



Towards a Future Battlefield Forensics Framework: A NATO Action Research Case Study

**PRACTICE-ORIENTED
ARTICLE**

RIKKE MICHELLE RIETVELD 

SCANDINAVIAN
MILITARY STUDIES

ABSTRACT

This article examines the key challenges and requirements for achieving interoperability in NATO *battlefield forensics* – the application of scientific methods to collect, analyse, and disseminate information, intelligence and evidence in conflict zones, bridging military and civilian domains. The article presents findings from three empirical inputs: a scoping mission and doctrinal review, NATO exercises and experimentation, and stakeholder engagement through surveys, workshops, and conferences. Five cross-cutting themes were identified: conceptual ambiguity; capability shortfalls; fragmented legal frameworks; weak interagency cooperation; and shared future needs. The analysis demonstrates that interoperability in NATO battlefield forensics is constrained not only by technical gaps but also by doctrinal, legal, organisational and cultural barriers. The article concludes that progress depends on three priorities: institutionalising a staffed Technical Exploitation (TE) function and fit-for-purpose doctrine; harmonising legal frameworks for operational and judicial use; and building predictable civil-military pathways and competence. It also highlights the need to overcome cultural barriers, notably the legacy perception of TE as a narrow counter-IED tool and the tendency to *exercise blindness*: the assumption that exploitation processes will function automatically in crises.

CORRESPONDING AUTHOR:

Rikke Michelle Rietveld

NATO, DK

rikkerietveld@gmail.com

KEYWORDS:

battlefield forensics; military intelligence; interoperability; technical exploitation; action research; military culture

TO CITE THIS ARTICLE:

Rietveld, R. M. (2025). Towards a Future Battlefield Forensics Framework: A NATO Action Research Case Study. *Scandinavian Journal of Military Studies*, 8(1), pp. 451–465. DOI: <https://doi.org/10.31374/sjms.333>

NATO operations increasingly rely on the rapid collection and exploitation of material from the battlefield for intelligence, legal, and humanitarian purposes. Technical exploitation (TE), battlefield evidence (BE), biometrics, among other forensic practices, are now recognised as essential contributors to decision-making, accountability, and operational effectiveness. The war in Ukraine has further demonstrated the centrality of forensic practices for documenting war crimes, supporting accountability processes, and shaping strategic communication (Trev, 2022; UN, 2023). Yet despite this recognition, NATO doctrine and practice remain outdated and inconsistent, with concepts, capabilities, and legal frameworks varying widely across nations and organisations.

This article forms a part of a larger PhD research project entitled *The Past, Present and Future of Battlefield Forensics*. Whereas the overall project seeks to develop a comprehensive framework that integrates military, government, and civilian contributors (Figure 1), this article focuses specifically on the NATO case study and military perspective. The purpose is not to propose a finalised framework, but to examine the challenges and requirements for interoperability in battlefield forensics within NATO structures.

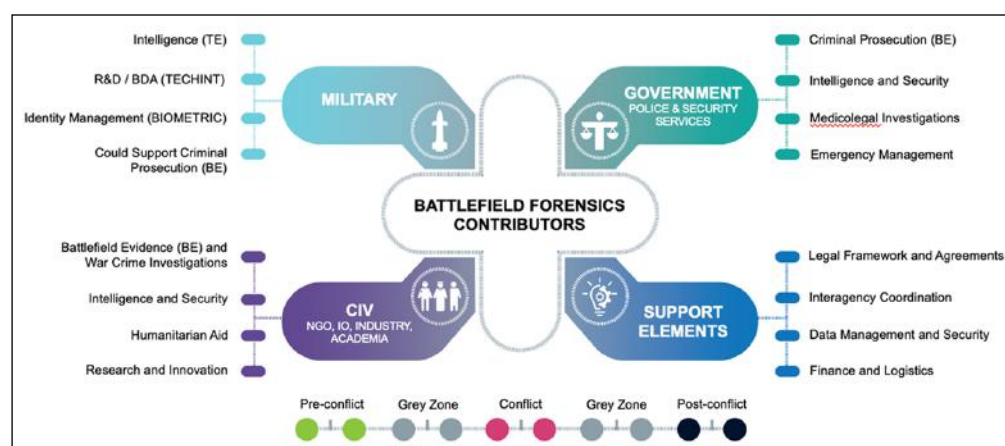


Figure 1 The Battlefield Forensics Framework (overall research project).

Note. Own work. This article focuses on the NATO/military dimension of the framework (Rietveld, 2025).

Hybrid warfare and grey-zone threats increasingly blur the boundary between conventional conflict, counterterrorism, and intelligence-led operations (Dobias & Christensen, 2022; Hoffman, 2007). In this context, battlefield forensics can no longer be understood solely as support to judicial processes but as a cross-domain capability that enhances resilience, situational awareness, and legitimacy (Borrell, 2023; MSB, 2025). The analysis also considers cultural and exercise-design factors that impede implementation in practice, foreshadowing issues I term *legacy bias* and *exercise blindness*; I discuss these below (for readers unfamiliar with NATO terminology, “Appendix 1 – Terms and Abbreviations”, below, defines key terms used throughout).

This paper’s guiding research question is: “What are the key challenges and requirements for achieving interoperability in NATO battlefield forensics?” To situate NATO’s current position, the next section reviews how battlefield and military forensics are defined and conceptualised in doctrine and scholarship.

STATE OF THE ART AND RESEARCH CHALLENGE

Despite the centrality of forensic practices in modern conflicts, battlefield forensics remains an underdeveloped field of study. While forensic science has a long tradition within civilian policing and judicial processes, its systematic integration into military operations is relatively recent. Early developments focused on the exploitation of improvised explosive devices (IEDs) in Afghanistan and Iraq, where NATO and coalition forces developed specialist technical exploitation units to gather intelligence and enhance force protection (Livingstone, 2008; Lorge, 2010). These practices gradually expanded beyond counter-IED (CIED) to encompass (among other things) biometrics, document exploitation, and the recovery of material from the battlefield more broadly. However, academic literature has largely overlooked this evolution. One of the few systematic attempts to map military forensics, undertaken by Lauren Wilson from an Australian perspective and Five Eyes context, underlined the lack of doctrinal clarity and limited engagement with civilian forensic science (Wilson, 2018).

Battlefield forensics can be understood as the adaptation of scientific methods to collect, analyse, and disseminate information, intelligence and evidence within crises or conflict zones. It encompasses both military forensics (technical exploitation, biometrics and battlefield evidence) and civilian forensics (e.g., contributions from government, academia, industry and non-governmental and international organisations). This multidisciplinary approach integrates forensic science disciplines to reconstruct events, identify combatants, and provide critical insights for military and civilian operations. By examining physical, digital and biometrical materials, battlefield forensics supports tactical, operational, and strategic decision-making, enhances operational security, and ensure accountability in conflict environments.

Military forensics is used here as an umbrella term for technical exploitation, battlefield evidence, and biometrics. It refers to the systematic collection, preservation, analysis and interpretation of collected exploitable material (CEM) removed during military operations (Figure 2). These materials can range from pocket litter to biometric data, electronic devices or weapon systems. The insight derived from military forensics can support commanders in making informed operational decisions, contribute to the identification of adversaries, and, under specific legal frameworks, feed into the judicial system (NATO, 2021b; Wilson et al., 2021).

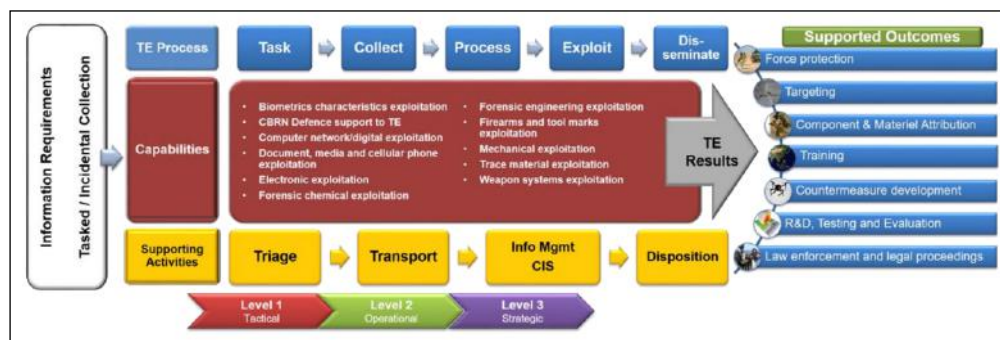


Figure 2 NATO's technical exploitation process, showing the different levels of exploitation, supporting activities, technical/forensic disciplines and supported outcomes (AIntP-10 Technical Exploitation Standard).

The civil-military divide represents a central challenge. Forensic science in its conventional form is orientated towards evidentiary standards and judicial procedures in a civilian context. Military forensics, by contrast, is often focused on immediate intelligence value and operational decision-making. This dual purpose creates both opportunities and friction. On the one hand, forensic expertise can significantly enhance situational awareness, targeting, and identity management on the battlefield. On the other hand, the military application of forensic techniques may not align with evidentiary requirements, creating uncertainty over whether materials collected in conflict zones can be used in judicial proceedings (Clegg, 2021; Wilson et al., 2021). Humanitarian perspectives reinforce this concern, emphasising obligations to ensure dignity in the treatment of the dead and preservation of material for accountability purposes (ICPM, 2019; ICRC, 2016).

While NATO doctrinal publications attempt to address these challenges, gaps remain. AIntP-10 (technical exploitation), AEODP-6 (reporting standards), and AJP-3.15 (counter-IED operations) provide a doctrinal framework for exploitation activities. Yet lessons identified, and experimentations from the NATO Technical Exploitation Group (NTEG) between 2021 and 2023, and Joint Analysis and Lessons Learned Centre (JALLC) in 2024, consistently emphasise doctrinal uncertainty, lack of integration with staff structures, and poor suitability of reporting formats for intelligence and evidentiary purposes (JALLC, 2024; NATO, 2021a; NTEG, 2022, 2023a). These observations suggest that while doctrine exists, it has not been fully operationalised to meet requirements of contemporary conflict.

The broader literature on interoperability provides useful insights to this problem. Studies of multinational operations highlight that interoperability is not only a technical matter of equipment compatibility; it is a social and organisational process that depends on shared doctrine, mutual trust, and aligned training (Derleth, 2015; Pinzariu et al., 2024; Sjøgren & Nilsson, 2025; Soeters & Goldenberg, 2019). These enablers are frequently absent in the forensic domain, where national caveats, different legal systems, and varying levels of technical capability undermine collective effectiveness. Battlefield forensics therefore reflects, in microcosm, the wider challenges of NATO interoperability.

Finally, a growing body of humanitarian and legal experts stress the importance of forensic practices in ensuring accountability and legitimacy. Organisations such as the International Committee of the Red Cross (ICRC), the International Commission of Missing Persons (ICMP), and the United Nations Investigative Team to Promote Accountability for Crimes Committed by Da'esh/ISIL (UNITAD) have emphasised the role of forensics in the identification of the dead, the treatment of remains, and the preservation of evidence of potential war crimes investigations (ICPM, 2019; ICRC, 2016; UN, 2023). These perspectives highlight that battlefield forensics is not only an operational enabler but also a humanitarian obligation. Integrating such considerations into military practice requires a multidisciplinary approach that aligns military forensics, civilian forensic science, and humanitarian law.

Beyond the practice literature, these issues connect to wider scholarly debates on military innovation, interoperability, and security governance. The incremental emergence of the Technical Exploitation function of the Joint Intelligence branch (J2E) and its Technical Exploitation Coordination Capability (TECC) through experimentation illustrates how change in complex military organisations often proceeds through practitioner-led adaptation rather than top-down reform. Interoperability in this domain is not only technical but socio-organisational, requiring aligned doctrine, training, and trust across national systems (Derleth, 2015; Pinzariu et al., 2024; Sjøgren & Nilsson, 2025; Soeters & Goldenberg, 2019). The civil-military interfaces discussed by humanitarian actors align with security governance perspectives that link operational effectiveness to legitimacy and accountability (Wilson et al., 2020a).

In sum, the state of the art reveals three key gaps. First, battlefield forensics remains conceptually ambiguous, with limited academic theorisation and vague doctrinal foundations. Second, its dual role across intelligence and legal domains has generated unresolved tensions between military and civilian practices. Third, interoperability challenges have been documented in related NATO domains but remain unexplored in forensic contexts.

This article addresses these challenges by analysing military forensics through an embedded case study of NATO, using empirical data from doctrine, exercises, and stakeholder engagement to identify the problem statements and requirements for interoperability within the broader battlefield forensics framework. Given these gaps, a methodological approach was required that could both establish under-researched areas and generate practical insights and recommendations in cooperation with practitioners.

ANALYTICAL APPROACH

The study employs a grounded theory (GT) approach combined with action research (AR; see Figure 3). GT is well-suited for under-researched domains such as battlefield forensics because it allows theory to emerge inductively from the data rather than being imposed a priori (Bryant et al., 2019; Charmaz, 2014; Flick et al., 2014). AR by contrast, embeds the researcher within practitioner communities and seeks to generate both practical outcomes and theoretical insights through cycles of observations, reflection, and intervention (Bryman, 2016).

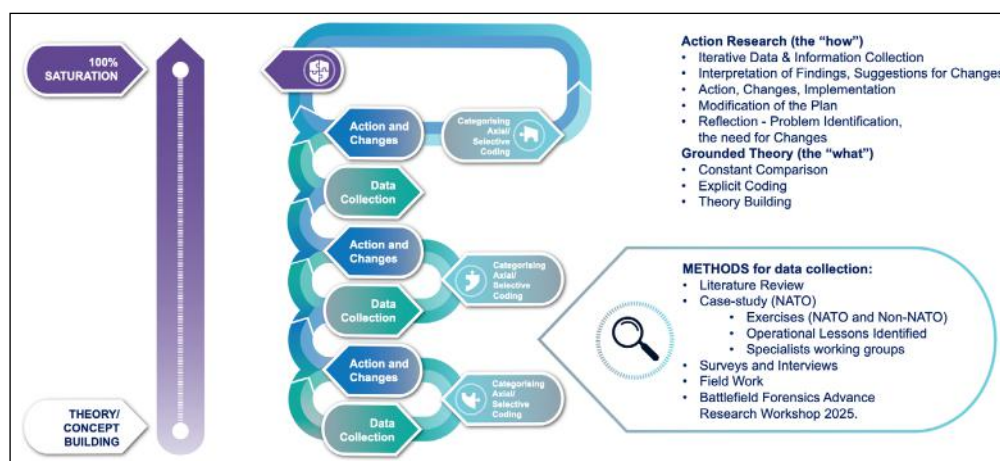


Figure 3 Mixed methodologies: Action Research and Grounded Theory.

Note. Own work. Data from exercises, stakeholder engagements, and field observations are analysed to generate recommendations, implemented, and re-assessed in iterative cycles (action research). In parallel, outputs are coded through constant comparison (open, axial, and selective coding) across datasets until thematic saturation, yielding concepts that inform theory building (grounded theory). The two cycles run concurrently so that practice improvement and theory development reinforce each other (Lingard et al., 2008).

Within the military domain, AR has been shown to enable innovation by linking research directly to operational practice, making it particularly relevant to NATO exercises and experimentation (Pumphrey, 2025). This dual approach is therefore especially suited to NATO operations, where interoperability is tested and adjusted through iterative cycles of planning, exercises, and evaluation. Combining AR and GT therefore permits both practice-informed change and theory-building in an under-researched domain.

Concepts of interoperability are drawn from the wider literature on coalition operations, which emphasises the importance of shared doctrine, mutual trust, and aligned training (Pinzariu et al., 2024; Soeters & Goldenberg, 2019). For battlefield forensics, interoperability is understood as the ability of NATO forces and partners to collect, exploit, and share forensic material in a consistent, legally robust, and operationally useful manner.

METHODS

The analysis is informed by the following three empirical inputs.

- 1. Scoping Mission and Doctrinal Review (Empirical Input 1).** A field mission to Erbil, Iraq in 2023 was conducted to interview humanitarian organisations and former military specialist. This was combined with analysis of NATO doctrines, and the 2021–2022 Martial Vision Subgroup (MMSG) Reports and the 2023 JALLC Report (JALLC, 2023; NATO, 2021a). These data provided an initial mapping of roles, challenges, and gaps in battlefield forensics.
- 2. NATO Exercises and Experimentation (Empirical Input 2).** Data were gathered from multiple NATO exercises and experimentation reports (Table 1), including Martial Vision 2022 and 2023 (NTEG, 2022, 2023a), the CBRN MERT Validation Experiments (NTEG, 2024), and an internal NATO TE Progress Report (Rietveld, 2025) based on the observation of TE in operational NATO headquarters at division (Multinational Division North (MNDN)) and corps level (Multinational Corps Northeast (MNCNE)). These sources provided evidence on how TE concepts and structures performed under both operational and simulated conditions.
- 3. Stakeholder Engagement (Empirical Input 3).** Engagement with practitioners was undertaken through semi-structured interviews, minutes of working group sessions, and surveys distributed via NATO and other expert networks such as ICRC and the Joint Deployable Exploitation and Analysis Laboratory (JDEAL). Survey responses (n~60) included both quantitative and qualitative data, complemented by expert statements from various conferences and working group meetings.

YEAR	EXERCISE/EVENT	HOST/LOCATION	FOCUS AREA	NOTES/DATA COLLECTED
2022	MV TE Experiment (MV22)	San Marcial Division HQ Spain	Tested TEF-2 (later TECC) concept	11 Vignettes incl. UAS, IEDs, maritime, CBRN, 50 Participants, 12 nations
2023	Ardent Defender 23 (AD23)	Canada	Counter Explosive Threat FTX	Evaluated TECC/TEG, reporting standards, 9 nations
2023	Bison Counter (BC23)	Germany	NATO C-IED LIVEX	Observed TE without TECC, 1000 participants, 12 nations
2023	Northern Challenge 23 (NC23)	Iceland	EOD/IEDD Multinational FTX	TECC Role in scenarios, 430 participants, 16 nations
2023	CBRN MERT Experiment – Toxic Valley 23 (TC23)	Slovakia	CBRN Exploitation	Level 1 CEM collection in CBRN-contaminated scenarios, 5 nations
2024	Trojan Footprint 24 (TF24)	NATO SOF Europe	SOF exploitation, CEM HOTO	Scripted SOF drills, tested CEM transfer to CIV authorities, identified cross-JOA sharing gaps
2024–2025	HQ Observations – Command Post Exercises (CPX)	MNCNE (Poland), MNDN (Latvia)	Operational Integration of TE on DIV and CORPS level	Observations, field notes, NATO reports, doctrinal review

Table 1 Summary of Exercises and Events from Which Empirical Data Were Drawn (Empirical Input 2).

CODING AND ANALYSIS

All three inputs were analysed using a systematic coding process combining open, axial, and selective coding (Table 2). Open coding was applied to identify descriptive concepts in the material (e.g., “terminology confusion”, “training shortfall”); axial coding was used to cluster these into higher-order categories (e.g., “Doctrine & Standards”, “Training & Awareness”); selective coding was used to integrate categories into cross-cutting themes (Charmaz, 2014; Flick et al., 2014). To ensure methodological transparency, coding was conducted iteratively, with categories refined through constant comparison between data sources (Bryman, 2016). Triangulation across the three empirical inputs increased the robustness of findings, consistent with best practice in qualitative research (Flick et al., 2014).

DATA SOURCE	EXAMPLE EVIDENCE	OPEN CODES	CATEGORIES	THEMES
Scoping Mission (Iraq 2023)	NATO/host-nation confusion over BE vs TE definitions	Terminology confusion	Doctrine & Standards	Conceptual clarity
NATO Exercises and Experimentation (2022–2025)	TECC improved outcomes but lacked SOPs and supporting doctrine	Undefined SOPs and outdated doctrines	Coordination and Command	Interagency cooperation
Surveys and Interviews	Most nations only at level 1 TE; civilian labs provide Level 2/3	Capability shortfall	Capability Gaps	Capability Development
Conferences and Working Groups	Legal advisor stressed need for biometric compliance	Legal risk	Legal Frameworks	Legal harmonisation

Table 2 Example of Coding Process Across Empirical Inputs.

The dataset displays limitations in that several observed exercises rehearsed only parts of the exploitation chain – focusing on collection, for example, with the assumption that transport, analysis, legal permissions, and dissemination would function automatically in practice. This pattern, described here as “exercise blindness”, reflects the current NATO exercise design and is therefore itself an important finding, examined in the Discussion section below.

The article will now present the findings, focusing on five themes that emerged consistently across the datasets.

FINDINGS

To connect the empirical results to wider scholarship, each theme is interpreted considering established work on coalition interoperability, military innovation, and security governance. Each theme is further illustrated with convergent evidence from exercises, documents and stakeholder input.

CONCEPTUAL CLARITY AND DEFINITIONS

NATO currently lacks a coherent conceptual foundation for battlefield forensics. Scoping interviews revealed that terms such as “battlefield evidence”, “technical exploitation”, and “battlefield forensics” were used interchangeably, creating confusion for practitioners and stakeholders. In the surveys many respondents explicitly wrote that “forensics” was confusing in a military context – some preferred “battlefield investigations”, others “technical exploitation”. In the Iraq scoping mission, a humanitarian NGO described NATO’s “overlapping use of BE, TE and BF” as unclear, especially when dealing with host-nations partners. In the Martial Vision 2023 report (NTEG, 2023a) doctrinal uncertainty was highlighted repeatedly. TECC was sometimes labelled “TEF-2”, other times “J2E”; CEM, meanwhile, was inconsistently defined. As one NATO practitioner observed during the surveys, “Forensics in its legal sense is different from how we use it in operations – we keep changing the terms.”

Exercise data reinforced this confusion, with Martial Vision 2023 reporting inconsistent classification of CBRN materials as CEM. In the CBRN MERT Validation Experiment 2023, national teams differed in whether they logged contaminated samples as “CEM” or retained them solely under CBRN protocols, underscoring the lack of clarity in NATO doctrine (NTEG, 2024).

The literature reinforces this ambiguity: Livingstone (2008) described battlefield forensics as the “rebirth of an ancient science,” pointing to its historical roots in documenting battlefield artefacts while noting that modern practice remains ill-defined. He emphasises that while militaries have always gathered material from the battlefield, the modern re-emergence of battlefield forensics largely through counter IED operations and weapons technical intelligence (WTI) has left it unevenly conceptual and applied. Wilson and her colleagues (2019) further emphasised the lack of clarity in NATO doctrine over whether military forensics is primarily intended to generate intelligence or admissible evidence, a doctrinal tension still evident in practice. This variation also links to the legacy bias discussed later.

This pattern reflects a well-documented problem in coalitions: when terminology and doctrinal intent are not shared, interoperability and evidentiary value both suffer (Sjögren & Nilsson, 2025; Wilson et al., 2020a). A single, NATO-wide definition of battlefield forensics, and consistent use of TE, BE and CEM, is prerequisite for interoperability.

CAPABILITY GAPS

The second theme relates to persistent gaps in NATO’s exploitation capabilities. NATO itself has no standing TE capability. Instead, it relies entirely on national contributions declared through Force Element Lists (FELs). If a member nation does not prioritise exploitation, NATO has little or no access to deployable capabilities. As a result, the quality and availability of TE support vary greatly across operations, from nations able to provide fully equipped teams and labs to others contributing nothing.

Surveys confirmed that most nations remain limited to Level 1 collection (to some extent), often outsourcing Level 2/3 analysis to national civilian laboratories (JALLC, 2024; Wilson, 2018). As one survey respondent from the NATO working group network noted, “We only do Level 1 – anything more goes straight to our national lab at home”. Field notes from the Iraq scoping mission also described exploitation as “improvised and inconsistent between contingents”, leaving commanders with uneven outputs (Rietveld, 2025).

Exercises reinforced these findings. Many units lacked Level 1 training, with contamination risk observed in the CBRN MERT experiment or lack of an exploitation process as observed at the division and corps level exercises. The technical exploitation coordination capability (TECC) was first tested during the MVSG experiments (NTEG, 2022, 2023). It is a scalable intelligence embedded function for coordination, standardised reporting and routing outputs to the commander’s information requirements (Figure 4). The MV22 report concluded that “without a central coordination node, exploitation activities remained stovepiped and failed to inform the commander’s priorities”. Similarly, MV23 noted that where no TECC was present, “exploitation reporting was fragmented and often bypassed the J2 structure entirely”. In contrast, when a TECC was established (e.g., during Ardent Defender 2023 and Northern Challenge 2023), interoperability and information-sharing improved markedly. The TECC Concept of Employment working document (NTEG, 2023b) formalises this role, describing TECC as the central node for tasking, coordination, and dissemination.

In line with the interoperability literature, uneven capability and non-standardised training are classic barriers to coalition performance, practitioner-led mechanisms and such as TECC translate experimental learning into institutional design (Casino et al., 2022; Derleth, 2015; Pinzari et al., 2024).

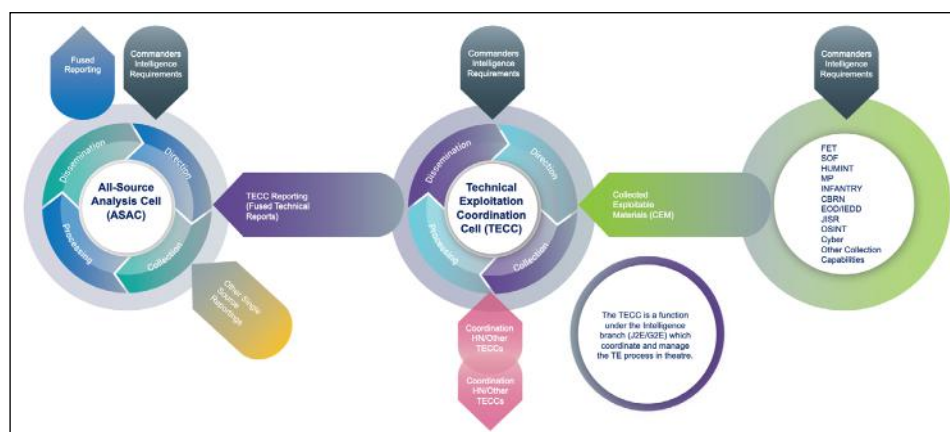


Figure 4 Military forensics intelligence cycle with TECC coordination.

Note. Own work. Collected exploitable material (CEM) may be recovered deliberately or incidentally by specialists or non-specialists. When routed via the technical exploitation coordination capability (TECC), technical outputs are validated, standardised, and translated into actionable intelligence, fused with other sources through the all-source analysis cell (ASAC), and disseminated to the wider community. The TECC also coordinates lateral exchange with other joint areas of operations and host-nation points of contact to optimise exploitation and the re-use of results (Rietveld, 2025).

Legal fragmentation emerged as a third theme. The absence of formal Status of Forces Agreement (SOFAs) and memoranda of agreement (MoAs) with host-nations was repeatedly flagged in exercises and reporting.

In the MNCNE and MNDN context, the TE Progress Report from the series of command post exercise and real-life observations, concluded that “limited interagency and Host-nation coordination frameworks, making collaboration and information-sharing inefficient” and “the absence of a legal framework to support TE and BE activities causes uncertainty in its application, particularly in multinational operations” (Rietveld, 2025). The consequences are inconsistent, limited, and outdated intelligence, with the risk of leaving commander’s less prepared on the battlefield or losing critical evidence for prosecution purposes.

The doctrinal gap also undermines evidentiary practice. MV23 observed that “AEODP-6, while adequate for EOD, is not fit for purpose as a reporting format for broader technical exploitation”, and concluded that without dedicated TE reporting templates, intelligence was inconsistent and failed to reach the commander’s intelligence cycle” (NTEG, 2023a).

Together, the After-Action Review from the ICRC Military Personnel Identification Project concluded that “each National Support Element in multinational operations handles its own recovery and identification processes,” adding that “no common NATO framework exists at Corps/Division level” (Rietveld, 2024). The consequences are uneven and outdated procedures for recovery, identification and repatriation of fallen soldiers, leaving legal authority inconsistent and dependent on national caveats.

International humanitarian law (IHL) and international human rights law (IHRL) obligations further complicate NATO practice. Ukraine’s Ministry of Defence voluntary IHL report confirms the duty to “search for, collect, and evacuate the bodies of the deceased from both sides of the conflict” and stipulates that “biometric data shall be collected and preserved, but only under procedures that ensure dignity, privacy, and compliance with human rights obligations”. It also emphasises that “families of the deceased must be informed, and identification must be pursued as a legal and humanitarian duty” (MoD Ukraine, 2024).

War-crimes and accountability processes magnify these challenges. A recent Ukrainian legal analytical review found that “the Prosecutor General’s Office relies on initial collection and preservation by defence forces in the field; admissibility depends on chain of custody established at the moment of recovery” (MoD Ukraine Legal Review, 2024). UNITAD has shown similar reliance in Iraq, where forensic recovery by defence forces fed directly into international accountability mechanisms (UN, 2023). Wilson and her colleagues (2021) document a successful prosecution built on extraterritorial battlefield evidence, though only under very specific national conditions. Clegg (2021) adds that dignity of the dead is itself a humanitarian obligation, not merely a technical matter.

Emerging technologies add another layer of complexity. As Wells (2025) warns, “AI-enabled forensic tools can enhance collection and analysis of battlefield evidence, but without procedural safeguards and admissibility standards, such evidence risks exclusion from judicial proceedings.”

Taken together, the legal challenge is twofold. First, external instruments such as SOFAs and MoAs, are often absent, limiting authority to collect and share; second, internal instruments, including reporting doctrine and staff SOPs, remain unsuited for intelligence and evidentiary standards. Where these were absent, exercises documented inconsistent reporting and limited value; where piloted (for example TECC/J2E), outputs more readily supported both operational and judicial ends.

These findings reinforce security-governance perspectives: effective and legitimate practice depends on agreed legal authorities, chain of custody procedures, and admissibility standards across jurisdictions (Clegg, 2021; Wells, 2025; Wilson et al., 2021).

INTERAGENCY COOPERATION

The fourth theme concerns cooperation between military and civilian actors. Across experiments, events and working groups, cooperation remained poorly integrated and often contingent on national and ad-hoc arrangements rather than a standing NATO mechanism.

The MNDN After-Action Review report records that each NSE conducts its own identification processes and must establish agreements with Host-nations, leaving corps/division HQs without a unified framework to exchange information on remains, biometrics, or evidentiary material. This produces inconsistent practices and delays when multiple nations operate in the same area of operations (Rietveld, 2024).

Exercises corroborated that staff integration is decisive. MV23 found that where a TECC/J2E function was not established, exploitation reporting tended to remain within unit stovepipes; conversely, with TECC/J2E, coordination improved and enabled engagement with external actors (NTEG, 2023a).

Several nations also indicated that they only possess Level 1 Exploitation and depend on civilian support for higher level analysis (e.g., biometrics/DNA, complex materials characterisation) – drawing on national laboratories, universities, and industry partners for equipment, techniques, and training. This reliance is visible in allied training pipelines, too, where multinational exploitation education is provided via programmes such as the EDA supported Joint Deployable Exploitation and Analysis Laboratory (JDEAL) and the NATO accredited C-IED Centre of Excellence, which pools expertise and resources across nations for deployable exploitation laboratories and training.

Practitioner literature aligns with these observations. Cobham et al. (2022) argue that integrating humanitarian action with humanitarian forensic action requires “structured partnerships”, not ad hoc arrangements – a lesson directly applicable to NATO exploitation chains that must connect military collection to civilian medico-legal systems. The Swedish Civil Contingencies Agency (MSB, 2025) emphasises that interagency collaboration mechanisms used for national civil defence are “dual use”, underpinning response to conflict, terrorism, and large-scale disasters alike. The same civil-military pathways enable response in disaster and mass-casualty events, increasing dual-use value without new structures.

This converges with studies of multinational information sharing, which show that trust, clear roles, and routinized interfaces are fundamental for effective cooperation (Cobham et al., 2022; Sjøgren & Nilsson, 2025; Soeters & Manigart, 2009).

NATO has acknowledged the gap at policy level through the “Battlefield Evidence Policy” to guide cooperation with law-enforcement and judicial authorities (NATO, 2020); however, multiple observations and surveys note that policy has not yet translated into routine practice at operational and tactical headquarters without a coordinating staff function.

Taken together, the evidence indicates that cooperation improves where a coordinating function exists and formal pathways to civilian partners are established; where these are absent, military forensics remains stovepiped. This leads directly to the “future needs” indicated below.

FUTURE NEEDS AND RECOMMENDATIONS

The fifth theme concerns future needs. To sharpen focus, three priority areas emerged across all data sources and map directly to the four preceding themes above.

Priority 1 is to institutionalise TE as a staffed function and update doctrine and reporting. This includes embedding TECC/J2E at tactical, operational and strategic levels, and publishing TE-specific reporting standards. It also requires aligning TE with adjacent doctrines and processes, such as CBRN, JISR, Stability Policing and C-IED, so exploitation outputs routinely inform the commander’s information requirements.

Priority 2 is to harmonise legal frameworks and protections. This involves concluding SOFAs and MoAs with host-nations prior to deployment and adopting NATO-consistent chain of custody, biometrics and data protection procedures to ensure collected material retains operational utility and where appropriate, evidentiary admissibility across jurisdictions.

Priority 3 is to build predictable civil-military pathways and competency by codifying Level-1/2 training and interfaces to Level-2/3 laboratories, formalising partnerships with national labs, universities, and industry, and designing exercises that rehearse the full end-to-end exploitation chain to overcome exercise blindness. These priorities also reveal deeper cultural and doctrinal issues, addressed explicitly in the Discussion section below.

Several changes are already in motion as a direct outcome of the experimentation and working-group cycles documented in this study. The first is NATO's *Capability Codes and Capability Statements* (CC & CS): the NTEG is working on including TE as its own collection capability (LVL-1) and moving away from an exclusive C-IED orientation towards dedicated technical exploitation entries, with proposals to recognise TE Level 1 as a distinct deployable capability and to re-designate the former C-IED Level 2 laboratory as a more general EXPL Level 2 laboratory that can handle the full range of CEM. This change will impact nations' agreed contributions to NATO's Force Element Lists (the agreed force matrix of employed capabilities) for operational planning and exercises. If the TE capabilities are expected to be present in theatre, commanders and nations must include them in the planning process (Rietveld, 2025).

The second is NATO reporting. The MVSG is trialling a TE messaging and reporting requirements standard (Canada acting as custodian) prior to submission for formal standardisation (NTEG, 2023a).

The third is NATO doctrine. Inputs have been given to update NATO's Allied Joint Publication Intelligence, Counter-Intelligence and Security (AJP-2 Edition C, Version1), so that TE is recognised as a collection capability and CEM is treated as an intelligence discipline (CEMINT), aligning exploitation outputs with the JISR cycle (Rietveld, 2025).

The fourth concerns NATO training. Two specialised courses are currently being developed and tested – the TE Awareness Course and the TE Staff Officer Course, both developed to give staff a better understanding of the TE process and the value of CEM.

The fifth, finally, concerns concept of employment. The TECC CONEMP (planned update to current TE doctrine) clarifies that Level 2 exploitation can be positioned closer to the tactical fight (e.g., division level) for Article 5 scenarios and that TECC is a scalable staff function that can be employed at multiple levels to coordinate tasking, laboratory throughput and dissemination (NTEG, 2023a).

DISCUSSION

This section discusses each finding in turn, considering implications for the three priorities above. It should be noted immediately that the findings show interoperability in NATO battlefield forensics to be hindered by conceptual, structural, legal, organisational and cultural barriers. Addressing the research question, five interlinked challenges and requirements emerge.

First, conceptual clarity is a precondition for effective interoperability. Without a unified definition, NATO risks continuing confusion between intelligence and legal functions. Wilson and her colleagues (Wilson et al., 2020b) noted that doctrinal uncertainty over whether exploitation should serve intelligence or evidentiary purposes has long undermined coherence, while Livingstone (2008) described battlefield forensics as a “rebirth” rather than a consolidated discipline. As the wider interoperability literature shows, the absence of shared terminology undermines coalition effectiveness (Sjögren & Nilsson, 2025; Soeters & Goldenberg, 2019). For battlefield forensics, this doctrinal uncertainty directly affects operational practice and evidentiary value.

Second, capability gaps constrain NATO's ability to exploit material effectively. Uneven availability of Level 1–3 capabilities mirrors wider interoperability challenges documented across NATO operations (NTEG, 2023a). Exercises confirmed that improvisation and ad hoc arrangements remain common. Similar concerns are visible in the digital domain: Casino et al. (2022) highlight how technical gaps in digital forensics risk undermining reliability and interoperability of outputs. Institutionalising a multi-level exploitation system with standard training is essential.

Third, legal fragmentation remains a critical obstacle. Divergent national frameworks and a lack of NATO-wide doctrine on battlefield evidence produce friction between operational imperatives and judicial requirements. Wilson et al. (2021) provide a single example where battlefield evidence supported a prosecution – but only under specific national conditions, illustrating the inconsistency across jurisdictions. Clegg (2021) underscores the humanitarian and ethical obligation to safeguard the dead of war, while UNITAD (UN, 2023) demonstrate that forensic recovery has become central to accountability for mass atrocities. The Ukraine Voluntary IHL Report (MoD Ukraine, 2024) reinforces that parties must “search for, collect,

and evacuate the bodies of deceased from both sides of conflict”, and handle biometrics with dignity and human rights in mind. Wells (2025) further warns that AI-enabled exploitation will compound admissibility challenges without updated safeguards.

Fourth, interagency cooperation is underdeveloped. Current collaborations are lacking coherence and depend on individual networks rather than institutional mechanisms. NATO has acknowledged this gap through its Battlefield Evidence Policy (NATO, 2020), but practice lags behind. Cobham et al. (2022) argue that integrating humanitarian mine action with forensic action requires structured partnerships, a lesson equally relevant to NATO exploitation. The Swedish Civil Contingencies Agency (MSB, 2025) similarly emphasise that interagency collaboration is central to resilience, whether in conflict, terrorism, or disasters. A structured and binding framework is needed to connect military collection to civilian forensic and legal systems.

Finally, the emphasis on future needs reflects a shared recognition of what is required. Standardised training, harmonised doctrine, clear command and control (C2) and integration of ethical considerations all align with scholarship on sustaining interoperability (Derleth, 2015; Pinzariu et al., 2024). The practical outputs already introduced – TECC concept, J2E staff functions, revised reporting doctrine, update of capability codes, and new training initiatives – show that NATO can adapt doctrine through experimentation and iteration (NATO Allied Command Transformation, 2024). Yet these remain partial steps. Comprehensive interoperability will require legal harmonisation, structured interagency frameworks, and integration of civilian forensic expertise.

Taken together, these findings contribute to broader debates on how militaries innovate and achieve interoperability. The introduction of TECC/J2E illustrates bottom-up innovation via exercises and experimentation, consistent with scholarship on organisational adaptation in defence institutions. The requirement to coordinate across military, government, and humanitarian actors reflects a security-governance logic in which effectiveness and legitimacy depend on integrating diverse capabilities within shared procedures and standards (Derleth, 2015; Pinzariu et al., 2024; Wilson, 2018).

Two cultural barriers to adoption emerged. The first is legacy bias – the association of TE almost exclusively with C-IED operations in Afghanistan and Iraq. This framing persists in current doctrines (AIntP-10 and AEODP-6), reinforcing the perception that exploitation is optional and obsolete outside C-IED contexts. The second is exercise blindness, where staff at the higher tactical and operational levels are accustomed to receiving scripted intelligence products and therefore neglect to rehearse and implement the TE process that generates them. The TE Progress Report (Rietveld, 2025) observed that host-nations agreements are often assumed rather than rehearsed. JALLC (2024), cautioned that neglecting exploitation in this way creates “significant operational vulnerabilities”. Overcoming these cultural barriers requires awareness training, staff integration, and doctrinal reform that present exploitation as a routine enabler of intelligence, security and accountability. When implemented correctly, TE adds value across all levels of war.

The changes outlined above illustrate how AR can accelerate alliance learning by linking experimentation, doctrinal drafting and capability planning. In line with research on multinational interoperability and mission command, the introduction of a TECC staff function, rebalanced Level 1–2–3 pathways, and a fit-for-purpose doctrine act as coordination mechanisms that reduce transaction costs between nations and echelons (Pumphrey, 2025; Soeters & Goldenberg, 2019). They also create governance infrastructure that security-studies scholars associate with durable interoperability: clear roles, common language, and routines exchanged across organisational boundaries (Sjögren & Nilsson, 2025; Soeters & Manigart, 2009). In this case, TE ceases to be an ad hoc legacy-framed activity, becoming instead an integrated intelligence contributor that can be tasked, resourced, and held to account.

Together, these findings indicate that achieving interoperability in battlefield forensics requires more than technical solutions. To implement this capability across all levels of operations demands conceptual coherence, institutional investments, legal clarity, cultural change, and collaborative innovation across military, governmental, and civilian domains.

CONCLUSION

This article examined the question “What are the key challenges and requirements for achieving interoperability in NATO Battlefield Forensics?” Based on three empirical inputs – scoping mission and doctrinal review, NATO and allied exercises and experimentation, and stakeholder engagement – five overarching themes were identified: conceptual ambiguity, capability gaps, fragmented legal frameworks, weak interagency cooperation, and shared future needs.

The analysis shows that NATO battlefield forensics is constrained not only by technical gaps but also by doctrinal, legal, organisational, and cultural barriers. Addressing these requires NATO to:

- Establish a unified concept of battlefield forensics, reconciling intelligence and evidentiary purposes.
- Institutionalise a multi-level exploitation system with standard training.
- Harmonise legal frameworks to ensure operational and evidentiary utility.
- Build structured interagency mechanisms linking military, civilian, and humanitarian actors.
- Integrate ethical and humanitarian considerations into doctrine and practise.

The analysis also demonstrates that change is already underway. NATO’s MVSG has produced innovations such as the TECC concept, dedicated staff functions (J2E roles), capability codes refinement, a new reporting standard, and designs for new training courses (Rietveld, 2025). A revision of AIntP-10 is scheduled for 2026, making exploitation doctrine more comprehensive and aligned with modern warfare. These concrete adjustments demonstrates that bottom-up innovation is taking hold; the remaining gap is sustained senior-level direction.

Yet progress will remain limited unless cultural barriers are also addressed. NATO must overcome the legacy bias perception that TE is merely an expeditionary C-IED tool and confront exercise blindness, whereby scripted intelligence products are accepted without rehearsing the processes, legal permissions, and coordination mechanisms required to produce them. These biases perpetuate under-investment and minimise exploitation’s potential as a function of a fully integrated intelligence discipline in modern warfare.

Sustained leadership and top-down endorsement are now required to normalise TE as an intelligence capability, resource changes, and signal battlefield forensics to be a core NATO responsibility rather than a niche, expeditionary adjunct.

APPENDIX 1 – TERMS AND ABBREVIATIONS

This annex provides definitions of key NATO technical terms and abbreviations used in the article (Ref: AJP-2.7 and AIntP-10).

TERM/ABBREVIATION	DEFINITION
AEODP-6	Allied Explosive Ordnance Disposal Publication 6: A NATO reporting standard designed for EOD that is also applied to TE reporting.
Battlefield evidence (BE)	Material collected during military operations that is intended for use in judicial proceedings.
Battlefield forensics (BF)	Battlefield forensics is the application of scientific methods to collect, analyse, and disseminate information, intelligence, and evidence within crisis or conflict zones. It encompasses both military forensics (e.g., technical exploitation) and civilian forensics (e.g., contributions from government, academia, industry, and NGOs/IOs). This multidisciplinary approach integrates forensic science principles to reconstruct events, identify combatants, and provide critical insights for military and civilian operations. By examining physical, digital, and biological materials, battlefield forensics supports tactical, operational and strategic decision-making, enhances operational security, and ensures accountability in conflict environments.
Civilian forensics	Forensic activities conducted by non-military actors, such as government medico-legal systems and law-enforcement, national laboratories, academia, industry, and NGOs/IOs, that support identification of the deceased, war-crimes investigations, disaster victim identification (DVI), digital/media analysis etc. Civilian forensics provides surge capacity and legal admissibility pathways, and interfaces with military collection through agreed procedures and standards.

(Contd.)

TERM/ABBREVIATION	DEFINITION
Collected exploitable material (CEM)	Items recovered from the battlefield (e.g., weapons, electronics, documents, biometrics) that can be exploited for intelligence or evidentiary purposes.
Exercise blindness	A tendency during exercises to validate scripted intelligence products without rehearsing and implementing the full end-to-end exploitations (collection, analysis, legal permissions, dissemination coordination). Authors definition.
Five Eyes	The Five Eyes is an intelligence alliance composed of Australia, Canada, New Zealand, the United Kingdom and the United States
Forensic science	Forensic science is defined as the application of scientific principles and techniques to matters of criminal justice especially relating to the collection, examination, and analysis of physical evidence (Merriam-Webster).
Joint intelligence, surveillance, and reconnaissance (JISR)	JISR is an integrated intelligence and operations set of capabilities, which synchronises and integrates the planning and operations of all collection capabilities with processing, exploitation, and dissemination of the resulting information in direct support of the planning, preparation, and execution of operations. TE is a component to the JISR process of the intelligence cycle.
Legacy bias	The cultural perception that TE is primarily an expeditionary counter-IED function (rooted in Afghanistan/Iraq experience), which limits its wider adoption as a routine intelligence and forensic capability. Authors definition.
Level 1/2/3 Exploitation	NATO's tiered exploitation structure: Level 1 – Tactical collection and initial screening at the point of capture. Level 2 – Advanced analysis (DNA, biometrics, electronics) in deployable or national laboratories. Level 3 – Specialist national or strategic laboratories with full forensic capabilities.
Military forensics	An umbrella term for technical exploitation (TE), battlefield evidence (BE), and biometrics focusing on the collection and exploitation of material in conflict environments to support intelligence, operations, and judicial processes.
MoA (Memoranda of Agreement)	Bilateral or multilateral agreements that establish operational and legal arrangements for cooperation in evidence collection and sharing.
SOFA (Status of Forces Agreement)	A legal framework between NATO/nations and Host-nations defining rights and responsibilities of deployed forces.
Martial Vision Subgroup	Martial Vision Subgroup (MVSG) is a Flagship Activity of the NATO Technical Exploitation Group (NTEG). MVSG aims to identify and pursue opportunities for testing and/or validating concepts, doctrine, and operational standards in NATO and/or national exercises and experimentation.
TE process	The TE process parallels the JISR process with a focus on the processing and exploitation steps. TE results fused with JISR results contribute to the development of intelligence products that define the operating environment (OE) and support the commander's decision-making process on all levels.
Technical exploitation (TE)	The process of using scientific methods and tools to derive data and information from potential intelligence or operational value from collected data, information, materiel, and materials.
Technical Exploitation Coordination Capability (TECC)	A scalable staff function, embedded in J2 (intelligence), responsible for coordinating TE contributions, fuse technical reporting, and disseminating exploitation outputs.

DATA ACCESSIBILITY STATEMENT

The data that support the finding of this study are available on request from the corresponding author (RMR). Some data are not publicly available due to restrictions – for example, where they contain information that could compromise the privacy of research participants and/or consist of NATO or national classified documents.

ACKNOWLEDGEMENTS

The author would like to thank colleagues and leadership in NATO and partner nations, Danish Defence, Cranfield University at United Kingdom Defence Academy, MNCNE and MNDN, and specialists from civilian organisations for their valuable discussions and insights.

Special thanks are extended to the survey respondents, interviewees, and the MVSG, who generously shared their expertise.

For the purposes of open access, the author has applied a Creative Commons Attribution (CC BY) licence to any Accepted Author Manuscript version arising from this submission.

FUNDING INFORMATION

This work was supported by the NATO Defence Against Terrorism Programme of Work (DAT POW), Cranfield University and Danish Defence.

COMPETING INTERESTS

No potential conflict of interest was reported by the author. All views expressed are those of the author and do not necessarily represent the official position of NATO, Danish Defence or Cranfield University.

AUTHOR AFFILIATIONS

Rikke Michelle Rietveld  orcid.org/0009-0002-0006-9713
NATO, DK

REFERENCES

- Borrell, J. (2023, May 29). *Lessons from the war in Ukraine for the future of EU defence*|EEAS. European External Action Service. https://www.eeas.europa.eu/eeas/lessons-war-ukraine-future-eu-defence_en
- Bryant, A., Charmaz, K., & Clarke, A. E. (2019). Situating Grounded Theory and Situational Analysis in Interpretive Qualitative Inquiry. *The SAGE Handbook of Current Developments in Grounded Theory*, 3–48. <https://doi.org/10.4135/9781526485656>
- Bryman, A. (2016). *Social Research Methods* (5th ed.). Oxford University Press.
- Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M., & Patsakis, C. (2022). Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews. *IEEE Access*, 10, 25464–25493. <https://doi.org/10.1109/ACCESS.2022.3154059>
- Charmaz, K. (2014). *Constructing Grounded Theory* (2nd ed.). SAGE.
- Clegg, L. (2021). The International Committee of the Red Cross and the protection of world war dead. *Forensic Science International*, 319. <https://doi.org/10.1016/j.forsciint.2020.110648>
- Cobham, L., Márquez-Grant, N., Harris, M., Barker, C., Medina, C. S., Naranjo-Santana, J., & Collett, G. (2022). Integrating Humanitarian Mine Action and Humanitarian Forensic Action. *The Journal of Conventional Weapons Destruction*, 25(3). <https://commons.lib.jmu.edu/cisr-journal/vol25/iss3/5>
- Derleth, J. (2015). NATO Review – Enhancing interoperability: the foundation for effective NATO operations. <https://www.nato.int/docu/review/articles/2015/06/16/enhancing-interoperability-the-foundation-for-effective-nato-operations/index.html>
- Dobias, P., & Christensen, K. (2022). The ‘Grey Zone’ and Hybrid Activities. *The Quarterly Journal*, 21, 41–54. <https://doi.org/10.11610/Connections.21.2.03>
- Flick, U., Thornberg, R., & Charmaz, K. (2014). Grounded Theory and Theoretical Coding. *The SAGE Handbook of Qualitative Data Analysis*, 153–169. <https://doi.org/10.4135/9781446282243>
- Hoffman, F. G. (2007). *The Rise of Hybrid Wars*. <http://www.potomac-institute.org/>
- ICPM. (2019). ICMP AGREEMENT: AN OVERVIEW – International Commission on Missing Persons. <https://icmp.int/news/icmp-framework-agreement-an-overview/>
- ICRC. (2016). ADVISORY SERVICE ON INTERNATIONAL HUMANITARIAN LAW *Humanity after Life: Respecting and Protecting the Dead*. <https://ihl-databases.icrc.org/ihl/full/GCI->
- JALLC. (2023). JALLC Publishes factsheet on its report covering Technical Exploitation and Battlefield Evidence: JALLC – NATO. <https://www.jallc.nato.int/articles/jallc-publishes-factsheet-its-report-covering-technical-exploitation-and-battlefield-evidence>
- JALLC. (2024). NATO UNCLASSIFIED TECHNICAL EXPLOITATION AND BATTLEFIELD EVIDENCE EXECUTIVE SUMMARY. www.jallc.nato.int
- Lingard, L., Albert, M., & Levinson, W. (2008). Grounded theory, mixed methods, and action research. *BMJ*, 337(7667), 459–461. <https://doi.org/10.1136/BMJ.39602.690162.47>
- Livingstone, C. N. (2008). *Battlefield Forensics: Rebirth of an Ancient Science – Domestic Preparedness*. Domestic Preparedness. <https://domprep.com/commentary/battlefield-forensics-rebirth-of-an-ancient-science>

- Large, E.** (2010, May 17). *Shining light on battlefield forensics*[Article/The United States Army. https://www.army.mil/article/39956/shining_light_on_battlefield_forensics
- MoD Ukraine.** (2024). *Voluntary report on implementation of international humanitarian law.*
- MoD Ukraine Legal Review.** (2024). *Legal aspects of the armed aggression of the Russian Federation against Ukraine* Legal Department of the Ministry of Defence of Ukraine.
- MSB.** (2025). *Developing Sweden's Civil Defence: Lessons from Ukraine.* Swedish Civil Contingencies Agency.
- NATO.** (2020, October). *NATO Allies agree Policy on Battlefield Evidence from operational theatres to boost efforts against terrorism.* NATO NEWSROOM. https://www.nato.int/cps/en/natohq/news_179194.htm
- NATO.** (2021a). *MARTIAL VISION 2021 Technical Exploitation Seminar Lessons Identified Report.*
- NATO.** (2021b). *TECHNICAL EXPLOITATION – AIntP-10 EDITION B (TECHNICAL EXPLOITATION – AIntP-10 EDITION B).*
- NATO Allied Command Transformation.** (2024, March 14). *Advancing Readiness: A Recap of NATO's LOYAL LEDA 2024 Exercise – NATO's ACT.* <https://www.act.nato.int/article/advancing-readiness-recap-of-loyal-leda-2024/>
- NTEG.** (2022). *MARTIAL VISION 2022 Technical Exploitation Experiment Lessons Identified Report.*
- NTEG.** (2023a). *MARTIAL VISION 2023 LESSONS IDENTIFIED REPORT.*
- NTEG.** (2023b). *TECHNICAL EXPLOITATION COORDINATION CAPABILITY (TECC) CONCEPT OF EMPLOYMENT (CONEMP).*
- NTEG.** (2024). *NATO TECHNICAL EXPLOITATION GROUP (NTEG) CBRN MERT Validation Experiment Final Report Note from the Secretary.*
- Pînzariu, S. G., Neag, M. M., & Pînzariu, A. I.** (2024). Enhancing Joint Training and Education in Nato: A Comprehensive Framework for Interoperability and Operational Effectiveness. *Scientific Bulletin*, 29(1), 111–117. <https://doi.org/10.2478/BSAFT-2024-0012>
- Pumphrey, J. V.** (2025). *Action Research in the Military: Experiences, Outcomes and Learning.* <https://doi.org/10.25316/IR-20303>
- Rietveld, R.** (2024). *After Action Review: ICRC Global Military Personnel Identification Conference OCT 2024.*
- Rietveld, R.** (2025). *Technical Exploitation and Battlefield Evidence in NATO: Progress Report and Recommendations.*
- Sjøgren, S., & Nilsson, N.** (2025). Multinational Mission Command: From Paper to Practice in NATO. *Scandinavian Journal of Military Studies*, 8(1), 89–103. <https://doi.org/10.31374/sjms.329>
- Soeters, J., & Goldenberg, I.** (2019). Information sharing in multinational security and military operations. Why and why not? With whom and with whom not? *Defence Studies*, 19(1), 37–48. <https://doi.org/10.1080/14702436.2018.1558055>
- Soeters, J., & Manigart, P.** (2009). Military Cooperation in Multinational Peace Operations: Managing cultural diversity and crisis response. *Military Cooperation in Multinational Peace Operations: Managing Cultural Diversity and Crisis Response*, 1–255. <https://doi.org/10.4324/9780203928721>
- Trev, B.** (2022, May 17). *Documentary: The true horror of Russia's war in Ukraine*[News/Independent TV. <https://www.independent.co.uk/tv/news/ukraine-russia-war-crimes-b2080736.html>
- UN.** (2023). *Investigative Team to Promote Accountability for Crimes Committed by Da'esh/ISIL (UNITAD).* UNITAD. <https://www.unitad.un.org/>
- Wells, W.** (2025). *Battlefield Evidence in the Age of Artificial Intelligence-Enabled Warfare*[Chicago Journal of International Law. Chicago Journal of International Law. <https://cjl.uchicago.edu/print-archive/battlefield-evidence-age-artificial-intelligence-enabled-warfare>
- Wilson, L. E.** (2018). *Forensic and technical exploitation in the military domain.*
- Wilson, L. E., Gahan, M. E., Lennard, C., & Robertson, J.** (2019). The black sheep of forensic science: military forensic and technical exploitation. *Australian Journal of Forensic Sciences*, 51(6). <https://doi.org/10.1080/00450618.2018.1541194>
- Wilson, L. E., Gahan, M. E., Lennard, C., & Robertson, J.** (2020a). The forensic intelligence continuum in the military context. *Australian Journal of Forensic Sciences*, 52(1), 3–15. <https://doi.org/10.1080/00450618.2018.1459839>
- Wilson, L. E., Gahan, M. E., Lennard, C., & Robertson, J.** (2021). Case study–crown prosecution of a British citizen for the extraterritorial murder of Sergeant First Class Randy Johnson, United States 2nd Cavalry Regiment. *Australian Journal of Forensic Sciences*, 53(1). <https://doi.org/10.1080/00450618.2019.1637939>
- Wilson, L. E., Kessler, M. P., Ellis-Smith, J., & Robertson, J.** (2020b). A systems approach to integration of military operations and law enforcement investigations: Toward a unified forensic intelligence model. *Wiley Interdisciplinary Reviews: Forensic Science*, 2(2), e1358. <https://doi.org/10.1002/WFS2.1358>

TO CITE THIS ARTICLE:

Rietveld, R. M. (2025). Towards a Future Battlefield Forensics Framework: A NATO Action Research Case Study. *Scandinavian Journal of Military Studies*, 8(1), pp. 451–465. DOI: <https://doi.org/10.31374/sjms.333>

Submitted: 15 September 2024

Accepted: 17 January 2025

Published: 27 November 2025

COPYRIGHT:

© 2025 The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC-BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited. See <http://creativecommons.org/licenses/by/4.0/>.

Scandinavian Journal of Military Studies is a peer-reviewed open access journal published by Scandinavian Military Studies.



DSPACE

<https://dspace.org/>

Towards a future battlefield forensics framework: a NATO action research case study

Rietveld, Rikke Michelle

2025-11-27

Scandinavian Military Studies

<https://doi.org/10.31374/sjms.333>

Rietveld RM. (2025) Towards a future battlefield forensics framework: a NATO action research case study. Scandinavian Journal of Military Studies, Volume 8, Issue 1, November 2025, pp. 451-465