabilities to complement and enhance human-driven operations.[13] AI, which was an emerging tech until very recently, has already begun to create a stronghold in all industries, including the intelligence community. This historical journey sets the stage for understanding the dynamic interplay between age-old human intelligence practices and the transformative impact of technology.

The Confluence of 21st Century Cyberspace, Artificial Intelligence, and HUMINT

The integration of cyberspace, Artificial Intelligence (AI), and HUMINT has ushered in a new era of intelligence gathering, blending the speed and efficiency of technology with the capabilities of human agents. The utilization of cyberspace as a domain for intelligence operations has become increasingly prevalent, where governments, non-state actors, and even individuals leverage the expansive and interconnected nature of the internet for information gathering and dissemination. In this context, AI emerges as a force multiplier, enhancing the analytical capabilities of intelligence agencies and augmenting the abilities of human agents.[14]

However, being components of the larger TECHINT, the increasing use of cyber and AI tools creates a question on the relevance of HUMINT components in an intelligence operation. One example is Micro Expressions. The field of psycho-linguistics and the study of microexpressions have emerged as critical components in the training of intelligence operatives for assessing

[12] Bergen, P. L. (2012). *Manhunt*. Crown.

[13] Fruhlinger, J. (2022, August 31). *Stuxnet explained: The first known cyberweapon*. CSO Online. https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

[14] Wallace, R. J. (2021). *Artificial Intelligence/ Human Intelligence: An Indissoluble Nexus*. World Scientific.

subjects. These subtle cues, often imperceptible to the untrained eye, provide valuable insights into an individual's emotions, intentions, and truthfulness. Traditionally, these micro-assessments have been considered unique capabilities of human agents, differentiating them from the capabilities of Technical Intelligence (TECHINT).

However, recent advancements in AI detection technology are challenging this distinction.[15] AI systems are now being developed to recognize not only overt emotional expressions but also subtle micro-facial expressions. This development raises intriguing possibilities for integrating technological tools into the realm of assessing human behaviour[16], potentially bridging the gap between the nuanced capabilities of human agents and the analytical power of technology.

The integration of AI into microexpression analysis brings both advantages and challenges. On the positive side, AI systems can process vast amounts of visual data at incredible speeds, potentially identifying patterns and microexpressions that human observers might miss. This could enhance the overall accuracy and efficiency of assessments conducted during intelligence operations. On the other hand, challenges such as the contextual understanding of emotions, cultural variations in facial expressions, and the dynamic nature of human communication pose hurdles for AI systems. Human agents, with their inherent ability to interpret complex socio-cultural contexts and adapt to nuanced communication, still hold a unique edge in certain scenarios.

The integration and tension between HUMINT and TECHINT has also become particularly evident in the realm of Unmanned Aerial Vehicles (UAVs) or drones. While conventional wisdom dictates on-ground validation of targets before the deployment of drones, the increasing reliance

[15] Zhou, Y., Song, Y., Chen, L., Chen, Y., Ben, X., & Cao, Y. (2022). A novel micro-expression detection algorithm based on BERT and 3DCNN. *Image and Vision Computing*, *119*, 104378. https://doi.org/10.1016/j.imavis.2022.104378

[16] *Work: Human-Machine Teaming Represents Defense Technology Future*. (n.d.). U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/628154/work-human-machine-teaming-represents- defense-technology-future/

on TECHINT has created a shift in the dynamics of intelligence operations. This is driven by the desire to minimize the risk to human assets in the field, even if it means accepting a certain level of uncertainty and potential collateral damage.

In the context of counterterrorism and military operations, the use of drones exemplifies the integration of TECHINT with traditional HUMINT practices.[17] Drones equipped with advanced sensors, cameras, and data analytics capabilities can gather vast amounts of information from the air. This TECHINT-driven approach enables intelligence agencies to track and monitor potential targets without exposing human agents to the dangers of hostile environments. However, this shift is not without its challenges and ethical dilemmas.[18] The precision of drone strikes relies heavily on accurate intelligence, and there have been instances where mistaken targets led to civilian casualties. The tension arises from the trade-off between minimizing the risk to human agents and the potential for unintended consequences in TECHINT-driven operations.[19] The question of accountability and the ethical considerations surrounding targeted killings through drone strikes remain subjects of intense debate and scrutiny. One prominent example highlighting the integration and tension between HUMINT and TECHINT in drone operations is the use of armed drones in the War on Terror. The United States' targeted killing program, particularly in regions like Pakistan, Yemen, and Somalia, has relied extensively on drone strikes to eliminate high-value targets associated with terrorist organizations.[20]

---

[17] *Counterterrorism from the Sky? How to Think Over the Horizon about Drones*. (n.d.). Www.csis.org. https://www.csis.org/analysis/counterterrorism-sky-how-think-over-horizon-about-drones

[18] Davies, P. H. (2013). Information warfare and the future of the spy. In *Cybercrime* (pp. 251-268). Routledge.

[19] Margolis, G. (2013). *The Lack of HUMINT: A Recurring Intelligence Problem* [Review of *The Lack of HUMINT: A Recurring Intelligence Problem*]. University of North Carolina Wilmington.

[20] Cyber, I., & Security. (2017). *An Intelligence Civil War: "HUMINT'" vs. "TECHINT."* *1*(1), 67. https://www.inss.org.il/wp-content/uploads/2017/03/An-Intelligence-Civil-War-%E2%80%9CHUMINT%E2%80%99%E2%80%9D-vs.-%E2%80%9CTECHINT%E2%80%9D.pdf

Impacts and Challenges

The integration of technology, especially cybertech into HUMINT has yielded a spectrum of positive impacts, enhancing the efficacy of intelligence operations on multiple fronts.

Rapid information retrieval stands as a cornerstone of the positive impacts that technology, particularly in the cyber realm, has had on HUMINT. This capability represents the ability to swiftly and efficiently access a vast array of data and information relevant to intelligence operations, providing significant advantages to intelligence agencies and their operatives. Big data analytics and Open-Source Intelligence (OSINT) allow operatives to access and analyse a staggering amount of data each day from open and classified sources in real-time. In the realm of cybersecurity and counterintelligence, rapid information retrieval is critical for identifying and mitigating cyber threats. Cyber Threat Intelligence (CTI) platforms leverage automated systems to collect, analyse, and disseminate information about potential threats in the digital landscape. This proactive approach enables intelligence agencies to stay ahead of cyber adversaries and prevent potential attacks.

Cloud computing has also revolutionized the storage and retrieval of vast datasets. Intelligence agencies can leverage cloud-based platforms to store, organize, and retrieve information rapidly from secure and accessible repositories.[21] This not only facilitates faster information retrieval but also ensures scalability and flexibility in handling large volumes of data.

Covert communication technologies play a critical role in ensuring the secure exchange of information among HUMINT operatives. Encryption tools, secure messaging applications, and anonymous communication platforms allow operatives to share sensitive information while minimizing the risk of interception. Covert communication is essential in protecting the identities of human assets and maintaining the confidentiality of intelligence operations. The use of

[21] *UK Intelligence Agencies and the Commercial Cloud: What Does It All Mean?* (n.d.). Www.rusi.org. https://www.rusi.org/explore-our-research/publications/commentary/uk-intelligence-agencies-and-commercial-cloud-what-does-it-all-mean

technology not only enhances the security of HUMINT operations but also enables operatives to operate in high-risk environments with reduced risk of compromise.

Another important result of tech fusion is Cybernetic influence operations, involving leveraging technology to shape perceptions, influence public opinion, and manipulate information in the digital realm.[22] Intelligence agencies employ cybernetic influence operations to advance strategic objectives, counter disinformation, and influence decision-making processes. Social media platforms, online forums, and digital communication channels serve as battlegrounds for these operations. Through the targeted dissemination of information, strategic messaging, and the creation of online narratives, HUMINT operatives can exert influence on a global scale.

However, this rampant advancement in technology of cyber and AI has also created challenges for the intelligence community.[23]

Marshall McLuhan, who is known for his contribution to the field of media studies, foresighted regarding a potential third World War, that it would be an information war with blurred lines between military and civilian participation, which resonates strongly in the contemporary landscape.[24] The evolution of technology has indeed democratized access to tools once restricted to government circles, leading to a paradigm shift where individuals, rather than organized entities, play significant roles in global information warfare.

The proliferation of misinformation campaigns on social media platforms and the surge in cyber-attacks on state-operated databases underscore McLuhan's prediction. The distinction between traditional warfare and information warfare is becoming increasingly blurred, with civilians

[22] P. Brangetto and M. A. Veenendaal, "Influence Cyber Operations: The use of cyberattacks in support of Influence Operations," 2016 8th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2016, pp. 113-126, doi: 10.1109/CYCON.2016.7529430.

[23] O'Brien, A. (2022, June 21). *The Power and Pitfalls of AI for US Intelligence*. Wired. https://www.wired.com/story/ai-machine-learning-us-intelligence-community/

[24] Mcluhan, M., & Fiore, Q. (2003). *War and peace in the global village*. Penguin Canada.

becoming inadvertent or willing participants in these activities. The digital realm has empowered individuals to wield influence beyond physical borders, making it a battlefield where ideological conflicts manifest through the dissemination of information.

Crosston and Valli's observations about the accessibility of technology to the masses further highlight this shift.[25] Encryption, coding, and data mining, once the domain of specialized professionals, are now skills that can be acquired through user-friendly applications and educational resources, through paid or even free sources like YouTube. The democratization of technology has implications not only for malicious activities but also for the empowerment of individuals seeking to protect their privacy and secure their communications.[26]

OSINT is a striking example of how technology has permeated public and private spheres. What was once a closely guarded technique limited to government circles is now openly taught at universities. The massive influx of data into the public domain, facilitated by the integration of technology into everyday life, has made OSINT a valuable tool for understanding trends, sentiments, and patterns.

This change is now also ironically highlighting the importance of on-ground traditional HUMINT operations. The ongoing conflict between Israel and Palestine, particularly along the Gaza Strip, underscores the critical role of traditional HUMINT operations amidst the challenges posed by misinformation on social media. The situation that unfolded since October 7th, 2023, following Hamas militants' attacks on Israeli targets, has led to a significant counter-offensive from the Israeli side.

While the visual evidence of the conflict is apparent, the spread of misinformation on social media platforms has added a layer of complexity. Inadequate fact-checking and the rapid dissemination

[25] Cyber, I., & Security. (2017). *An Intelligence Civil War: "HUMINT'" vs. "TECHINT."* 1(1), 67. https://www.inss.org.il/wp-content/uploads/2017/03/An-Intelligence-Civil-War-%E2%80%9CHUMINT%E2%80%99%E2%80%9D-vs.-%E2%80%9CTECHINT%E2%80%9D.pdf

[26] Ibid

of unverified information through official news platforms can contribute to a distorted narrative. In such circumstances, relying solely on technical sources or open-source data, even with the assistance of data mining AI, may result in flawed intelligence.

Traditional HUMINT operations, involving on-the-ground human agents, become crucial in verifying information, understanding the nuances of the conflict, and providing context that might be absent in purely technical analyses. HUMINT allows for a deeper understanding of the local dynamics, perspectives, and motivations behind the events, offering a more comprehensive and accurate intelligence picture.

Another issue of relevance is the fiscal policy aspect in intelligence communities, where the budget allocation balance between HUMINT and TECHINT resources is strained. The current landscape of intelligence operations has resulted in a substantial allocation of budgetary resources to technological development, which, while offering significant capabilities, also brings about risks such as the rapid obsolescence of innovations.[27] In this context, TECHINT has gained financial attention and investment priority, potentially at the expense of HUMINT resource development.[28] Despite the undeniable importance of technological advancements, it is crucial to acknowledge that HUMINT, involving human agents, remains indispensable at the forefront of conflict and espionage. Instead of viewing these elements in competition, an integrated approach should be pursued, leveraging technological capabilities to enhance human intelligence and vice versa.

Future Trends and Developments

A major reason for assessment of how technology has been integrated with HUMINT operations

[27] Cyber, I., & Security. (2017). *An Intelligence Civil War: "HUMINT'" vs. "TECHINT."* 1(1), 67. https://www.inss.org.il/wp-content/uploads/2017/03/An-Intelligence-Civil-War-%E2%80%9CHUMINT%E2%80%99%E2%80%9D-vs.-%E2%80%9CTECHINT%E2%80%9D.pdf

[28] Margolis, G. (2013). *The Lack of HUMINT: A Recurring Intelligence Problem* [Review of *The Lack of HUMINT: A Recurring Intelligence Problem*]. University of North Carolina Wilmington.

up till now is to also understand the potential impact of the rapidly developing emerging technologies on intelligence communities in the near future.

Artificial Intelligence and Machine Learning, which were emerging technology just over a decade ago, are now rampantly spreading technologies in all industries, and have revolutionised the way in which data is assimilated and analysed. The most talked about emerging tech, Quantum computing is expected to introduce reshaping possibilities for the landscape of intelligence gathering. Similarly, the proliferation of biometric technologies and genetic profiling will unlock a huge dataset for human identification and profiling. China has already created a mega surveillance system comprising multiple levels of bio-identification data for state purposes. The increase in the number of malware cyber-attacks on public and private sector systems in recent years has also increased the necessity for developing more robust methods for attributing cyber threats to specific actors.

As technology continues to evolve, intelligence agencies must adapt to these trends, harnessing emerging capabilities while addressing the associated challenges.

Conclusion

In conclusion, the integration of technology with Human Intelligence represents a paradigm shift in the realm of intelligence operations. The historical journey from traditional espionage to the contemporary era of cybernetic HUMINT reflects the adaptability of intelligence agencies to technological advancements.

The use of technology in HUMINT operations has had a number of positive impacts, including reduction of on-field risk, rapid information retrieval and the ability to interact and deal with extremely large datasets. However, this has also raised concerns regarding the disbalance in attention towards HUMINT in favour of TECHINT, creating a policy impact on resources and operations.

As intelligence operations continue to evolve, the future of HUMINT requires a proactive approach to navigate national security imperatives, individual privacy rights, and the ethical

considerations that underpin democratic societies. There also needs to be a balance in approach towards integrating Tech into HUMINT operations. The synergy between human intuition and technological advancement will define the effectiveness of intelligence efforts in an increasingly interconnected and complex world.

Bibliography

- Assayag, J. (1998). [Review of Empire and Information. Intelligence Gathering and Social Communication in India, 1780-1870, by C. A. Bayly]. L'Homme, 146, 289–293. http://www.jstor.org/stable/25133332
- Alvarez, D. (2013). Allied and Axis Signals Intelligence in World War II. Routledge.
- Bergen, P. L. (2012). Manhunt. Crown.
- Beechy, T. (2023). Aesthetics and the Incarnation in Early Medieval Britain. University of Notre Dame Press.
- Counterterrorism from the Sky? How to Think Over the Horizon about Drones. (n.d.). Www.csis.org. https://www.csis.org/analysis/counterterrorism-sky-how-think-over-horizon-about-drones
- Cyber, I., & Security. (2017). An Intelligence Civil War: "HUMINT'" vs. "TECHINT." 1(1), 67. https://www.inss.org.il/wp-content/uploads/2017/03/An-Intelligence-Civil-War-%E2%80%9CHUMINT%E2%80%99%E2%80%9D-vs.-%E2%80%9CTECHINT%E2%80%9D.pdf
- Davies, P. H. (2013). Information warfare and the future of the spy. In Cybercrime (pp. 251-268). Routledge.
- Duckett, R. (2017). The Special Operations Executive (SOE) in Burma. Bloomsbury Publishing.
- Fruhlinger, J. (2022, August 31). Stuxnet explained: The first known cyberweapon. CSO Online. https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html
- History of Encryption | SANS Institute. (n.d.). Www.sans.org. https://www.sans.org/white-papers/730/
- Kahn, D. (1996). The Codebreakers. Simon and Schuster.
- Kautilya, & Rangarajan, L. N. (1992). The Arthashastra. Penguin Books India.
- Margolis, G. (2013). The Lack of HUMINT: A Recurring Intelligence Problem [Review of The Lack of HUMINT: A Recurring Intelligence Problem]. University of North Carolina Wilmington

- Masterman, J. C. (2011). Double-Cross System. Rowman & Littlefield.
- Mcluhan, M., & Fiore, Q. (2003). War and peace in the global village. Penguin Canada.
- Newton-Matza, M. (2017). The Espionage and Sedition Acts: World War I and the image of civil liberties. Routledge.
- O'Brien, A. (2022, June 21). The Power and Pitfalls of AI for US Intelligence. Wired. https://www.wired.com/story/ai-machine-learning-us-intelligence-community/
- P. Brangetto and M. A. Veenendaal, "Influence Cyber Operations: The use of cyberattacks in support of Influence Operations," 2016 8th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2016, pp. 113-126, doi: 10.1109/CYCON.2016.7529430.
- UK Intelligence Agencies and the Commercial Cloud: What Does It All Mean? (n.d.). Www.rusi.org. https://www.rusi.org/explore-our-research/publications/commentary/uk-intelligence-agencies-and-commercial-cloud-what-does-it-all-mean
- Wallace, R. J. (2021). Artificial Intelligence/ Human Intelligence: An Indissoluble Nexus. World Scientific.
- Work: Human-Machine Teaming Represents Defense Technology Future. (n.d.). U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/628154/work-human-machine-teaming-represents- defense-technology-future/
- Zhou, Y., Song, Y., Chen, L., Chen, Y., Ben, X., & Cao, Y. (2022). A novel micro-expression detection algorithm based on BERT and 3DCNN. Image and Vision Computing, 119, 104378. https://doi.org/10.1016/j.imavis.2022.104378