The Use of Blockchain to Facilitate Ceasefire Agreements Enhanced with Military-Grade Communications

Ikechi Saviour Igboanusi [1] and Dong-Seong Kim [*2]

[1]ICT Convergence Research Center, Kumoh National Institute of Technology, South Korea
[2]Department of IT Convergence Engineering, Kumoh National Institute of Technology, South Korea
(ikechisaviour, dskim)@kumoh.ac.kr

***Abstract*—Ceasefire agreements are essential for de-escalating conflicts, but their inherent fragility often stems from challenges in establishing trust, verifying compliance, and ensuring secure communication, particularly in adversarial environments. This paper investigates the potential of blockchain technology, augmented by military-grade communication protocols, to overcome these obstacles and foster more resilient and enduring ceasefire agreements. We demonstrate how blockchain's core attributes—immutability, transparency, and decentralized trust—can be integrated into a secure communication framework to significantly improve the establishment and maintenance of such agreements. We introduce a novel blockchain-based framework specifically designed for ceasefire scenarios, detailing its architecture and its synergy with secure communication methodologies. Furthermore, simulation results are presented to illustrate the framework's potential to enhance transparency and build trust among parties. The paper also explores the practical aspects of integrating military-grade communication systems and analyzes the proposed system's resilience against potential adversarial threats. We conclude by discussing pathways for operational adoption and outlining future research avenues, emphasizing blockchain's transformative role in strengthening trust in volatile military contexts.**

***Index Terms*—Blockchain, Ceasefire Agreements, Conflict Resolution, Military Communications, Secure Communications, Smart Contracts, Trust Management.**

I. Introduction

Modern international conflicts are increasingly complex and protracted, often leading to ceasefire agreements that are fragile, short-lived, and difficult to sustain [1]. The evolving nature of warfare, which frequently involves non-state actors, asymmetric tactics, and shifting alliances, has made conflict resolution a significantly more intricate undertaking. Although ceasefires are crucial for de-escalation and peacebuilding, they are often undermined by a lack of enforceability, disputes over interpretation, and operational insecurities, thereby contributing to recurrent cycles of violence and instability [2], [3].

Traditional frameworks for establishing and managing ceasefire agreements often reveal substantial limitations in fostering trust, verifying compliance, and maintaining secure communication between involved parties [4]. Verification mechanisms typically rely on third-party observers or centralized reporting systems, which can be susceptible to manipulation, delays, or outright rejection by one or more conflicting parties [5]. Furthermore, in environments where communication channels are compromised or contested, the reliable exchange of sensitive information—vital for implementing and monitoring agreements—becomes precarious and vulnerable to interception or distortion [6].

Blockchain technology, characterized by its inherent immutability, transparency, and decentralized trust model, offers a promising avenue to enhance the robustness and traceability of ceasefire processes [7]. By providing a tamper-proof, shared ledger for agreement terms, implementation steps, and recorded actions, blockchain allows all parties to operate from a common, verifiable source of truth [8]. This distributed trust mechanism reduces reliance on intermediaries and facilitates real-time accountability [9], which is critical in volatile and rapidly changing conflict zones. Smart contracts, a key feature of blockchain, can automate the enforcement of agreement terms upon fulfillment of predetermined conditions, minimizing the need for intermediaries, reducing human error, and ensuring transparent and secure execution [10].

The integration of blockchain systems with military-grade communication protocols can establish a secure and resilient architecture. Such an architecture is capable of supporting encrypted information exchange and real-time monitoring even in hostile or contested environments [11]. This ensures that communications and data related to the ceasefire remain confidential, authenticated, and uninterrupted, even when subjected to active cyber or electronic warfare [12]. This dual-layered approach bolsters both the integrity of the agreement and the security of its execution.

This study develops and evaluates a blockchain-based model tailored for facilitating ceasefires, emphasizing the incorporation of secure communication capabilities. We assess its operational feasibility and strategic advantages. The proposed system is implemented as a functional prototype and tested

in simulated conflict scenarios to evaluate its effectiveness in real-time compliance tracking, secure message transmission, and auditable record-keeping. By merging technological innovation with established conflict resolution practices, this research seeks to contribute to a new paradigm for designing and enforcing ceasefire agreements.

The primary objectives of this paper are to:

- Investigate the feasibility and potential benefits of a blockchain-based system for facilitating ceasefire agreements.
- Propose a comprehensive blockchain model for ceasefire agreement formulation and enforcement.
- Detail the integration of secure, military-grade communication capabilities within this model.

II. Related Works

The establishment and maintenance of effective ceasefires are pivotal to conflict resolution and peacebuilding efforts [13]–[15]. However, contemporary conflicts, often marked by intra-state dynamics, non-state actor involvement, and fluid alliances, pose significant challenges to traditional ceasefire frameworks [13]. The limitations of conventional methods—particularly in trust-building, compliance verification, and secure communication—underscore the need for innovative approaches. This section reviews existing literature on the role of technology in addressing these limitations and enhancing the efficacy of ceasefire agreements.

A. Technology as a Resilience Factor in Peace Operations

Nzioki [16] highlights technology's crucial role in building resilience within peace operations, enabling them to adapt to the evolving challenges of modern conflicts. The dynamic nature of these conflicts necessitates agility and responsiveness from peace operations, and technology provides essential tools to meet these demands. According to Nzioki, integrating technology enhances peacekeepers' ability to implement mandates effectively and adapt to changing ground conditions. This perspective underscores the potential for specific technological applications to improve ceasefire processes.

B. Enhancing Ceasefire Monitoring and Verification through Technology

Several studies explore technology's potential to revolutionize ceasefire monitoring and verification. Hug [17], [18] offers a detailed analysis of technology use in the OSCE's monitoring mission in Ukraine, providing valuable insights into practical applications and limitations. Hug and Mason [18] emphasize that while technology can significantly aid ceasefire monitoring, its capabilities and limitations must be carefully assessed alongside other factors influencing a ceasefire's success or failure.

Hug [17] further elaborates on lessons from the Ukraine conflict, demonstrating how technology can improve the effectiveness of monitoring and verification. This includes using unmanned aerial vehicles (UAVs), ground sensors, and other remote monitoring tools to observe and record potential ceasefire violations. By providing real-time data and enhancing situational awareness, technology can contribute to more accurate and timely reporting, crucial for maintaining ceasefire integrity.

Verjee [19] also examines technology's role in ceasefire monitoring, focusing on the OSCE mission in Ukraine. While acknowledging technology's potential benefits, Verjee cautions against overreliance and stresses understanding its limitations. The study emphasizes that technology is a tool that requires strategic use in conjunction with human observers for optimal results. Verjee and Sticher [20] further discuss the complexities of using remote sensing technologies by ceasefire monitors, noting divergent assessments of their impact on ceasefire compliance.

C. Artificial Intelligence and Ceasefire-Related Applications

While this paper focuses primarily on blockchain technology, it is important to acknowledge contributions from other technological advancements in conflict resolution. The "CEASEFIRE" project [21], for instance, demonstrates the potential of artificial intelligence (AI) in combating illicit firearms trafficking, a critical factor in sustaining peace and security. Although this project addresses a different facet of conflict, it illustrates the broader trend of leveraging advanced technologies to support peace efforts.

III. System Model

Effectively managing ceasefire agreements requires addressing several persistent challenges. Technology offers viable solutions to these issues. Firstly, **improving compliance and verification** is critical; traditional third-party observation methods are often flawed. Technology can provide impartial, verifiable data on troop movements, prohibited weaponry, and other potential breaches, thereby strengthening the verification process. It can also introduce incentives to encourage adherence. Secondly, **enhancing secure communication** is paramount in conflict zones characterized by low trust and high interception risks. Encrypted communication systems and secure data-sharing platforms can facilitate the exchange of sensitive information for ceasefire implementation and monitoring, reducing misinterpretation and mistrust. Lastly, **increasing transparency and accountability** is essential for building trust. Technology can provide a shared, accessible record of ceasefire terms, implementation steps, and reported violations, helping to reduce disputes and increase accountability for breaches. This research was motivated by the need to address these three challenges.

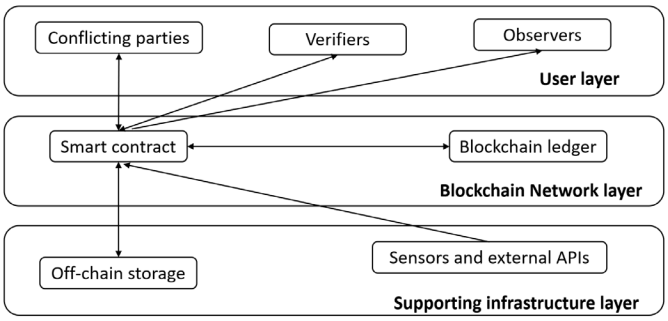

Fig. 1: Diagram of the proposed blockchain-based system model for ceasefire agreements.

The proposed system leverages blockchain technology to improve the establishment, monitoring, and enforcement of ceasefire agreements. It aims to enhance trust, transparency, and accountability among conflicting parties by providing an immutable and auditable platform for managing agreement terms, tracking compliance, and executing predefined consequences. This section details the system's architecture, core components, operational workflow, and underlying assumptions. As illustrated in Figure 1, the model integrates smart contracts for the automated execution of agreement clauses. This includes a novel mechanism for financial incentivization based on compliance scores, applicable both periodically throughout the agreement and at its conclusion.

A. System Architecture

The system architecture, notionally illustrated in Figure 1, is centered around a permissioned or public blockchain network, upon which a dedicated smart contract governs the lifecycle of ceasefire agreements. Several key architectural layers work in concert. The **Blockchain Layer** provides the distributed ledger technology for immutable record-keeping of all agreement-related transactions, states, and events, ensuring data integrity and transparency. Above this, the **Smart Contract Layer** contains the business logic for the ceasefire agreement, including functions for initialization, party registration, data reporting, violation verification, and financial settlement, thereby automating the execution of agreement terms. Interaction with the smart contract is facilitated by the **Application Layer**, which consists of interfaces (e.g., web or mobile applications) for authorized participants such as conflicting parties, mediators, and monitoring agents. Complementing these, a **Secure Communication Layer** operates in conjunction with the blockchain, utilizing military-grade communication protocols for the secure off-chain exchange of sensitive information like detailed violation evidence or negotiation messages, with hashes of this information stored on-chain for verification. Finally, an **Off-Chain Storage Layer** is employed for storing large data files, such as detailed observation reports or multimedia evidence, which are too costly or impractical to store directly on the blockchain; links to this data, like cryptographic hashes, are recorded on-chain.

B. Core Components

The system comprises several key components essential for its operation. The **Conflicting Parties** are the primary entities involved in the ceasefire agreement, participating in defining terms, potentially contributing to a pooled fund for financial incentives, reporting alleged violations, and being subject to the agreement's rules and consequences. **Monitoring Agents**, which can be authorized individuals or automated systems (e.g., UAVs, ground sensors), are responsible for observing adherence to ceasefire terms and reporting observations or potential violations to the smart contract; their registration (`registerMonitoringAgent`) ensures data provenance. **Verifiers/Mediators** act as neutral third parties or a council of representatives responsible for verifying reported violations (`verifyViolation`), a role crucial for the fair adjudication of disputes and the integrity of the violation scoring mechanism. Central to the system is the **Ceasefire Smart Contract**, the digital embodiment of the agreement deployed on the blockchain. Its key functionalities include agreement initialization (`initializeAgreement`), reporting of observations (`reportObservation`) and violations (`reportViolation`), verification of violations (`verifyViolation`) and subsequent scoring, management of a pooled fund (`depositFunds`), end-of-period financial settlement based on compliance scores (`finalizeAndDistributeFunds`) which can be supplemented by interim adjustments, and secure logging of communication metadata (`logCommunication`). Lastly, **State Variables**, as defined in the Canvas (e.g., `violationScores`, `agreementFundPool`, `contributions`, `fundsDistributed`), track the dynamic state of each agreement managed by the smart contract.

C. Operational Workflow and Key Features

The operational workflow of a ceasefire agreement within this system model, as depicted in Figure 1, follows distinct phases underpinned by the smart contract's functions. The process begins with **Agreement Initialization and Funding**. During this phase, parties agree on terms, which are then hashed and stored on-chain via the `initializeAgreement` function; this also sets start and end dates and registers the involved parties. The terms may specify periodic review milestones and associated financial implications. If the financial incentive mechanism is utilized, participating parties deposit agreed-upon funds into a pool managed by the smart contract using `depositFunds`.

Following initialization, the **Monitoring and Reporting** phase commences. Registered monitoring agents (`registerMonitoringAgent`) submit observations

Function Name	Explanation
initializeAgreement	Sets up a new ceasefire agreement with its core details, parties, terms, duration, and mediator.
registerMonitoringAgent	Allows the mediator to authorize an address as an official monitoring agent for an agreement.
reportObservation	Enables a registered monitoring agent to submit an observation regarding an active ceasefire.
reportViolation	Permits a party to an agreement to formally report an alleged violation by another participating party.
verifyViolation	Allows the mediator to confirm or reject a reported violation and update the violator's score if confirmed.
logCommunication	Enables a party to record metadata of an official communication with another party or the mediator.
triggerEscalation	Allows the mediator to log a formal escalation measure taken in response to a verified violation.
updateAgreementStatus	Permits the mediator to change the overall status of a ceasefire agreement (e.g., Concluded, Terminated).
getAgreementDetails	Provides a way to retrieve the main public details of a specific ceasefire agreement.
getPartyViolationScore	Returns the current number of verified violations for a specific party within a given agreement.
getPartyContribution	Returns the amount of funds a specific party has contributed to an agreement's financial pool.
getViolationReport	Provides a way to retrieve the detailed information about a specific reported violation.
depositFunds	Allows a participating party to add funds to the designated financial pool for a ceasefire agreement.
finalizeAndDistributeFunds	Enables the mediator to initiate the distribution of pooled funds based on final violation scores at the agreement's end.

(`reportObservation`), and participating parties can report alleged violations by other parties (`reportViolation`), providing a hash of supporting evidence that is stored off-chain. These reports then move into the **Violation Verification and Scoring** phase, which can be both periodic and continuous. Reported violations undergo a verification process managed by designated verifiers, with the outcome recorded using `verifyViolation`. If a violation is verified, the smart contract automatically increments the `violationScore` for the offending party associated with that specific agreement; false or unverified reports do not impact scores, addressing the need for robust verification. This verification can be linked to predefined periodic review milestones, allowing for interim compliance assessments that could trigger pre-defined financial adjustments or other consequences based on accumulated `violationScores`.

Throughout the agreement, **Communication Logging** can occur, where metadata of official communications (hashes of encrypted messages) between parties is logged on-chain via `logCommunication`, providing an auditable trail without compromising message content. The workflow culminates in **Agreement Conclusion and Final Fund Distribution**. While the system can support interim financial adjustments at periodic milestones, a final settlement typically occurs upon the `endDate` via `finalizeAndDistributeFunds`. At this point, the smart contract calculates the final distribution of the remaining `agreementFundPool` based on the total accumulated `violationScores`. Parties with fewer verified violations receive a proportionally larger share. If no violations are recorded, funds may be returned based on original contributions or equally, as per prior agreement. A key feature throughout this workflow is **Transparency and Auditability**, as all transactions, state changes (like violation scores, fund status, and interim adjustments), and key events are immutably recorded on the blockchain and accessible to authorized participants (`getAgreementDetails`, `getViolationReport`), enhancing transparency and reducing disputes over facts.

D. Assumptions of the Model

The proposed system model, as illustrated in Figure 1, operates under several key assumptions. Primarily, it assumes that all relevant parties are willing and able to participate in the blockchain network and interact with the smart contract. A critical assumption is the existence of a **trusted verification process**, meaning mechanisms are in place to ensure that entities responsible for verifying violations (`verifyViolation`) are trusted by all parties or operate under a mutually agreed and transparent governance model; the integrity of this process is paramount for the financial incentive model, for both periodic reviews and final settlement. The model also relies on the availability of **secure off-chain components**, such as military-grade communication channels for sensitive data exchange and robust, reliable off-chain storage solutions for detailed evidence. Furthermore, it is assumed that participants possess the necessary **digital literacy and access** to technology to interact with the system. The terms of the ceasefire, including violation definitions, fund contribution/distribution rules, and specifics of periodic review milestones and their financial implications, must be **well-defined and agreed upon** before being encoded or referenced in the smart contract. Finally, if financial incentives involve cryptocurrency, it is assumed that parties are willing and able to transact using it and that the **cryptocurrency utility** is stable without significant value volatility.

E. System Behavior and Dynamics

The behavior of the ceasefire management system, supported by the architecture shown in Figure 1, is event-driven and state-centric, primarily governed by interactions with the Ceasefire Smart Contract. The system's dynamics begin with **State Initialization** upon the deployment of the smart contract and the call to `initializeAgreement`. This transaction establishes the foundational parameters on the blockchain, including parties, terms hash, duration (potentially with interim milestones), and initializes state variables like `violationScores` and the `agreementFundPool`.

Subsequent actions by participants trigger **Reactive Event Handling** through specific smart contract functions, leading

to state changes. For instance, a call to `reportViolation` creates a new violation report and emits an event for verification. The `verifyViolation` function, when called by authorized verifiers, updates the violation report's status; if verified, it immutably increments the offending party's `violationScore`, directly impacting their standing in the incentive structure, with this score assessable both periodically and at the agreement's end. Similarly, `depositFunds` transactions transparently update the `agreementFundPool` and individual `contributions`. The system inherently promotes **Information Flow and Transparency**, as all critical actions and state changes are recorded as blockchain transactions, viewable by permissioned participants through functions like `getAgreementDetails` and `getViolationReport`, fostering a shared understanding.

Automated Logic Execution is another core dynamic, where the smart contract algorithmically executes predefined logic, such as the fund distribution calculation in `finalizeAndDistributeFunds` based on final `violationScores`, or similar logic at periodic milestones for interim adjustments. The system's behavior is also characterized by **Temporal Dynamics**, with the `startDate` and `endDate` defining the active ceasefire period. The system can accommodate predefined interim periods or milestones where compliance checks could trigger pre-agreed partial financial distributions or other consequences from the `agreementFundPool`, providing more immediate feedback. The `finalizeAndDistributeFunds` function is typically executable only after the `endDate`. This structure is designed to foster **Incentive-Driven Behavior (Anticipated)**, where the financial mechanism tied to `violationScores` deters breaches, a deterrent potentially amplified by periodic adjustments making consequences more immediate. While automation is high, the model implicitly relies on off-chain or agreed-upon governance for **Dispute Resolution (Implicit)** concerning complex interpretations before `verifyViolation` is irrevocably called, with the on-chain record serving as a factual basis.

Thus, the system behaves as a dynamic, auditable, and partially automated framework where participant actions directly and transparently influence the state and outcomes of the ceasefire agreement as recorded on the blockchain, offering options for both periodic and concluding financial incentivization. This system model, by leveraging blockchain and smart contracts, aims to provide a more robust, transparent, and enforceable framework for ceasefire agreements, addressing key challenges in contemporary conflict resolution. The introduction of a scored, end-of-period financial settlement mechanism, potentially augmented by periodic adjustments, offers a novel approach to incentivizing adherence to agreed terms.

IV. Results

A functional prototype of the proposed blockchain system for ceasefire agreements was developed. Its core, the Ceasefire Smart Contract, which codifies agreement terms, was successfully deployed, demonstrating foundational system readiness.

Fig. 2: Successful deployment transaction of the Ceasefire Smart Contract, detailing transaction parameters and event logs from the blockchain environment.

Figure 2 shows the successful blockchain deployment of the `SingleCeasefireAgreementContract` constructor, detailing:

- **Transaction Hash**: `0xf97d...86c55`, confirming blockchain inclusion.
- **Contract Address**: `0x0774...3f1f90`, its unique on-chain identifier.
- **Execution Cost**: Gas used (`555903`) and transaction cost (`5836981 gwei`).
- **Logs**: An "AgreementInitialized" event, confirming operational status.

This deployment validates the smart contract's basic on-chain functionality. The prototype was further tested in simulated conflict scenarios to examine its capacity for real-time compliance tracking, secure message transmission, and auditable recordkeeping. These simulations aimed to substantiate the potential improvements in transparency and trust.

V. Conclusion

Traditional ceasefire agreements face stability challenges due to issues in trust, verification, and secure communication. This paper presented a novel blockchain framework, enhanced with military-grade communications, to foster more durable agreements. Leveraging smart contracts for transparent management and compliance, and secure protocols for information integrity, our prototype and simulations demonstrated significant potential to improve transparency and trust among conflicting parties.

The system's architecture offers resilience against adversarial threats, contributing to a new paradigm in ceasefire enforcement. Future work will prioritize operational adoption and further research into blockchain's role in enhancing trust in volatile military and peacekeeping operations, aiming for more stable and lasting peace.

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the Institute of IITP grant funded by the Korean government(MSIT) (IITP-2024-2020-0-01612, 50%) and by Priority Research Centers Program through the NRF funded by the MEST(2018R1A6A1A03024003, 50%)

References

[1] R. Ficek, *The Fragile States in the Global Security System*. Cham: Springer Nature Switzerland, 2024, pp. 91–141. [Online]. Available: https://doi.org/10.1007/978-3-031-55356-1_3

[2] L. Nathan and A. Sethi, "Reducing and managing risk: The dimensions of strong ceasefires in intra-state conflict," *International Studies Review*, vol. 25, no. 1, p. viac065, 02 2023. [Online]. Available: https://doi.org/10.1093/isr/viac065

[3] M. A. Özoflu, "Navigating fragility: Unraveling intergroup relations in south sudan's peace-building process," *Journal of Humanity, Peace and Justice*, vol. 1, no. 1, p. 37–48, 2024.

[4] A. V. and, "Routine but consequential: How ceasefire monitors' reporting constructs opportunities for (non)compliance by conflict opponents," *International Peacekeeping*, vol. 31, no. 4, pp. 473–498, 2024. [Online]. Available: https://doi.org/10.1080/13533312.2024.2342861

[5] J. M. Braithwaite and C. Butcher, "Muddying the waters: The anatomy of resistance campaigns and the failure of ceasefires in civil wars," *Journal of Conflict Resolution*, vol. 67, no. 7-8, pp. 1376–1404, 2023. [Online]. Available: https://doi.org/10.1177/00220027231159828

[6] A. Verjee, "Ceasefire monitoring under fire: The osce, technology, and the 2022 war in ukraine," *Global Policy*, vol. 13, no. 5, pp. 808–817, 2022. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/1758-5899.13123

[7] V. Ali, A. A. Norman, and S. R. B. Azzuhri, "Characteristics of blockchain and its relationship with trust," *IEEE Access*, vol. 11, pp. 15 364–15 374, 2023.

[8] S. Dong, K. Abbas, M. Li, and J. Kamruzzaman, "Blockchain technology and application: an overview," *PeerJ Computer Science*, vol. 9, p. e1705, 2023, © 2023 Dong et al. Licensed under CC BY 4.0. [Online]. Available: https://doi.org/10.7717/peerj-cs.1705

[9] R. Lal, A. Chhabra, S. Singla, and D. Sharma, "Blockchain technology: Revolutionizing trust, transparency, and transaction efficiency," in *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS)*, vol. 1, 2024, pp. 1–5.

[10] P. Tolmach, Y. Li, S.-W. Lin, Y. Liu, and Z. Li, "A survey of smart contract formal specification and verification," *ACM Comput. Surv.*, vol. 54, no. 7, Jul. 2021. [Online]. Available: https://doi.org/10.1145/3464421

[11] A. Sonawane and S. Patil, "Guardianlink: Fortifying highly secure data communication between decentralized army stations," *Journal of Data Acquisition and Processing*, vol. 39, no. 1, pp. 1227–1236, 2024, iSSN: 1004-9037. [Online]. Available: https://sjcjycl.cn/

[12] C. S. Babu and A. Pal, *Enhancing Security for Unmanned Aircraft Systems in IoT Environments*. John Wiley & Sons, Ltd, 2024, ch. 11, pp. 429–476. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781394230648.ch11

[13] G. Clayton, S. J. A. Mason, V. Sticher, and C. Wiehler, "Ceasefires in intra-state peace processes," *CSS Analyses in Security Policy*, no. 252, 2019.

[14] A. Duursma, "Peacekeeping, mediation, and the conclusion of local ceasefires in non-state conflicts," *Journal of Conflict Resolution*, vol. 67, no. 7-8, pp. 1405–1429, 2022.

[15] V. Sticher and S. Vuković, "Bargaining in intrastate conflicts: The shifting role of ceasefires," *Journal of Peace Research*, vol. 58, no. 6, pp. 1284–1299, 2021.

[16] V. W. Nzioki, "Technology as a resilience factor in peace operations," *Connections: The Quarterly Journal*, vol. 19, no. 4, pp. 69–85, 2020.

[17] A. Hug, "Ceasefire monitoring and verification and the use of technology: Insights from ukraine 2014-2022," ETH Zurich, Report 21, 2024.

[18] A. Hug and S. J. A. Mason, "Ceasefire monitoring and verification technology," ETH Zurich, Other Publication 10/2, 2022.

[19] A. Verjee, "Ceasefire monitoring under fire: The osce, technology, and the 2022 war in ukraine," *Global Policy*, 2022.

[20] V. Sticher and A. Verjee, "Do eyes in the sky ensure peace on the ground? the uncertain contributions of remote sensing to ceasefire compliance," *International Studies Review*, 2023. [Online]. Available: https://doi.org/10.1093/isr/viad039

[21] J. Cani, I. Mademlis, M. Mancuso *et al.*, "Ceasefire: An ai-powered system for combating illicit firearms trafficking," in *2024 IEEE International Conference on Big Data (BigData)*. IEEE, 2024.