RESEARCH DESIGN MODULE · LOUGHBOROUGH UNIVERSITY · APRIL 2026

KAM: Knowledge Analysis Monitor

How can an AI-assisted OSINT platform provide expert geopolitical and security capabilities through human-machine teaming to the civilian across both peacetime and conflict scenarios?

Karam Binning · BA History & Politics · Essay text

KAM is the civilian intelligence platform for the multipolar world. The platform aims to provide the civilian with expert capabilities and human-machine teaming through open-source intelligence, academic research and iterative development. This research proposal demonstrates its practical application within international security using a design-based research methodology to assess how an AI-assisted OSINT platform could provide expert geopolitical and security capabilities to the civilian with humanmachine teaming. No existing OSINT platform utilises AI to provide a digitally unified system for the civilian - in an era of uncertainty, this gap motivates the work. This research aims to contribute a replicable academic framework for civilian intelligence capability at a moment of national and geopolitical urgency.

KAM is an OSINT intelligence system that facilitates human-machine teaming through a three-way relationship between the platform, the user, and artificial intelligence. This assignment plans to develop modules within KAM at the academic level to facilitate expert analytical tool capabilities for the civilian (within the realms of geopolitics and security). It serves as a preliminary for the dissertation and provides a framework for other students. For this development process, the question on how an AI-assisted OSINT system could enhance civilian capabilities provides a design-based methodology. This methodology involves an assessment of the current state of KAM in the NEWS, WORLD, SIGNAL and COUNCIL modules, conducting academic research and literature review within geopolitics and security, then using obtained knowledge to implement improvements that will provide enhancement of civilian capability.

Research question

How can an AI-assisted OSINT platform provide expert geopolitical and security capabilities through human-machine teaming to the civilian across both peacetime and conflict scenarios?

1. How does OSINT methodology democratise intelligence capability at the civilian level?
2. How does human-machine teaming augment rather than replace human judgment?
3. What are the ethical implications for an AI-assisted civilian intelligence platform?

OSINT and Intelligence methodology

> *"The concept of OSINT methodology allows for search, collection, analysis and use of information from open sources, as well as the techniques and tools used." (Evangelista et al., 2021, p.1)*

While OSINT emerged from military necessity, this research provides the analytical tools and framework to enhance and democratise civilian capability. The researchers address the gap of AI use in OSINT platforms, but fail to address the gap of civilian use in OSINT platforms. The

article demonstrates that public information has its advantages for collection, but for civilian OSINT platforms, the disadvantages of security and privacy must be addressed under the same institutional frameworks as professional intelligence. All four stages of OSINT are critical for civilian use, with AI fitting across this chain as a tool for democratising capability through human-machine teaming. This means that for full capability, professional military analysis and established intelligence disciplines need to be implemented. Each discipline showcases how OSINT methodology provides practical analytical capabilities for its distinctive role. OSINT methodology allows for live monitoring of political developments and political science data; provides access to archives and documentary sources for historical contextualisation and uses open source to assess threat and verify sources for investigative reporting. OSINT platforms provide these capabilities for each distinct role, but no platform integrates these disciplines into a unified civilian OSINT system – this work is motivated by this research gap and what KAM can contribute.

War studies and historical contextualisation

The gap addressed by Kennedy-Pipe (1995) on ignoring historical complexity and producing strategic miscalculation shows that integrating historical contextualisation in the analytical tools used for live geopolitical analysis is necessary. Analytical frameworks that prioritise current threats over historical patterns identify how they produce strategic error (Kennedy-Pipe, 2018), similarly Wendt (1999) demonstrates that state behaviour cannot be understood without historical context.

Mearsheimer's (2001) realist philosophy describes the world order as an anarchic system and battleground for regional hegemony. He discusses and opposes Fukuyama's view (1992) that the liberal world order is the end of history, stating that unipolarity is temporary, and a multipolar world is not a matter of if but when for war.

When addressing this claim for the current and future state of the world, historical contextualisation is crucial. After the Cold War, the bipolar world order transitioned to US-led unipolarity, which may be fading, pushing us to a new multipolar world, potentially producing the regional hegemony of great powers that Mearsheimer examines. To historically contextualise the Darwinist nature of the self-help international system, the author uses the Partitions of Poland to showcase how Prussia sought to destroy Poland for its own survival. On the concept of peace, Mearsheimer contradicts Doyle's peace thesis (1983) by demonstrating that both autocracies and democracies necessitate security. Therefore, when assessing the OSINT system, historical contextualisation is not an academic exercise but a necessity to ensure both national and personal security for peacetime and the probable conflicts in a multipolar world - no existing OSINT platform addresses this necessity.

AI and human-machine teaming

Terrorism and Technology (Ashraf and Filippidou, 2019) outlines how technology is used by terrorists both instrumentally and symbolically, with information exploitation being made explicit - we can gather that information is just as important as the physical aspects of terrorism. It is also made clear that defence is just as important as offense with counter-terrorism

requiring matching technological capabilities. With intelligence agencies, police and military converging in tech requirements, it is the combination of people, technology and actions that allows for prediction – this can only be produced with a holistic OSINT platform.

The work from Ashraf and Kennedy-Pipe on Afghanistan (2022) exposes how Western analytical frameworks that ignore local historical and cultural context produce strategic failure; therefore, cultural relativism is insightful, as intelligence that is not completely contextualised is ineffective. Both authors argue that understanding belief systems and culture produces analytical accuracy, noting that even sophisticated actors with resources can produce analytical error when context is missing. Through this insight, the human-machine teaming and analytical accuracy of KAM can democratise the capabilities of a sophisticated state actor to the civilian.

Power in the modern world derives from information and economic interdependence, not just military capacity (Keohane and Nye, 1977). Power and Interdependence addresses how complex interdependence among nations means states are vulnerable through multiple channels simultaneously, with information management as a form of power. This suggests those who control analytical capability are at a strategic advantage. Human-machine teaming extends this capability to the civilian democratising this form of strategic power, currently exclusive to state actors.

COUNCIL is an epistemic pluralist system that addresses multiple reductionist analytical approaches, allowing the user to access intelligence through competing academic frameworks and the capability to synthesise holistic analysis through artificial intelligence to make their own judgement – enabling augmentation, not replacement. This structure allows the human to remain central – human-machine teaming means the user directs, interprets and judges with artificial intelligence extending analytical reach. The three-way relationship – KAM, User, AI – ensures human sovereignty.

Information resilience in conflict

Clarke and Knake (2010) establish the threats posed by cyber warfare using Syria, Iraq, Estonia and Georgia to present their case and examine how it is the civilian who is most at risk, with much cybertechnological focus on attack rather than defence. The Middle Eastern cyber-attacks demonstrate two fronts – the physical and the psychological – blocking Syrian air defence radars and using encrypted emails to desert Iraqi soldiers.

With Estonia being a digitally unified country, it became an easy target for the Russian DDOS attacks that spread through worm infections across the domains, leading to a shutdown of external communications and the spread of misinformation. Similarly, Georgia experienced cyber-attacks that framed the country as hostile to foreign banks – both cases demonstrate how advanced and adaptive Russian cyber warfare left both countries digitally paralysed. Clarke's analysis reveals the current limitations of KAM as a civilian intelligence platform – with its digital unification, it also becomes a target to cyberattack that must be mitigated through AI cyber defence, not only for platform uptime and user protection but also for platform integrity, keeping an honest analysis across the system as information is one front of cyberwarfare.

Design-based Methodology

The design-based methodology is an iterative process that involves assessing the current state of KAM across the NEWS, WORLD, SIGNAL and COUNCIL modules, identifying gaps through academic literature, implementing research-based improvements and evaluating these improvements against academic frameworks.

Other methodologies fall short due to the practical application of this OSINT system, where it is not a theoretical concept but real. Therefore, the practical reality demands a design-based approach.

To assess data accuracy, cross-examination of data feeds against external information is critical. For assessing expert-level functionality for enhanced civilian capability, academic discussion with Ashraf and Kennedy-Pipe on security and war studies provides professional analytical frameworks for the system. The NEWS module requires expanding and evaluating the current 29 sources to ensure regional and political balance. The methodology for the COUNCIL includes assessing each reductionist approach against its academic literature and determining the number and structure of approaches for credible holistic synthesis through KAM.AI and testing this against individual approach outputs to provide augmentation to the user.

Cyber War presented the physical and psychological fronts of cyberwarfare through the Iraqi and Syrian case studies and displayed the vulnerability of digital unification with Estonia and Georgia. These findings can be tested against the platform's information resilience and SIGNAL, as well as the platform's own security architecture and the cyber defence requirements. Ashraf and Kennedy-Pipe's assessment of the western analytical failures in Afghanistan presents findings that can test against the cultural and contextual relativism necessary for the system's intelligence briefing. During early development, an incidental intelligence discovery from NEWS provided information on automated robot use on the Ukrainian front, without a specific search, therefore already demonstrating the system's live analytical value. For future conflict scenarios such as Taiwan invasion and Arctic security, the geopolitical layer of WORLD can be tested against Mearsheimer's multipolar inevitability thesis and as a preliminary dissertation case study.

The ethical implications and risks associated with the platform to be examined include:

data accuracy and source bias can be informed by Said's (1978) analysis of how knowledge systems embed political assumptions; thus, the OSINT methodology requires source triangulation, dual use concern with the system being theoretically misused, and platform security issues with the vulnerability posed from its digital unification. All AI use is fully declared per Loughborough University guidelines.

The limitation of this methodology presented is the iterative nature of design-based research, with findings remaining contingent on the current development stage and requiring ongoing refinement from academic research and expert consultations as the platform evolves.

Dr Afzal Ashraf is a practitioner-scholar with 30 years of RAF experience with operations in Iraq and Afghanistan, with current research on AI in cybersecurity, will provide an expert assessment of OSINT military applications, and the future AI cybersecurity/defence

implementations for the platform, with his knowledge on hybrid warfare and counter-terrorism also having implications for KAM. His expertise will directly inform the SIGNAL module for the cyber defence architecture and a reductionist security approach for the COUNCIL.

After first discussion with Ashraf (21 April, 2026), a reflection on the purpose of this research proposal and the identified gap this research aims to address has been reassessed.

Dr Caroline Kennedy-Pipe is a Professor of War Studies with Cold War and contemporary conflict expertise, having been the specialist advisor to the House of Commons Defence Committee, providing historical contextualisation frameworks and historical analysis methodology as well as sentiment on contemporary Russian and Arctic conflict scenarios. Kennedy-Pipe's expertise will directly inform the historical layer of the WORLD module – and the historical reductionist approach of the COUNCIL – giving a contextualised analytical framework to prevent retrospectivity.

To conclude, no existing OSINT platform utilises AI to provide expert analytical frameworks and human-machine teaming to enhance the capabilities of the civilian for both peacetime and conflict. We are entering a period of multipolar transition and technological revolution, with the UK government (HM Government, 2026) placing civilian AI security applications as a national priority. This research proposal establishes not just a platform but a replicable academic framework that is deployable across disciplines to future researchers contributing academic expertise.

Bibliography

Ashraf, A. and Filippidou, A. (2019) Terrorism and Technology. [online] Available from: https://www.researchgate.net/publication/330039460 [Accessed 21 April 2026]

Ashraf, A. and Kennedy-Pipe, C. (2022) 'Woman, war, and the politics of emancipation in Afghanistan', LSE Public Policy Review, 2(3), pp. 1–11.

Clarke, R.A. and Knake, R.K. (2010) Cyber War: The Next Threat to National Security and What to Do About It. New York: Ecco.

Doyle, M.W. (1983) 'Kant, liberal legacies, and foreign affairs', Philosophy and Public Affairs, 12(3), pp. 205–235.

Doyle, M.W. (1997) Ways of War and Peace. New York: Norton.

Evangelista, J.R., Sassi, R.J., Romero, M. and Napolitano, D. (2021) 'Systematic literature review to investigate the application of open source intelligence (OSINT) with artificial intelligence', Journal of Applied Security Research, 16(3), pp. 345–369.

Fukuyama, F. (1992) The End of History and the Last Man. New York: Free Press.

HM Government (2026) AI Opportunities Action Plan. London: DSIT.

Keohane, R.O. and Nye, J.S. (1977) Power and Interdependence: World Politics in Transition. Boston: Little, Brown.

Kennedy-Pipe, C. (1995) Stalin's Cold War: Soviet Strategies in Europe, 1943–1956. Manchester: Manchester University Press.

Kennedy-Pipe, C. (2018) 'Terrorism studies: what we have forgotten and what we now know', Government and Opposition, 53(2), pp. 356–384.

Mearsheimer, J.J. (2001) The Tragedy of Great Power Politics. New York: Norton.

Said, E.W. (1978) Orientalism. New York: Pantheon Books.

Wendt, A. (1999) Social Theory of International Politics. Cambridge: Cambridge University Press.

Anthropic (2026) Claude [online]. Available from: https://claude.ai [Accessed 19–22 April 2026]