Assessing Non-Kinetic Effects in Support of Military Operations: An Inference-Driven Framework

Bruce Chojnacki and Nick Harrell
Army Cyber Institute, West Point, NY, USA

bruce.chojnacki@westpoint.edu
nicholas.harrell@westpoint.edu

Abstract: Modern military operations increasingly integrate non-kinetic effects to support and enhance kinetic operations on the battlefield. Intelligence, surveillance, and reconnaissance assets provide a reliable means to measure kinetic effects on adversaries during combat. However, there is a gap in intelligence collection for assessing and quantifying non-kinetic effects, such as shaping perceptions, influencing decision-makers, or degrading adversary morale. These effects are difficult to measure with traditional intelligence techniques because they occur in the cognitive dimension, where observable indicators are limited, and measurement is complex. This limitation introduces operational risks for military leaders, as they cannot always be sure whether a non-kinetic asset will achieve the desired effect or if a behavioural change has taken place. This paper introduces a framework for developing measures of effectiveness for cyber, information warfare, and psychological operations planners to evaluate non-kinetic operations supporting kinetic actions. Drawing on case studies such as the Russo-Georgian conflict and the Second Nagorno-Karabakh war, the framework combines intelligence indicators from OSINT, social media analytics, changes in adversary leadership behaviour, shifts in military posture, and other measurable phenomena to generate quantifiable metrics. It also considers collateral, second-, and third-order effects to assess whether non-kinetic operations are achieving their operational objectives. By offering intelligence analysts, planners, and military leaders a rigorous method for planning, executing, and evaluating non-lethal effects, this approach improves effect synchronization, enhances risk assessment, and aids leaders' decision-making.

Keywords: Cyber, Information warfare, MoE, Non-kinetic, Indicators, Influence, PSYOPs

1. Introduction

Military operations worldwide increasingly depend on cyber activities, information warfare, and Psychological Operations (PSYOPs) as essential tools to shape favourable battlefield conditions and achieve mission objectives against adversaries. Throughout history, military leaders have conducted battle damage assessments (BDA) of enemy forces after kinetic strikes, including arrow barrages, cavalry charges, artillery fire, and precision aerial bombing (Chairman of the Joint Chiefs of Staff, 2019). These actions have a clear cause-and-effect relationship that can be observed by a scout, an aerial drone, or a surveillance satellite.

Measuring the impact of non-kinetic effects and confirming if the desired outcome is being met can be difficult. These effects often occur in the electromagnetic spectrum (EMS), cyberspace, or the human brain's cognitive space (Paul et al., 2015). These domains are usually not observable to humans. Observing these effects requires monitoring indicators that are secondary or tertiary to the original target. Even when these indicators can be monitored, there is a gap in the training, experience, and knowledge of military intelligence analysts in observing changes and assessing the effectiveness of non-kinetic effects (Fortson, 2007).

This presents a dilemma for military leaders when employing non-kinetic effects during combat operations. They must understand their capabilities and trust that these assets can produce the desired effect on enemy forces (Aguirre et al., 2024). These choices put soldiers' lives, military resources, and mission success at risk. While military leaders are generally confident in their ability to employ, deliver, and assess the effects of kinetic weapons and equipment on the battlefield, uncertainty about non-kinetic effects and the inability to conduct BDA can lead to hesitation in relying on these capabilities.

It is essential to develop a comprehensive framework for measuring non-kinetic effects, including both traditional and non-traditional indicators. This requires planners and intelligence analysts to thoroughly understand the operational plan and coordinate non-kinetic resources to support the mission (Richardson, 2009). Resources should be allocated to detect and evaluate environmental changes in adversary behaviour, cyberspace, and the information environment that are either beneficial or detrimental to friendly forces. Systems must be established to alert when a significant deviation from the baseline is observed.

This paper will explore operations that employed non-kinetic effects to support military operations. It will analyse the strengths, weaknesses, opportunities, and threats of these operations and offer insights into why they succeed or fail. The framework provided will give leaders, planners, and analysts a comprehensive, quantitative approach for planning and evaluating non-kinetic effects in support of military operations.

2. Assessment Gap

2.1 Doctrinal Framing of Assessment

NATO and U.S. doctrine, specifically JP 3-13 (Information Operations), JP 3-12 (Cyberspace Operations), and AJP-3.10 (Allied joint doctrine for information operations), recognize that assessing information and cyberspace operations is inherently difficult, especially when effects do not cause observable physical damage (Joint Chiefs of Staff, 2012; Joint Chiefs of Staff, 2018; NATO, 2015). The difficulty is increased by a time gap between action and effect: kinetic operations produce immediate, visible damage, while information and cyberspace effects may take days, weeks, or months to appear, often outside tactical decision cycles. Many effects occur in the cognitive or informational dimension of the operational environment and require monitoring of indirect indicators. NATO doctrine states that successfully conducting Info Ops depends on ongoing monitoring and assessment (NATO, 2015). These efforts require collecting all-source intelligence and paying close attention to the adversary's behaviour and attitudes.

NATO and U.S. doctrine are consistent in their use of measures of performance (MOP) and measures of effectiveness (MOE). But the doctrine provides little guidance on how to move from observed indicators to confident conclusions about whether an effect occurred and whether that effect resulted from the operation in question. The doctrine explains how these metrics fit within the decision-making framework for authority; however, the effectiveness of the metrics themselves remains unclear. JP 3-13 mentions weighting metrics to highlight the relative importance of one over the other but provides no transparent methodology for deriving these weights (Joint Chiefs of Staff, 2012). The absence of an inferential methodology can be consequential when commanders must choose between kinetic and non-kinetic options. Without transparent, defensible assessment frameworks, non-kinetic effects remain difficult to measure and assess. This creates a potential bias in operational planning toward options that yield more legible, observable strategic value through measurable outcomes.

2.2 Non-kinetic Assessment

There is a doctrine for non-kinetic assessments, but it remains isolated by capability and limited to observable indicators. CJCSI 3162.02 (Methodology for Combat Assessment) includes a Cyberspace Assessment Determination Matrix that categorizes temporary cyber effects as DENIED, DISRUPTED, DEGRADED, DECEIVED, and MANIPULATED (Chairman of the Joint Chiefs of Staff, 2019). JP 3-12 covers the evaluation of cyberspace operations using MOPs and MOEs, which help determine how efforts contribute to the larger operation or objective. JP 3-13 adopts a similar approach with MOP and MOE in Information Operations; however, it highlights observability and quantification as critical for measuring effects, and MOEs are often linked to the progress of the operation (Joint Chiefs of Staff, 2012).

Two interconnected challenges exist within these doctrines. First, the timeframe for observing non-kinetic effects often surpasses tactical decision cycles, creating pressure to assess prematurely using proxy indicators. Second, the doctrine assumes observability without clearly defining its boundaries. The absence of boundaries makes it unclear whether indirect indicators (e.g., economic behaviour, migration patterns, social media sentiment) are legitimate data or inadmissible inferences. Recognizing which observable indicators can be identified through second- and third-order observations is crucial for increasing commander confidence in non-kinetic options. JP 3-13 highlights observable indicators such as rallies and demonstrations, but many other assessment avenues exist, including economic behaviour and migration. However, this process is not sufficiently addressed within the planning phases of a military operation.

In JP 3-13, these indicators are called measures of effectiveness indicators (MOEIs). They are usually developed during the planning phase, especially during course of action development (COADEV). The difficulty lies in measuring MOEs, which are often unobservable and mostly qualitative. In the doctrine, an example of an effect is "increase in a city populace's participation in civil governance." The MOE here is qualitative, with metropolitan citizens showing increased support for the democratic leadership elected on July 1. Then, an MOEI is a decrease in the number of anti-government rallies or demonstrations in a city since July 1. Three MOEIs are provided that can be directly measured to infer the MOE, indicating that the effect has occurred. This doctrinal approach is fundamentally sound; however, it assumes a single causal pathway from operation to effect. The doctrine does not address the issue of equifinality, or the possibility that alternative competing hypotheses could produce the same observable outcomes. For example, a decrease in anti-government rallies since July 1 could align with several hypotheses: the target population genuinely shifted support for governance (the intended effect), security crackdowns made public gatherings too risky (coercion rather than persuasion), opposition groups

shifted to less visible tactics, or exogenous factors (economic conditions, seasonal patterns) temporarily reduced mobilization. Without a framework to distinguish among these hypotheses, the same indicator data can yield contradictory conclusions about operational effectiveness.

For PSYOPs, JP 3-53 offers guidance on planning, executing, and assessing effects in joint military operations. However, the doctrine also openly recognizes inherent limitations, including the absence of a clear method for determining whether those psychological effects were achieved. It specifies the need for direct observability, which remains a common challenge in conducting non-lethal operations (Joint Chiefs of Staff, 2003). The doctrine also discusses the coordination and synchronization of PSYOPs with IO capabilities; however, there is no procedural guidance for assessing the impact of a PSYOP operation.

By examining the doctrine in relation to non-kinetic operations, we see that indirect, observable indicators are mentioned but not explained. This might be due to a lack of reliable evidence from alternative indicators. However, non-kinetic operations are becoming increasingly intertwined with military operations as the military incorporates more non-lethal assets.

2.3 Analytical Gaps in Doctrine

The current doctrine outlines the observation requirements but does not provide sufficient guidance on interpreting those observations to reach a conclusion. The three analytical gaps that impact non-kinetic assessment include:

Gap 1: Lack of formal procedures for hypothesis discrimination. The doctrine states that observed indicators support the hypothesized effects, but the same indicators could be explained by two or more different mechanisms. Without structured procedures, such as Analysis of Competing Hypotheses (ACH), to differentiate among explanations, the analysis is vulnerable to confirmation bias and enemy deception.

Gap 2: Absence of a methodology for combining evidence. Joint Publication 3-13 acknowledges that multiple MOEIs might be needed to make a judgment about a single MOE and suggests using weights based on relative importance, but it does not specify a clear method for assigning those weights or for integrating seemingly unrelated indicators.

Gap 3: Absence of a shared vocabulary for expressing confidence. The assessment results differ based on capability and level. In cyber operations, results are reported in CTEAR format with category labels such as (DENIED, DEGRADED, DISRUPTED); for information operations, results are assessed qualitatively using an MOE; and for psychological operations, results recognize the difficulty of measuring PSYOP effects but do not offer a methodology for measurement. This gap in doctrine hampers the ability to compare kinetic and non-kinetic courses of action, as commanders cannot assess their relative effectiveness.

These gaps are more than just administrative issues. They reveal structural pressures that favour actions with clear, visible outcomes over those with potentially greater strategic importance but that require more time-consuming data collection, inferential reasoning, and acceptance of uncertainty. Closing these gaps demands both methodological and doctrinal changes.

3. Analytical Framework: Analysis of Competing Hypotheses

3.1 Rationale for Framework Selection

The issue outlined in Section 2 (Assessment Gap) is fundamentally inferential: although guidelines for indicators exist, there is no formal way to draw reliable conclusions about effects based on observed indicators. This has historically been a challenge in intelligence analysis, which often involves inferring from incomplete, ambiguous, or deceptive information (Richardson, 2009). Therefore, applying intelligence analytical techniques to operational assessment is not a category error; rather, it acknowledges that assessing non-kinetic effects is an intelligence challenge within an operational setting.

Several structured analytical techniques are crucial for finding potential solutions. Red teaming offers alternative perspectives but lacks a formal process for evaluating these options against evidence (Department of Defense, 2016). These methods either generate alternatives without thorough evaluation, depend on probabilistic data that are missing in operational environments, or identify reasoning errors without providing ways to fix them.

The Analysis of Competing Hypotheses (ACH), developed for the CIA by Richards Heuer, addresses the problem of equifinality, which is choosing among multiple hypotheses that each fit a body of evidence (Heuer, 1999). In ACH, analysts create several hypotheses that could yield the same outcome. They then present their evidence

and arguments to assess how likely each piece of evidence is to align with the different hypotheses. This process helps analysts reduce their own cognitive biases and make decisions based on evidence about causality (Valtorta et al., 2005). It also shows how ACH can be used within a Bayesian model, illustrating how analysts might use Bayesian graphs to continuously update their evidence and assumptions; however, there is no proven effectiveness of this method for operational use.

3.2 ACH Methodology

Analysis of Competing Hypotheses is an eight-step process based on cognitive psychology and the scientific method. It counteracts Confirmation Bias by considering all competing hypotheses against the evidence at the same time (Heuer, 1999).

Step 1: Identify Hypotheses. Engage a variety of analysts in a brainstorming session to generate possible answers, ensuring the hypotheses are mutually exclusive and limited to a few (no more than 7).

Step 2: List Evidence and Arguments. Gather all available evidence for each hypothesis, including indicators, deductions, and assumptions, and state assumptions clearly so they can be challenged.

Step 3: Create a matrix and evaluate diagnosticity. Organize the matrix with the hypotheses as columns and the evidence as rows. Enter each cell as "C," "I," or "N/A." Evaluate the rows from left to right, noting which hypotheses each piece of evidence differentiates. The higher the evidence's diagnosticity, the more it will support some hypotheses and refute others. Evidence that fits all hypotheses has low diagnosticity.

Step 4: Refine your matrix. Eliminate non-diagnostic evidence and identify gaps. Make changes as needed.

Step 5: Tentative conclusions. Rank the hypotheses based on the weight of the incompatible evidence and choose the one with the least incompatible evidence rather than the one with the most compatible evidence.

Step 6: Sensitivity Analysis. Determine which piece of evidence or assumption supports the answer, and if removing an item changes the answer, examine it further.

Step 7: Report conclusions. Report all hypotheses and the reasons for rejecting alternatives, providing an audit trail of reasoning.

Step 8: Determine future milestones. Establish indicators of changes in probability to enable continuous monitoring rather than a point-in-time assessment.

The power of ACH lies in its ability to externalize hypotheses, evidence, and their connections, making shortcuts visible and correctable.

3.3 Adaptation for Operational Assessment

One of the primary outputs of this type of assessment is a matrix that clearly displays the development of each MOEI and whether each one contributes to or detracts from the overall effect. Planners can assign more detailed weights to each indicator for each effect. This helps the operations officer assess success criteria more thoroughly and avoid relying too early on proxy indicators to determine effects, which could lead to errors in BDA.

3.4 Assessment Criteria for Use-case Analysis

To evaluate the usefulness of ACH for non-kinetic assessment, the next section examines two historical cases. Each case is analysed using four criteria derived from the framework:

1. **Hypothesis identification** — Were multiple competing explanations for the observed indicators considered?
2. **Diagnostic evidence** — Was any evidence identified that could discriminate among hypotheses, or was it only evidence consistent with the preferred explanation?
3. **Evidence integration** — Was a systematic method used to weigh and synthesize the indicators?
4. **Confidence expression** — Was uncertainty about the assessment explicitly communicated?

4. Case Review

In this case review, we apply the ACH to two historical cases in which non-kinetic effects were used alongside military actions on the battlefield. ACH matrices are employed to evaluate alternative explanations for observed changes in the information environment and to refute competing hypotheses by systematically comparing them to available indicators. The limitation of this analysis is that it is conducted after the fact, since we already know

the outcomes of the specific operation; however, this case review shows how a military planner could use this approach to overcome cognitive biases when assessing non-kinetic effects on a given target.

4.1 Russo-Georgian War (2008): Cyber and Info Warfare in Support of Maneuverer Forces

4.1.1 Operational background

The Russian military invaded Georgia on August 8, 2008. This campaign is seen as the first major instance of a large-scale cyberattack coinciding with military action. The cyber operations were notable because they were not directly linked to the Russian government. Evidence shows they were carried out by hacktivists and Russian organized crime (Shakarian, 2011). Russian forces also launched an information warfare (IW) campaign to justify their actions and sow confusion. Before the invasion, tensions between Russia and Georgia increased throughout the year, mainly over disputes involving the separatist regions of Abkhazia and South Ossetia (White, 2018).

Russia supported South Ossetian separatist forces and influenced their attacks on Georgian forces starting on August 1, 2008, using artillery fire and bombings. The first phase of the cyber operation began on August 7, 2008, involving coordinated attacks, including Distributed Denial-of-Service (DDoS) attacks on government and media websites. In the second phase, the operation targeted financial and educational institutions. This was followed by website defacement and the recruitment of Russian patriots (Shakarian, 2011). The cyber operations coincided perfectly with Russia's land invasion of Georgia with armoured and mechanized forces.

4.1.2 Non-kinetic effects

Cyber Operations:

- DDoS attacks targeting critical communication systems used by the government, businesses, and media.
- Website defacement of official pages.
- Spam email campaigns against Georgian politicians (Shakarian, 2011).

Information Warfare:

- Russia influenced South Ossetia to attack Georgian villages in the area. This led the Georgian military to launch an offensive against South Ossetian forces. Russia expected this and used the opportunity to claim that Georgia was committing genocide in the region, thereby justifying Russia's invasion to stop the genocide (Chincharadze, 2024).
- Posting pro-Russian messages, disparaging Georgian leaders, and spreading disinformation about current events (Shakarian, 2011).
- Disruption of communication channels to isolate, silence, and delay the Georgian government, military, and civilian population.

4.1.3 Assessing Effects And Attribution

Three competing hypotheses are analysed as potential causes of Georgian communication degradation. Behavioural and informational indicators are assessed for their potential to offer alternative explanations. This analysis incorporates the indicators into an ACH matrix and assigns a confidence level to each indicator.

Based on available historical evidence, there is no indication that Russian planners used a formal assessment framework, although observable adaptations suggest they conducted informal evaluations of effects. These effects appear to have been tested experimentally, and Russian forces were ready to exploit any changes that gave them an advantage in the conflict. The analysis of the conflict mainly relies on what was observed or detected through technical means, such as troop movements, website shutdowns, and network traffic disruptions, rather than on whether the Russians achieved their desired effects.

Known Observable Outcome: The Georgian government experienced degraded internal communications and denied access to international audiences (Shakarian, 2011).

Hypothesis	Description
H1	Cyber-attacks directly degraded Georgian C2 and external communications
H2	Georgian communications failures were primarily due to pre-existing infrastructure limitations

Hypothesis	Description
H3	Georgian government organizational dysfunction caused coordination failures

Indicators	H1 (Cyber)	H2 (Infrastructure)	H3 (Organizational)
Delayed Georgian official statements to international media	C	I	C
Loss of Georgian media websites during the invasion window	C	C	I
Relocation of web hosting to foreign servers	C	I	I
Russian narrative dominance in the early conflict phase	C	I	C
National Bank suspended electronic services	C	C	N/A
Georgian shift to diplomatic channels for messaging	C	I	C

(C = Consistent, I = Inconsistent, N/A = Not applicable)

Assessing the conflict using these observable behavioural and informational indicators suggests that cyber operations significantly contributed to the degradation of the Georgian government's internal and external communication channels (H1). Although the indicator set does not prove complete causality, the timing of communication delays, website outages, digital service relocations, and Russian narrative dominance provides enough evidence to support this hypothesis over explanations based on infrastructure limitations or organizational dysfunction. The Georgian government's infrastructure and organizational problems likely worsened the disruptions, but the indicators point to cyber operations and information warfare as the main cause. This case highlights the value of inferential, behaviour-based indicators for attributing non-kinetic effects when there are no directly observable changes in cyberspace or the information environment.

4.2 Second Nagorno-Karabakh War (2020): Information Warfare, Psychological Operations

4.2.1 Operational background

The Second Nagorno-Karabakh War started on September 27, 2020, and ended on November 9, 2020. This conflict between Azerbaijan and Armenia was over contested territories in the Karabakh region. Azerbaijani forces are considered the winners of the conflict, and their victory was credited to the skilful use of information warfare combined with kinetic operations (Marinus, 2021).

In September 2020, Azerbaijani forces took the initiative, using unmanned aerial vehicles (UAVs) and artillery to destroy a significant portion of Armenia's tanks, vehicles, and anti-aircraft systems. The Azerbaijani military employed information operators to capture imagery and video of the destroyed equipment and published them for their enemy and the broader global audience. As the conflict progressed, both sides targeted civilian locations in pursuit of their goals. The Azerbaijani forces demonstrated an information centre that responded quickly and effectively. They were able to censor nearly all media showing strikes on Armenian civilian populations while simultaneously showcasing Azerbaijani civilians being targeted by Armenian military strikes. This created the narrative that Azerbaijan was using precision strikes to hit military targets, while Armenia was recklessly firing artillery and missiles into civilian areas (Marinus, 2021).

The information warfare campaign and the Azerbaijani ground forces collaborated to influence the Armenian population in the disputed territories to flee in early November 2020. This rapid effort resulted in a swift victory for the Republic of Azerbaijan in the region.

4.2.2 Non-kinetic effects

Information Warfare

- Release of UAV strike footage showing the destruction of Armenian armour, artillery, and air defence systems.

- Azerbaijani domestic and international narratives demonstrate accurate and lawful military operations.
- Suppression of imagery showing Azerbaijani attacks on Armenian civilian targets.

Psychological Operations

- Messaging aimed at undermining Armenian morale and confidence in their defensive capabilities.
- Influence the Armenian military to withdraw and the civilian population to flee.

4.2.3 Assessing Effects And Attribution

Unlike the Russo-Georgian case, Azerbaijan appeared to employ a planning and execution framework to synchronize non-kinetic effects, enhancing kinetic operations aimed at influencing the will of the Armenian people. The Azerbaijani military continuously adjusted IW and PSYOP messaging based on observable results throughout the conflict. This indicates a dynamic feedback loop linking battlefield successes to non-kinetic activities. In this conflict, assessment mainly depended on adversary behaviour and population response rather than disruption of technical systems.

Known Observable Outcome: The Armenian military and civilian population in the disputed territories quickly fled the area by the end of the conflict.

Hypothesis	Description
H1	Information warfare and psychological operations directly damaged Armenian morale and their willingness to remain in the territory.
H2	The Armenian collapse was primarily due to kinetic losses and the opponent's technological advantage.
H3	Armenian organizational dysfunction led to the withdrawal of military and civilian personnel.

Indicators	H1 (Info/PSYOPS)	H2 (Kinetic)	H3 (Organizational)
Persistent release of UAV strike footage	C	C	I
Armenian public acknowledgment of battlefield losses	C	C	C
Civilian exodus from contested territories	C	I	C
The collapse of Armenian defensive lines	C	I	I
Azerbaijani narrative dominance in international media	C	I	I
Armenian leadership messaging is inconsistent and reactive	C	I	C

(C = Consistent, I = Inconsistent, N/A = Not applicable)

Assessing the Second Nagorno-Karabakh War through observable behavioural and informational indicators suggests that information warfare and PSYOPs were the main causal factors weakening Armenian morale and decreasing the population's willingness to stay in the disputed territories (H1). Azerbaijani kinetic operations and technological superiority (H2) were enabling conditions, but they do not fully account for the scale and speed of the civilian exodus from the disputed areas. Organizational dysfunction (H3) is a plausible contributing factor, but, on its own, it is insufficient to explain the rapid departure of the Armenian population. Unlike the Russo-Georgian case, this conflict demonstrates a more advanced and coordinated use of non-kinetic effects alongside kinetic actions to achieve strategic objectives. This case highlights how behavioural and informational indicators can support real-time battlefield decision-making. It underscores the importance of inferential assessment in providing leaders with situational awareness of non-kinetic effects.

5. Discussion

These two cases illustrate the evolving use of non-kinetic effects in military operations. They demonstrate how kinetic operations can be enhanced with non-kinetic effects through a structured assessment approach. During

the Russo-Georgian War, effects were employed to exploit vulnerabilities, and assessments depended on technical and behavioural indicators, though these indicators offered limited confidence in establishing causal links for non-kinetic effects. The Second Nagorno-Karabakh War, 12 years later, showed a sophisticated integration of information warfare and PSYOPs with kinetic operations, with indicators monitored to support tactical decisions. In both examples, this analysis reveals that non-kinetic effects do not occur in isolation. These effects can influence, amplify, and improve military operations by shaping the information environment. The use of ACH provides a structured framework for evaluating effects, reducing cognitive bias, and using observable indicators to infer from change.

This analysis is subject to the following limitations and constraints. The limitations include limited access to classified processes and internal decision-making within the military forces in this study, and the indicators used are specific to this context and may not apply to conflicts in different cultural or political settings. The constraints are that these case studies are retrospective, rely on open-source and secondary reports, and there are only a limited number of well-documented historical examples of non-kinetic support to military operations.

This ACH framework provides a significant benefit to military leaders and planners by enhancing combat operations. The use of behavioural and informational indicators, along with confidence and uncertainty assignments, improves transparency in planning, executing, and assessing non-kinetic operations. It allows leaders to compare kinetic and non-kinetic courses of action using inferential logic. Future research should explore adapting ACH for planning large-scale deception operations and using human-AI teaming to develop competing hypotheses.

6. Conclusion

Military forces are increasingly equipped with non-kinetic assets on the battlefield, yet the ability to assess their effects has not kept pace. Non-kinetic effects are best used within a structured framework to ensure proper evaluation and synchronization with military operations. This paper set out to provide a tool that fills the gap between employing and assessing non-kinetic effects. The Analysis of Competing Hypotheses offers a much-needed, structured framework for assessing non-kinetic effects through observable behavioural and informational indicators, which is currently lacking in military intelligence and planning processes. The framework gives military commanders a rigorous tool for developing courses of action to plan and execute non-kinetic effects predictably, enabling military units to synchronize all capabilities.

Ethics Declaration: This research did not involve human participants or the collection of personal data and therefore did not require institutional ethical approval. The study is based on publicly available documents, doctrinal publications, and secondary sources.

AI Declaration: AI tools were used in a limited capacity to support the preparation of this paper, including language refinement, reference formatting, and clarity of expression. All substantive analysis, interpretation, and conclusions are the sole work of the authors, who take full responsibility for the content.

References

Aguirre, J., Fujiwara, J., Warren, K., López III, E., Lovell, S., Hodgson, Q., Johnson, N., and Roberts, J. (2024) *Scaling non-kinetic capability integration in the information age* (RAND Research Report RRA1934-1). Santa Monica, CA: RAND Corporation.

Chairman of the Joint Chiefs of Staff (2019) *CJCSI 3162.02: Methodology for combat assessment*. Washington, DC: U.S. Department of Defense.

Chincharadze, K. and Goodson, L.P. (2024) 'The enduring impact of the 2008 Russo-Georgian War', *War Room – U.S. Army War College*, 19 December.

Department of Defense (2016) *The Red Team handbook*. Washington, DC: Office of the Secretary of Defense.

Fortson, L.W. Jr. (2007) *Towards the development of a defensive cyber damage and mission impact methodology* (Technical Report ADA467549). Fort Belvoir, VA: Defense Technical Information Center.

Heuer, R.J. Jr. (1999) *Psychology of intelligence analysis*. Washington, DC: CIA Center for the Study of Intelligence.

Joint Chiefs of Staff (2018) *Joint Publication 3-12: Cyberspace operations*. Washington, DC: U.S. Department of Defense.

Joint Chiefs of Staff (2012) *Joint Publication 3-13: Information operations*. Washington, DC: U.S. Department of Defense.

Joint Chiefs of Staff (2003) *Joint Publication 3-53: Doctrine for joint psychological operations*. Washington, DC: U.S. Department of Defense.

Marinus (2021) *Information operations and maneuver warfare* (Maneuverist Paper No. 13). Quantico, VA: Marine Corps Gazette.

NATO (2015) *Allied joint doctrine for information operations (AJP-3.10)*. Brussels: North Atlantic Treaty Organization.

Paul, C., Yeats, J., Clarke, C.P., Matthews, M. and Skrabala, L. (2015) *Assessing and evaluating Department of Defense efforts to inform, influence, and persuade: Handbook for practitioners* (RAND Research Report RR-809/2). Santa Monica, CA: RAND Corporation.

Richardson, J.J. (2009) *A tradecraft primer: Structured analytic techniques for improving intelligence analysis*. Washington, DC: CIA Center for the Study of Intelligence.

Shakarian, P. (2011) 'The 2008 Russian cyber-campaign against Georgia', *Military Review*.

White, S.P. (2018) *Understanding cyberwarfare: Lessons from the Russia–Georgia war* (MWI Report). West Point, NY: Modern War Institute.

Valtorta, M., Dang, J., Goradia, H., Huang, J. and Huhns, M. (2005) 'Extending Heuer's analysis of competing hypotheses method to support complex decision analysis', *Proceedings of the International Conference on Intelligence Analysis*, February.