Research Output Journal of Arts and Management 5(1):1-10, 2026

ROJAM Publications PRINT ISSN: 1115-6112

https://rojournals.org/roj-art-and-management/ ONLINE ISSN: 1115-9065

https://doi.org/10.59298/ROJAM/2026/5111000

Conflict Early-Warning with Big Data: Ethics, Accuracy, and Governance

Kato Nabirye H.

Faculty of Business, Kampala International University, Uganda

ABSTRACT

Conflict early-warning systems (CEWS) enhanced by big data analytics represent a transformative approach to predicting and preventing violent conflict. This study explores the intersection of ethics, accuracy, and governance in the deployment of such systems, emphasizing their interdependence within complex socio-technical environments. Drawing on existing literature and multi-context evidence, the paper examines how big data sourced from social media, satellite imagery, and transactional records improves predictive capabilities through advanced methodologies such as machine learning, anomaly detection, and probabilistic forecasting. However, these innovations introduce critical challenges, including data bias, privacy violations, lack of transparency, and risks of political manipulation. The study highlights the importance of robust evaluation metrics, data quality assurance, and model interpretability in ensuring predictive reliability. It further analyzes governance frameworks, focusing on accountability mechanisms, stakeholder involvement, and legal compliance necessary for responsible deployment. Empirical evidence reveals mixed predictive performance, underscoring the limitations of current models and the need for methodological rigor and reproducibility. Ultimately, the paper argues that while big data significantly enhances early-warning capacities, its effectiveness depends on embedding ethical safeguards and governance structures that ensure fairness, trust, and accountability. The study contributes to the literature by offering a comprehensive framework that integrates technical performance with ethical and institutional considerations.

Keywords: Conflict Early-Warning Systems (CEWS), Big Data Analytics, Political Violence Prediction, Algorithmic Governance, and Ethical AI.

INTRODUCTION

Conflict early-warning systems that leverage the rapid development of big data analytics hold great promise for improving the well-being of society [1]. By integrating disruptive technologies into existing methodologies, the capabilities of quantifying and predicting the risk of violent conflict have been substantially advanced. The main contribution of such systems is the enhanced predictive accuracy, involving the spatial and temporal dimension of certain types of conflict and some popular methods adapted from the area of forecasting to determine the trend evolution of a specific conflict [2]. However, the ethical and governance challenges of these emerging systems remain open for discussion. While much work has focused on early-warning systems and big data analytics independently, the literature on the interdependence of the two topics remains scarce. The case for the interconnectedness of ethics, accuracy, and governance can be substantiated with examples. Violent content shared by a government on social media can be blamed on a certain party to the situation [3]. Without a formal investigation, this material containing an expanded definition of violence could be ignored by the system. If not taking into account geopolitical power, a systematic bias in the expected number of conflict events overestimates the risk trajectory in certain locations [4]. Furthermore, regulation guarantees an acceptable threshold on the above faults.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

Conceptual Foundations of Early-Warning Systems

The notion of early warning encompasses diverse definitions and interpretations owing to its historical use across varied contexts ranging from natural hazards to financial crises. Most importantly, the concept remains ill-defined when isolated from specific authorities and social values [5]. There is general agreement, nonetheless, that early warning assumes three primary components: the identification of critical systems or processes that issue response signals, the recognition of system or process monitoring capabilities in place (without such capabilities, speeds of change cannot be duly assessed), and the existence of response mechanisms to deal with such impending changes.

Conflicts, like human- or socio-political systems, arise from differing values among communities [6]. When shared values do not emerge during the life-cycle of conflicts, the condition of public contestation intensifies, resulting in the elaboration of socio-political processes to abandon the contestation and return to the maintenance of peace [1]. Early warning defines the point on the socio-psychological spectrum where contestation relies on resources to pursue alternatives to dialogue, which ultimately emerge as real or stated conflicts of interest [5]. Policies arising too early or too late massively increase risks of enhancement in conflicts and both access to dialogue and its contribution to peace-building [5]. Considering conflict processes one of the major dimensions of human behaviour shaping singular post-Cold War SDG conflicts through various cycles, fires, and descriptions of movement behaviours towards possible early-warnings of conflict recognition become crucial for preventing escalation or aggravation of peer civil wars [6].

Big Data in Conflict Prediction: Opportunities and Challenges

Big Data offers unprecedented opportunities for conflict prediction, but it also poses significant technical, ethical, and governance challenges [1]. The term refers to large volumes and varieties of data collected from diverse digital sources, such as social media, web forums, and transaction records, that may help identify risk factors and monitor conflict dynamics [2]. An analytic approach involves exploring correlations, anomalies, and causal relationships to estimate time horizons and impact [3]. High-dimensional and relational data provide early indicators of emerging conflicts, while irregular and low-frequency observations enable continual monitoring between conflict events, generating both lead-time advantages and real-time risk assessments[4]. Furthermore, Big Data protects privacy through model-based analysis that attenuates geographical and individual specificity, a crucial feature for sensitive contexts where human rights abuses are at stake [5]. Technically, Big Data imposes stringent requirements on the collection, integration, processing, modelling, and validation of heterogeneous, high-dimensional, and rapid-flow information. Governance and ethical concerns similarly become paramount, as confidentiality violations, discrimination, politicization, manipulation, irresponsibility, and opacity are not merely theoretical risks [6]. Uncontrolled Big Data deployment can undermine confidentiality agreements and threaten the safety of informants, in some cases exposing entire ethnic communities to retribution. Such risks are magnified in Internet environments characterised by adaptation, exploitation, and competition among conflicting parties [7, 8]. The catalytic adoption of a novel data-driven paradigm also promises to reshape institutional and societal configurations.

Data Sources and Integration

Early warning systems rely on data to inform diplomats and humanitarian actors about risks of violence in societies facing conflict [9]. Available datasets determine what information can be processed, which limits predictive sophistication and integrity. Forecasting systems integrating automatic text analysis and statistical data fail to outdo predictions based on simpler datasets manually supplemented to enrich content [4]. Data sources play different roles in early warning for global crises that need comprehensive monitoring from various angles and at different organisational levels, from local to national, regional, and international[8]. Because violence can have multiple causes, monitoring through multiple channels helps actors interpret the situation, and data identified as relevant beforehand can be tracked over time [7, 10].

Methodologies for Prediction and Risk Assessment

The dynamic character of conflicts has raised the need for disaggregated prediction on trends at multiple scales [3]. These developments highlight the importance of versatile methodologies to characterize trends that translate to heterogeneous applications and user requirements [3]. International interventions have increasingly operated at a lower berth to stabilize civilian or humanitarian crises before they escalate to intrastate wars [4]. Educational materials accompanying risk maps detail the analytical foundations of the broader trends being transmitted on a national or collective scale and inform the associated preventative narratives being activated at the combined level. Predictive analytics constitute an umbrella term for methodologies aiming to characterize future developments at a certain time and context based on historical data [5]. Conflict-contingent crisis phenomena cover violence, civilian displacement, governance weakening, and crime. Such developments form a disaggregated component of trends often resulting in concerted international intervention [6]. Monitoring the prevalence of these phenomena provides a channel for anticipation within the wider preventative framework [7].

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

Evaluation Metrics and Validation

Early-warning and risk-assessment systems for conflicts or crises based on big data rely on various machine learning techniques [6]. These techniques include, among others, regression methods (for predicting the time until a critical event occurs), supervised classification (for determining the onset of a specified event), probabilistic prediction (for determining the uncertainty about when a particular event will happen), and anomaly detection (for identifying emerging patterns that deviate from past precedents) [6]. Evaluating predictive performance can be done through standard and widely used metrics. However, these metrics might not capture all the dimensions that the different prediction tasks offer [8]. Taking, for instance, binary classifiers predicting the occurrence of certain phenomena, standard metrics like AUC-ROC (area under the receiver operating characteristic curve) or PRAUC (area under the precision-recall curve) estimate the expected utility when the policy is to intervene on the emerging events [7]. Priority ranking, a relevant dimension to explore, assesses how well the model ranks the better candidates to intervene, as early as possible [9]. This consideration is crucial when many emerging events are predicted to happen. Another aspect of analysis might relate to the co-occurrence of certain phenomena, employing the same expected utility as a criterion. Standard evaluation metrics capture a specific dimension of the problem, but other viewpoints could be beneficial when assessing the predictive performance of the models [10].

Ethical Considerations and Responsible Innovation

The ethical implications of conflict early-warning systems employing big data warrant serious consideration, especially as such systems proliferate [3]. Conscientious practitioners are urged to take ethical issues into account throughout the research and development (R&D) process, addressing not only public concerns about accuracy and governance but also issues such as privacy, consent, bias, and transparency many of which are amplified by the scale and complexity of big data [4]. Such deliberation must continue after the systems are put into use, as experience may illuminate new ethical dilemmas. This section identifies several common ethical challenges and proposes potential avenues for responsible innovation [5]. The first concern is privacy, particularly regarding the ethics of data collection without explicit consent or knowledge of affected individuals [6]. Individuals increasingly have difficulty controlling their own data, as the proliferation of sensing devices creates detailed profiles of online and offline activities [7, 8]. Early warning systems that collect, combine, and analyze big datasets in real time may amplify such problems, with substantial commercial and reputational incentives for pervasive data collection. This raises fundamental questions about the very notion of consent, especially when data is de-identified or obtained from public sources [9]. The second concern relates to the underlying datasets, which may embed bias against particular groups or populations. Such biases can stem from the selection of variables, the construction of measures, or the characteristics of data sources [10]. Biases propagate through the modelling and training process, undermining fairness and accuracy in the resulting predictions. Biases that are already present can also be amplified, with automated learning technologies introducing machine bias [11]. The increasing use of automated and black-box machine-learning techniques poses formidable challenges for transparency, as the very nature of such techniques renders explanations difficult [12]. Yet transparency is seen as a prerequisite for accountability: for the system to be trusted, an understanding of how it arrives at results must be available [13].

Privacy, Consent, and Data Rights

Governance frameworks should integrate ethical safeguards into the use of big data for conflict early warning [10]. Privacy is a fundamental right, and individuals can choose whether to reveal their personally identifiable information (PII). A recent survey highlights areas needing improvement, such as a lack of awareness about the extent of government surveillance, inadequate consent procedures, and insufficient transparency regarding the flow of data and the identity of manufacturers and service providers [11]. Privacy remains a topic of concern in many countries: even with the introduction of laws directing companies to inform users of data breaches, the report showed a glaring lack of awareness against confidential information being shared [12]. Judicial management of big data is becoming increasingly important; this can be fulfilled by establishing a digital bill of rights based on the principles of dignity, knowledge, freedom, prudence, benefit, and trust [13]. To ensure the legitimacy of information sharing, three complementary conditions must be satisfied: it must be a collective good, the information hosting and providing service must be reasonable and open, and an effective information management approach must be in place [12]. Data for the public good, forbids the use of participants' data for commercial purposes. Such data sharing transcends the boundaries of traditional data sharing within the enterprise; in a sense, hidden relationships can be mined by social network analysis, max- imizing the value of the data without any extra cost [14]. The mutual-consent design principle provides the necessary mechanism for data holders to agree on data usage rules and truly run a "data market"[15].

Bias, Fairness, and Transparency

Big data can enhance conflict early-warning systems (CEWS) by generating predictions from sources such as news articles, social media, and satellite imagery [1]. Addressing these issues through ethics guidelines or similar frameworks is crucial for CEWS development and implementation [9]. The predictive capacity of big data relies on statistical analyses of existing data to identify patterns linked to conflict onset, escalation, or resolution. Data-

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

driving prediction can amplify underlying biases, with trained models giving primacy to the most readily available datasets [10]. Generally, CEWS cannot guarantee equitable model performance across diverse populations and historical contexts; the inclusion of additional features, regions of interest, and unanticipated data is inevitable. Regardless of the analytical framework or data requirements, any operational model must fully disclose the features, datasets, and approaches employed; provide the rationale for these choices; and communicate any accompanying limitations [10].

Accountability and Governance Mechanisms

The concept of accountability is often closely associated with three distinct elements: the attribution of responsibility, the establishment of trust, and the necessity for governance [9]. The modern governance landscape demands a rethinking of accountability rooted not only in the sovereign state but in political, socio-economic and technological levels [11]. Assessing the individual accountability of technology and its consequences also necessitates a level of interconnectivity fundamental to society today [10]. Consequently, accountability frameworks that focus exclusively on the technology referred to as Smart Machine Accountability (SMA) risk missing interactions with other political and social stakeholders [11]. Rather than focusing solely on technology itself, Green & Hu recommend a multidimensional framework applicable to humans, machines, organizations, and systems that identifies mechanisms, agents, domains, and activities in socio-technical accountability arrangements[12]. The primary goal of an accountability framework is to provide governance guidance throughout the investigation and assessment processes [12]. Such a framework is especially pertinent in the emerging domain of algorithm accountability, where decisions are increasingly delegated to automated algorithms lacking sufficient transparency for effective independent scrutiny [13]. Governance mechanisms vary depending on whether a scientific activity is performed in a research or production context, though most research activities also adhere to institutional or sectorial guidelines, such as Open Science. Effective governance therefore requires delineating the operational context [14]. Ethical governance is also dependent on context, shifting emphasis from the types of data employed to the broader socio-technical context in which governance is applied and the balance of power among involved actors [15]. A comprehensive governance framework must also address validity, safety, security, performance, resilience, robustness, sustainability, and risk for both the socio-technical system as a whole and the individual components involved [13]. Increasing concern over empowered algorithmic autonomy has led to a focus on algorithmic accountability, ensuring that socio-technical systems enable parties to answer for their algorithmic actions [14]. However, systems and stakeholders also require empowerment, as algorithms, machines, software, and services take on roles previously performed by humans [15]. Conflicts of interest exist among the involved actors throughout the governance process. The need to actively mitigate harm and enable its persistent employment must therefore be acknowledged when articulating responsibility an imperative that varies with the socio-technical context and other external pressures [16].

Governance Frameworks for Deployment

Governance arrangements for deploying conflict early-warning systems with big data must address decision-making on data sharing and integration; legal and regulatory frameworks; and the safety, security, and risk of associated technologies [14].

Institutional Arrangements and Stakeholder Involvement

A key challenge for conflict early-warning systems (CEWS) is to establish effective governance frameworks that clarify institutional responsibilities and corresponding ethical duties, thereby facilitating appropriate collaborations [8]. Governance consists of negotiated agreements and conducive institutional arrangements that allow stakeholders to collectively oversee a predicted problem and decide on necessary actions [15]. A CEWS generates predictive data that is not only political but also involves sensitive human dimensions. Such a system may therefore benefit from the involvement of multiple complementary stakeholders, including politicians and humanitarian organizations, who could contribute alternative perspectives and relevant experience to enhance an overall understanding of potential consequences [15]. The required arrangements may differ depending on the purpose of the CEWS, whether it is primarily informational, for advocacy, or to serve as a basis for resource allocation [15].

Legal and Regulatory Compliance

The increasing complexity and interconnectedness of the contemporary world give rise to a new generation of emergent, interconnected, and multifaceted risks at all levels from the individual to the global [6]. These risks exacerbated by climate change, the COVID-19 pandemic, and other cumulative shocks, interact and compound through feedback loops, providing only binary or monolithic early warning signals [7]. Only analysis at the intersection of global social, technological, economic, environmental, and political (STEEP) changes, preferably through an epistemic community such as an academically rigorous foresight network with publications and peer-reviewed articles, can help cope with the added uncertainty [8]. Very high-resolution European satellite imagery, Anglophone news sources, and ubiquitous sensors further bring new opportunities for a new generation of foresight tools [9]. Scholars urge consideration of the ethical implications of artificial intelligence to ensure

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

alignment with human values. The need for procedures to harmonize legal and regulatory laws globally has also increased notably [16]. Legislation, regulation, and disruptive crises are colliding, leaving institutions unable to cope with highly frequent, abrupt, and multilayered strategic disruptive acceleration [7]. The need for easy-to-use foresight simulation tools that assimilate vast multilevel STEEP changes to visualize potential cascading systemic shocks instead of a prior score of potential drivers has drastically gone up [13]. It is not impractical to consider helping open-source experimental democracies by monitoring of the potential sequencing of clashes between new policies and old legislative requirements from the design stages of new tools [11]. Institutions also need to spell out mapping or structuring of potential multilayered STEEP changes together with any accompanying new experimental governance models being worked on [12]. While some preparatory descriptive scenario work might be helpful for cooperations with small intimate post-industrial diverse, broad-minded, experimental open-source type ECM networks, such representatives of emerging experimental governance as e-diplomacy teams, social workers, humanitarian NGO big-data scientists, and government AIs, seeking, gathering, addressing, and helping record very high-resolution visible and reportable on-the-ground system shifts emerging simultaneously across wide number n of countries today could form decent candidate groups[13].

Safety, Security, and Risk Management

Managing safety, security, and risk concerns is crucial for deploying early-warning systems that draw on traditional and nontraditional information sources [10]. These systems must follow relevant laws, regulations, and institutional guidelines in order to preserve personal data protection, trade-secrets assurance, and privacy protection [11]. Noncompliance can expose stakeholders and users to potential liability and loss of reputation, and it can even render predictions invalid if the underlying data processing is compromised [8]. Safety and security risks also stem from malefactors using conflict analyses and forecasts for ulterior motives, targeting vulnerable countries and regions or generating misinformation to induce less principled responses [16]. Protecting prediction systems against adversarial exploitation improves confidence in their integrity and can enhance model transparency by teaching data owners how to guard against threats.

Case Studies and Empirical Evidence

In recent years, conflict early-warning systems powered by big data have rapidly emerged as a promising innovation to predict, preempt, and mitigate violent conflict escalation on a range of scales [13]. Academic and policy interest in the potential of big data for multi-faceted conflict prediction has grown significantly since the early 2010s, stimulating extensive implementation and evaluation of methodological experiments by scholars and practitioners alike [14]. An investigation into the ethical, governance, and accuracy dimensions of conflict prediction finds that they are strongly interdependent [15]. The deployment of algorithmic models to predict violent conflict, such as civil war, urban unrest, or international war, offers unprecedented opportunities and poses substantial risks. Systems capable of accurately predicting the onset and escalation of crises and advising timely diplomatic and humanitarian interventions have the potential to save lives and prevent suffering [8]. Yet predictive performance can be severely compromised if ethical and governance questions are neglected and a deep understanding of the underlying data, the associated statistical properties, and the limitations of these methods is lacking [13]. Informal discussions with practitioners engaged in the sensitive domain of conflict early warning reveal pervasive skepticism about enthusiasm for big-data models, concern that interest is often motivated by the prestige associated with the possibility of predicting conflict at truly large scales rather than by instrumental relevance, and the view that current predictive performance remains inadequate [5]. The rapid proliferation of early-warning models using both traditional and unstructured data attests to a concurrent thirst for knowledge about the extent to which any of these models, data sources, or approaches are informative about the future of conflict [7]. Insights gathered from the existing literature are distilled to illuminate opportunities and challenges associated with adapting state-of-the-art big-data analytics to conflict prediction and situate them within a broader methodological landscape [13]. The result is a mounting body of evidence, meta-analytic comparisons, and statistical tests demonstrating that big-data sources enable reasonable short-term prediction of large-scale conflicts, notably civil war, at broad geographic granularity, while guidance on other potential applications remains scarce [17].

Regional Applications and Lessons Learned

Six case studies illustrate how emerging efforts to apply big data technologies for conflict prediction are developing in diverse socio-political contexts and address different governance issues [15]. They preview analytical findings that will be reported in full elsewhere [17].

Comparative Analyses of Predictive Performance

Big data analytics has opened up new opportunities for generating insightful predictions. Even so, uncertainty remains regarding the ability of many analytical approaches to extract meaningful and actionable information from vast data streams [13]. An analysis of Big Data approaches to the prediction of state-based conflict reveals mixed findings concerning predictive performance [14]. In one study, a logistic regression model fitted on national-level conflict data and trained to detect new, imminent conflicts or conflict escalation was found to be no more accurate

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

than random prediction [18]. Nevertheless, 23 different models addressing various facets of national conflict predicted various forms of future conflict better than random prediction [3]. Geographically, models that targeted instability in specific African states received mixed assessments. Despite the prevailing idea that countries like Sudan and South Sudan were modeling candidates, the model did not select them. Speculation on the reasons suggested that the countries might already be in a "low-stability" equilibrium, attracting less attention from predictive analytics; or the historical data could have been of insufficient length to support an accurate prediction, with models requiring a decade or more of history poorly predicting outcomes requiring only one or two years of data[21]. Yet the study concluded that prediction-oriented analyses were not isolated to countries with high conflict levels [22].

Methodological Rigor and Reproducibility

Although numerous analyses explore the quality and validity of early-warning systems focused on violent conflict, remarkably few of these investigations examine the underlying methodologies and processes that generate the predictive models [9]. Of those that do, the overwhelming majority of prospective studies focus on fairness, bias, or accuracy, while neglecting comparable discussions of methodological rigor or reproducibility [10]. A systematic review of early-warning systems for violent conflict indicates that model interpretability, a crucial factor in understanding the relationship between input variables and projected outcomes, receives limited attention [4]. None of the papers employs process tracing to investigate the rationale behind variable selection, thus permitting public scrutiny of any biases that may compromise validity or reliability [5]. The absence of formalised criteria governing model selection and evaluation likewise hampers the assessment of alternative approaches [6].
Many available reforms improve the systematic consideration of these and other aspects of reproducibility through the adoption of established frameworks [17]. Despite substantial steps toward open science elsewhere, the burden of proof remains disproportionately high in conflict prediction, owing to entrenched barriers to knowledge exchange and multi-investigator collaboration [18]. Recent studies proposing large-scale dissemination of models have yet to consider the permissibility of access to sensitive datasets in data-rich/poor settings. Reproducibility remains a priority across other domains of data science, and numerous initiatives extend standards and guidelines to the specific context of early-warning systems for violent conflict [19]. Building on established conventions that focus on parameter-sharing and more comprehensive materials, the process of "reproducible dissemination" conveys a richer spectrum of insights than conventional "reproducibility" through the publication of models and inputs [20].

Data Quality Assurance

The integrity, security, provenance, and appropriateness of data must be guaranteed with regard to studies on data and algorithms [11]. Important dimensions of data quality are identified for health data, accuracy and completeness being the leading ones [19]. Further, the phenomenon of unregulated data sporadically reaching and influencing key decisions constitutes a considerable threat.

Model Interpretability and Explainability

The interpretability and explainability of algorithms are crucial for responsible deployment. Data-driven models can amplify existing imbalances in society, reproduce discriminatory behaviours, and create new inequities [13]. Countries with historical injustices such as caste, racial, and ethnic discrimination have an explicit obligation to consider bias and discrimination in algorithmic systems and ensure that systematically disadvantaged groups are not further victimised [20]. Model interpretability is a key component of responsible governance because it provides essential insight into how the data used to train a model, and the design of the model itself, can lead to biased algorithmic outputs [21]. In the precision of algorithms informs decision-making in sectors such as housing, credit, healthcare assistance, and employment, algorithms can inadvertently amplify historical imbalances [21]. There have been documented cases of algorithms exhibiting racist or sexist biases, which have sometimes surfaced only after the model has been deployed [13]. Recurrent discrimination against historically disadvantaged groups or populations can lead to that group becoming even more disadvantaged, or silenced altogether [22].

Reproducibility Standards and Open Science

Preventing armed conflict depends on predicting the complex and interconnected processes that lead to violence. In particular, social media has been suggested as a way to understand the social interactions that underpin these processes [10]. The vast amounts of data available can be examined by machine learning techniques and lead to compelling insights about how violence spreads through societies [11]. These techniques are being increasingly adopted by organizations seeking to predict violent conflict. Yet they also carry considerable risks [12]. Machine learning approaches to conflict prediction rely on observational data. The datasets used in machine learning methods have thus far rarely been made publicly available, making it difficult to judge the quality of the data or the robustness of the predictions [13]. High standards of reproducibility could help to address these issues. Such standards encourage researchers to publish both their data and the code used in their analyses [14]. Such resources allow other researchers to conduct independent checks that the reasoning matches the conclusions and to explore alternative approaches. The research community concerned with violent conflict prediction has been

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

slow to adopt such practices. Better data and wider sharing of datasets will enhance scrutiny of this important area [12].

Practical Implications for Policy and Practice

Early-warning systems serve as essential tools in safeguarding the international community from emerging threats and preparing timely responses [3]. As the potential danger of conflict escalation looms, these systems track relevant events, recall prior occurrences, and issue warnings accordingly [4]. In this light, big data technologies offer exciting opportunities for improving the timeliness and accuracy of early-warning systems. By leveraging widely available real-time datasets, existing systems can enhance their predictive capabilities [3]. However, deploying systems that make predictions based on extensive worldwide datasets raises significant ethical concerns [6]. Considering the surrounding ethical dilemmas, several fundamental parameters define the acceptable deployment of conflict early-warning systems relying on big data [6]. First, such systems must maintain high levels of accuracy. Refugees, diplomats, humanitarian organizations, and government officials regularly rely on the outputs of early-warning systems to predict violent outbreaks. If such systems produce misleading or incorrect outputs, they risk generating unintended consequences, such as the aggravation of conflict or unwarranted military involvement [7]. This in turn increases humanitarian suffering in large areas of the world. Second, as highlighted in the preceding section, implementing sufficient governance mechanisms assumes critical importance in balancing a society's value of individual privacy against the societal benefits of preventing costly conflicts. Third, safeguarding observance of ethical principles during development and deployment stands as a prerequisite towards proper governance [11]. Prioritizing ethical imperatives allows other critical aspects namely, accuracy and governance, to emerge and reinforce one another. As such, big data analytics applied to conflict early-warning systems at the global scope of the early-warning platform provides important opportunities for advancing the prevention of, and response to, violence [12].

Early-Warning in Diplomacy and Humanitarian Action

Early warning enhances diplomatic and humanitarian efforts to avert and mitigate violent conflict, providing time to intervene before armed violence breaks out [19]. Sophisticated big-data tools and predictive analytics can facilitate the analysis of thousands of early-warning signals. Some organizations are using these tools to act on early warnings received by local informants before a situation escalates fatally [18]. Judicial and customary law prohibits the publication of such information that could endanger lives. Modelers have bypassed this problem by predicting the likelihood of violence preceding an event that would make such information fatal to share, without endangering informants [16]. Such estimates furnish strategic foresight to adjust activities, but many obstacles impede timely interventions nonetheless [3].

Resource Allocation and Crisis Preparedness

Conflict Early-Warning with Big Data: Ethics, Accuracy, and Governance [20]. The use of big data analytics in conflict early warning provides opportunities for improving situation awareness, but it is not without risks. Effective data integration requires a framework for safeguarding data rights and enabling responsible data sharing, without which the utility of big data is severely limited [23]. Individual country assessments influence global resource allocation, including the distribution of humanitarian assistance and the dispatch of peacekeepers, and crises or increases in conflict risk in one country can generate overlaps in resource requirements across neighbouring countries [24]. Decision makers routinely faced with competing demands for limited resources can consider not only a country's individual risk signal but also the estimated risk levels of a country's neighbours. Crises that escalate or persist signal a need for urgent attention; a situation that escalates unexpectedly warrants high-level scrutiny and preventive power, while a country at crisis levels just below the threshold requires monitoring[25].

Challenges, Limitations, and Future Directions

Conflict prediction models remain plagued by significant challenges that inhibit scalability and generalizability across geographic and temporal contexts [4]. Deployment experiences often reveal unexpected hazards 2. Existing frameworks lack the needed comprehensiveness [11]. Efforts typically focus on mechanistic improvements for accuracy rather than sustaining the equilibrium between accuracy, ethics, and governance. Adversarial actors can compromise large datasets by injecting deliberate noise [12]. Scales of big data architectures skew toward high-throughput processing, neglecting fine-grained analyses such as early warning. High-density conflict areas direct attention disproportionately, with overlooking broader areas leading to missed risks [13]. Time-dependent models often fall short because of incomplete or intermittent source data. Single-disaster predictions, such as nonconsecutive political regime changes, amplify these limitations. Missing, noisy, or ambiguous signals stymie advances [14]. Large datasets do not automatically ensure generalizable methods; adaptive reengineering remains essential. Prospective empirical assessments alongside retrospective evaluations will remain critical yet generally unavailable [15]. Predictive accuracy remains contingent upon proper institutional forms and investment. Resourcing independent of purely technical improvements constitutes a fundamental prerequisite [16].

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

Uncertainty, Noise, and Adversarial Exploitation

Conflict early-warning systems (CEWS) based on big data analytics can generate signals about potential crises, thereby creating a sensitive information situation in which various actors, including governments, non-governmental organisations, and commercial enterprises seek to exploit the insights available [16]. CEWS outputs are largely probabilistic estimates, potentially leading to the spread of misinformation or disinformation by parties wishing to undermine confidence in a system's outputs or in the integrity of a data provider [17]. These concerns are familiar from the early years of the pandemic, when inaccurate, misleading or unverified information about the COVID-19 virus circulated widely [18]. CEWS based on big data thus face a credibility challenge [19], arising from uncertainty, noise, and adversarial exploitation. The trustworthiness of an output (and, therefore, of the entire modelling process) depends on the fidelity of data collection and the choice of methods, parameters, and procedures across multiple temporal and spatial scales [20].

Scalability and Global Applicability

Current approaches in Big Data conflict forecasting tend to focus on a specific region (e.g., a country or a sub-national region such as a province or a city) [25]. Other geographic entities are usually ignored; scales below established precision thresholds become exempt from all monitoring; and monitoring does not cover geographically dispersed threats against transnational actors [24]. Questions of global coverage arise. The capacity of a given Big Data system to compute predictions for a new region or scale unobtrusively engages the ethical concerns highlighted above [24]. A systematic exploration of theoretical drawing-board conditions that would license expansive responsibilities could help precipitate more precise characterizations of future participation objectives [12].

Interdisciplinary Collaboration and Capacity Building

Collaborative projects involve a variety of disciplines and skills that address different aspects of the same problem. They benefit from quasi-permanent contacts with social scientists, policymakers, and journalists [26]. Scientists and practitioners from mathematics, computer science, political science, and security studies engaged in early exercises [24]. They contributed cyber-security, social-media analysis, population modelling, conflict-cause analysis, and evaluation of biases arising in full-text corpus studies of socio-political unrest [17]. Addressing social justice, diversity, and the need for responsible use and sharing of data, the network is committed to connecting with various disciplines, practitioners, and institutions [26]. Insecurity, mistrust, and associated conflicts confront urban habitats, leading to alternative data collection and usages. Capacity-building for data-inclusive governance is essential for implementation of the New Urban Agenda and monitoring of the Sustainable Development Goals [27-30].

CONCLUSION

This study has demonstrated that conflict early-warning systems powered by big data analytics hold significant promise for improving the prediction and prevention of violent conflicts. By leveraging vast and diverse data sources alongside advanced analytical techniques, these systems can provide timely and actionable insights that support diplomatic, humanitarian, and policy interventions. However, the findings reveal that the effectiveness of such systems cannot be evaluated on predictive accuracy alone. Instead, accuracy, ethics, and governance must be understood as deeply interconnected pillars that jointly determine the legitimacy and impact of early-warning frameworks. The analysis underscores that ethical challenges particularly those related to privacy, bias, consent, and transparency pose substantial risks if left unaddressed. Biased datasets and opaque algorithms can reinforce existing inequalities, misrepresent vulnerable populations, and ultimately undermine trust in predictive systems. Similarly, governance deficits, including weak accountability structures and inadequate regulatory oversight, can lead to misuse, politicization, or harmful deployment of predictive insights. These risks are further compounded by technical limitations such as data quality issues, model uncertainty, and susceptibility to adversarial manipulation. Empirical evidence suggests that while big data approaches can achieve reasonable short-term predictive performance, their reliability remains uneven across contexts and regions. This variability highlights the need for stronger methodological rigor, improved reproducibility standards, and more transparent model design. Moreover, effective deployment requires inclusive governance frameworks that engage diverse stakeholders ranging from governments and international organizations to civil society and local communities, in decision-making processes. Looking forward, the development of conflict early-warning systems must prioritize interdisciplinary collaboration, capacity building, and the integration of ethical safeguards throughout the system lifecycle. Future research should focus on enhancing model interpretability, addressing structural biases, and exploring scalable approaches that maintain sensitivity to local contexts. Ultimately, harnessing the full potential of big data for conflict prevention depends on striking a careful balance between technological innovation and responsible governance. Only through such an approach can early-warning systems contribute meaningfully to global peace, security, and sustainable development.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

REFERENCES

1. Brecke P. Conflict alert systems and conflict prevention. Atlanta (GA): Georgia Consortium on Negotiation and Conflict Resolution; 1996 Nov. Working Paper No.: 96-4.
2. Jani K. The promise and prejudice of big data in intelligence community. arXiv [Preprint]. 2016. arXiv:1610.08629. doi:10.48550/arXiv.1610.08629.
3. Ogenyi FC, Ugwu CN, Ugwu OP. Securing the future: AI-driven cybersecurity in the age of autonomous IoT. Frontiers in the Internet of Things. 2025 Sep 4;4:1658273.
4. Duursma A, Karlsrud J. Predictive peacekeeping: strengthening predictive analysis in UN peace operations. Stability: International Journal of Security and Development. 2019;8(1):1. doi:10.5334/sta.663.
5. Vayena E, Gasser U, Wood A, O'Brien DR, Altman M. Elements of a new ethical framework for big data research. Wash Lee Law Rev Online. 2016;72(3):420-441.
6. Oswald C, Ohrenhofer D. Click, click boom: using Wikipedia data to predict changes in battle-related deaths. Int Interact. 2022;48(4):678-696. doi:10.1080/03050629.2022.2061969.
7. Ogenyi FC, Ugwu CN, Ugwu OP. A comprehensive review of AI-native 6G: integrating semantic communications, reconfigurable intelligent surfaces, and edge intelligence for next-generation connectivity. Frontiers in Communications and Networks. 2025 Sep 30;6:1655410.
8. Hutchinson B, Rostamzadeh N, Greer C, Heller K, Prabhakaran V. Evaluation gaps in machine learning practice. In: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency; 2022 Jun 21-24; Seoul, Republic of Korea. New York (NY): ACM; 2022. p. 1859-1876. doi:10.1145/3531146.3533233.
9. Schuler A, Bhardwaj A, Liu V. Performance metrics for intervention-triggering prediction models do not reflect an expected reduction in outcomes from using the model. arXiv [Preprint]. 2020. arXiv:2006.01752. doi:10.48550/arXiv.2006.01752.
10. Jiya T. Ethical implications of predictive risk intelligence. ORBIT J. 2019;2(2). doi:10.29297/orbit.v2i2.112.
11. Chukwudi OF, Nneoma UC, Paul-Chima UO. A narrative review of power allocation strategies and successive interference cancellation enhancement in NOMA based 5G and future wireless networks. Discover Internet of Things. 2025 Oct 17;5(1):109.
12. Tolan S. Fair and unbiased algorithmic decision making: current state and future challenges. arXiv [Preprint]. 2019. arXiv:1901.04730. doi:10.48550/arXiv.1901.04730.
13. Pombal J, Cruz AF, Bravo J, Saleiro P, Figueiredo MAT, Bizarro P. Understanding unfairness in fraud detection through model and data bias interactions. arXiv [Preprint]. 2022. arXiv:2207.06273. doi:10.48550/arXiv.2207.06273.
14. Hand DJ. Aspects of data ethics in a changing world: where are we now? Big Data. 2018;6(3):176-190. doi:10.1089/big.2018.0083.
15. Leonelli S. Locating ethics in data science: responsibility and accountability in global and distributed knowledge production systems. Philos Trans A Math Phys Eng Sci. 2016;374(2083):20160122. doi:10.1098/rsta.2016.0122.
16. Ho CWL, Ali J, Caals K. Ensuring trustworthy use of artificial intelligence and big data analytics in health insurance. Bull World Health Organ. 2020;98(4):263-269. doi:10.2471/BLT.19.234732.
17. Hawn Nelson A, Zanti S. Four questions to guide decision-making for data sharing and integration. Int J Popul Data Sci. 2023;8(4):2159. doi:10.23889/ijpds.v8i4.2159.
18. Hristova T, Magee L, Kearney E. Academic institutions in multilateral data governance: emerging arrangements for negotiating risk, value and ethics in the big data economy. arXiv [Preprint]. 2023. arXiv:2301.12347. doi:10.48550/arXiv.2301.12347.
19. Dabab M, Craven R, Barham H, Gibson E. Exploratory strategic roadmapping framework for big data privacy issues. In: 2018 Portland International Conference on Management of Engineering and Technology (PICMET); 2018 Aug; Honolulu, HI. IEEE; 2018. p. 1-9. doi:10.23919/PICMET.2018.8481834.
20. Tanweer A, Bolten N, Drouhard M, Hamilton J, Caspi A, Fiore-Gartland B, et al. Mapping for accessibility: a case study of ethics in data science for social good. In: Proceedings of the Bloomberg Data for Good Exchange Conference; 2017 Sep 24; New York, NY. 2017.
21. Lepri B, Staiano J, Sangokoya D, Letouzé E, Oliver N. The tyranny of data? The bright and dark sides of data-driven decision-making for social good. arXiv [Preprint]. 2016. arXiv:1612.00323. doi:10.48550/arXiv.1612.00323.
22. Juddoo S, George C. Discovering the most important data quality dimensions in health big data using latent semantic analysis. In: 2018 International Conference on Advances in Big Data, Computing and

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

Data Communication Systems (icABCD); 2018 Aug 6-7; Durban, South Africa. IEEE; 2018. doi:10.1109/ICABCD.2018.8465129.
23. John-Mathews JM. Some critical and ethical perspectives on the empirical turn of AI interpretability. Technol Forecast Soc Change. 2022;174:121209. doi:10.1016/j.techfore.2021.121209.
24. Yoon CH, Torrance R, Scheinerman N. Machine learning in medicine: should the pursuit of enhanced interpretability be abandoned? J Med Ethics. 2022;48(9):581-585. doi:10.1136/medethics-2020-107102.
25. Delcaillau D, Ly A, Papp A, Vermet F. Model transparency and interpretability: survey and application to the insurance industry. Eur Actuar J. 2022;12(2):443-484. doi:10.1007/s13385-022-00328-y.
26. Lee CC, Comes T, Finn M, Mostafavi A. Roadmap towards responsible AI in crisis resilience management. arXiv [Preprint]. 2022. arXiv:2207.09648. doi:10.48550/arXiv.2207.09648.
27. Nickel PJ. The ethics of uncertainty for data subjects. In: Krutzinna J, Floridi L, editors. The ethics of medical data donation. Cham: Springer; 2019. p. 55-74. doi:10.1007/978-3-030-04363-6_4.
28. Ryan M, Antoniou J, Brooks L, Jiya T, Macnish K, Stahl BC. Technofixing the future: ethical side effects of using AI and big data to meet the SDGs. In: 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation; 2019 Aug 19-23; Leicester, UK. IEEE; 2019. p. 335-341. doi:10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00101.
29. Evans Harris N. Data-driven collective impact: driving social change as a community [conference presentation]. In: 2018 ADRF Network Research Conference; 2018 Nov 1. 2018.
30. Koseki SA. Globalizing the digital: a cross-cultural framework for the ethics of operationalizing big data [poster presentation]. In: Swiss Inter- and Transdisciplinarity Day 2018; 2018 Nov 15; EPFL, Lausanne. 2018.

CITE AS: Kato Nabirye H. (2026). Conflict Early-Warning with Big Data: Ethics, Accuracy, and Governance. Research Output Journal of Arts and Management 5(1):1-10.
https://doi.org/10.59298/ROJAM/2026/5111000

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited