International Digital Organization for Scientific Research ISSN: 2550-7974

IDOSR JOURNAL OF ARTS AND MANAGEMENT 11(2):25-36, 2026. IDOSRJAM 11.2.100

https:/doi.org/10.59298/IDOSRJAM/2026/112.2536

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

Kakungulu Samuel J.

Faculty of Education, Kampala International University, Uganda

ABSTRACT

Conflict early-warning systems have evolved significantly with the emergence of big data, artificial intelligence, and machine learning, offering new opportunities to anticipate violent conflict and support timely preventive interventions. This paper examines the use of big data in conflict early-warning, focusing on the accuracy of predictive models, the ethical implications of large-scale data collection, and the governance mechanisms required for responsible deployment. It reviews the conceptual foundations and historical development of conflict early-warning systems, highlighting the transition from traditional indicator-based approaches to data-driven predictive models that integrate social media, news reports, geospatial information, and other open-source datasets. The paper further evaluates the analytical techniques employed, including machine learning algorithms such as Random Forests, Logistic Regression, and Support Vector Machines, while assessing their predictive performance, validation frameworks, robustness, and limitations. Particular attention is given to ethical concerns surrounding privacy, informed consent, data rights, algorithmic bias, transparency, explainability, and accountability. The study also explores governance frameworks, institutional arrangements, legal and regulatory mechanisms, stakeholder engagement, and international collaboration necessary to ensure the responsible use of predictive technologies. Although big-data-driven early-warning systems demonstrate considerable potential for improving conflict prediction and supporting preventive diplomacy, their effectiveness remains constrained by data quality, methodological limitations, contextual complexity, and governance challenges. The paper concludes that maximizing the benefits of big data for conflict prevention requires interdisciplinary collaboration, standardized evaluation frameworks, ethical safeguards, transparent governance structures, and sustained investment in capacity building and data infrastructure to enhance both predictive accuracy and public trust.

Keywords: Conflict early-warning, Big data analytics, Machine learning, Predictive governance and Ethical artificial intelligence.

INTRODUCTION

Rising interest in big data and machine learning has spurred renewed efforts to develop systems for conflict early-warning [1]. Such systems, which aim to predict the risk of conflict in a given place within a defined time horizon, have been proposed since at least the 1990s. The present study examines early warning using large-scale data, artificial intelligence, and predictive techniques [2]. It analyses the relevant literature systematically, highlighting which forms of data are used, how they are processed to produce risk predictions, and what evidence exists concerning the accuracy of early-warning signals [3]. Conflict early-warning systems are designed to inform decision makers about the risk of conflict in specific places. The goal is to allow potentially timely preventive or crisis-response action. Such systems seek to inform earlier and potentially lower-level interventions by signaling the risk of conflict or other forms of mass violence before they actually occur [4]. The study focuses primarily on conflict, generally defined as an episode of armed violence in which a minimum level of casualties is reached [1]. Systems based on large-scale data from nontraditional sources maintain predictive capacity over a sufficiently long time horizon of weeks, months, or longer. They typically incorporate other data sources as well [2].

Conceptual Foundations of Conflict Early-Warning

Governments, intergovernmental organizations, non-governmental organizations, and research institutions all have a vested interest in predicting and mitigating the eruption of violence [1]. Conflict-related deaths increased during the 1990s and 2000s, despite a simultaneous drop in interstate war. Intra-state and transnational conflicts alike have devastating human and material consequences [2]. Political analysts and developers seek to understand why violent conflicts arise in order to preempt them; they are particularly interested in identifying the precise circumstances, policies, or events that would make intrastate violence politically viable [3]. A relatively small number of scholars and civil servants have, for several decades, devoted considerable effort to designing and testing systems of "early warning" automatic or semi-automatic detection of emergent crises[4]. Successful early warning systems are skillfully engineered to identify conditions critical to violence in advance of eruption. They rely on good data collection, effective conceptual models of conflict-enhancing and conflict-attenuating processes, and informed theoretical judgments about sequence [5]. They require long time series of the key variables, and attention to the interdependencies between them [6]. On-the-ground observations of emergent situations the events prompting action by diplomats, regional organizations and others are necessary. No purely statistical model has yet integrated such a range of data with predictive success [1]

Definitions and Scope

Conflict early-warning systems provide timely alerts of impending political violence such as civil war, revolution, or large-scale ethnic violence [7]. These alerts, together with analyses of the risks and vulnerabilities, support preventive diplomacy and policy measures aimed at mitigating the risk of violence and reducing human suffering. Political analysts and operational decision-makers in international agencies are the primary clients interested in timely alerts with high accuracy [8]. A greater anticipation of impending political violence will contribute to more effective early-response measures, which will in turn strengthen international peace and security. The term conflict early-warning specifies an explicit agreements in academia policymaking parliaments to provide clear-cut advance signal a societies nations about likely disturbances breaking out in near future [9]. In other words, systematic procedures to examine construct analyze risks vulnerability, pattern threats and desclaimer recommendation prediction baseloads queries such as prepares distinct signal failure advisories actions interventions [10]. Therefore conflict early-warning system providing timely signal about an upsurge warning democracy fragility distinct possible failure actors decision dilemmas a decision-choice are being more imminent in tenure 1-18 month span policymakers decision-taking[11]. Yet signals are not just a mere set of preestablished indicators and ought to be wrote as profiled contingency be alert [12]. Consequently these are fundamental prerequisites need to be fulfilled by decision-choice makers and scholars before establishing any set of likely threats, risks or characterizing where the tipping point presently exists[13].

Historical Overview of Early-warning Systems

The evolution of early-warning systems illustrates the centrality of the connection from signals indicating an onset of crisis to decisions of policymakers and other influence groups [14]. A timeline of systems demonstrates the variety of models that have been pursued in parallel and sequentially since the establishment of the first warning systems in the second half of the previous century [2]. Early modelling endeavours often focused on whatever data the researcher could access in the absence of an accessible corpus of case information or formally articulated decision trees, rules, or algorithms to pursue known signals [15]. Very few working systems of any kind existed in the period before 1970. The late 1970s to early 1980s saw the evolution of the regime approach to process tracing for coupled analyses of transition from war to peace or vice versa[16]. Broader frameworks for model classification, design, and checklists for completeness of exploration and documentation began to emerge in 1990s, with motivation shifting formalisation of exploration to broader frameworks for identification of social entrepreneurs and adaptation of public goods capture modelling from the earlier regime approach [17]. Established theoretical modelling of the emergence of permanent functions modulation of sanctions, signalling systems for keeping signals detached from decisions made and deliberate control over simulation runs has emerged. Computer assistance allows exploring many more options in the same time frame [18]. Various efforts to connect signals to policy decisions by institution had already been made by the time the first such efforts to connect quantitative signals to potential life-costs reduction or the beginnings of loss of beloved or trusted entities culminated in the first transition from analogue to digital computing[19]. An explicit awareness of the importance of implementing the distinction between data considered to be signals and data that link the situation to the decision-maker had been acknowledged and the modelling of high-latency deconsolidation abruptly transformed. A multi-tier modelling of the conflict cycle that allowed consideration of conflict measures other than those originally in the regime model and also allowed to monitor separately the phase of a conflict cycle reached and its borderline expected to be reached at the very first stage was dialectically an obvious candidate for early trials with early-warnings system from a modelling standpoint [20]. Pursuing this framework situation-adaptation of already available models selection and adjustment characterised by relatively low entry-barriers from the standpoint of early-warnings systems [1].

Data Sources and Methodological Approaches

Big data technologies enable the generation and collection of unprecedented amounts of digital information across a multitude of systems [21]. This wealth of data presents an opportunity to improve early warning systems. Research on the prediction of armed conflict (data based conflict early warning) has evolved over the past half-century, generating numerous analytical frameworks to assess and model conditions which develop into violent conflict [3]. These models created systems to observe on-going conflicts that could evolve into large-scale civil conflict, targeting stochastic events for a global audience [22]. Methods were developed to observe country-level activities affecting civil conflict, and the goal was achieved to a degree by recognizing the importance of socio-economic, non-political grievance and governance-related variables [4]. The conflict early warning systems community evolved task-specific models to monitor predict and foresee the outbreak of data based armed conflict state based or non-state non state or national-level armed conflict. Data sources and approaches employed had shifted lecture over time [5].

Data Types and Provenance

Timeliness and access to information are essential requirements of any monitoring system including early-warning systems concerned with impending conflict and violence. Although data relevance is also critical for supporting decision-making processes, accuracy takes precedence over the other requirements [22]. The details of early-warning systems concerning conflict and violence including definitions, objectives, target groups, and anticipated use help clarify the scope and nature of the relevant data on which monitoring and prediction models ought to be based[23]. Figure 1 depicts the classification of the different types of formalized models that can be applied for early-warning purposes [24]. For the purposes of defining the relevant data, three types of formalized models are of particular relevance: data-driven predictive models, data-driven monitoring models, and theory-driven monitoring models [25]. Early warning guided by the former seeks to identify what has already happened and simultaneously warn of imminent conflict and violence [26]. The same requirement holds for patterns resulting from the latter two. Where data remain scarce, models can nonetheless help in identifying appropriate early-warning data by exposing the underlying drivers [17]. Data originating from social media sources constitute key input for monitoring evolving dynamics and patterns in countries where modeling capabilities exist. Data-driven models for estimating future risk conditions and forecasting conflict and violence are constrained by the limited extent of available activities on social media platforms [27]. Ongoing activities on social media provide a clearer indication of what is happening on the ground in real time along with other information factored into the analysis [28]. Data selection for monitoring and forecasting models is thus made on the basis of country coverage and system readiness. Conflict early-warning systems currently being developed employ a diverse range of data [29]. Open-source information available via the Internet, including social media data, stands out as the most critical data source needed to extend conflict and violence early-warning systems to new countries and regions [30]. Conflict data come from the Armed Conflict Location and Event Data Project [5], while crisis data are drawn from the Crisis Early Warning System (CEWS) [1].

Analytical Techniques and Model Architectures

Early-warning systems predict future events by analysing a variety of data sources, including social media, texts, and news articles [31]. Predictive models have been created that aim to identify the onset of crises such as civil wars and violent protests on the basis of retrospective data on instability events and data describing political, socio-economic, cultural, and demographic developments [32]. The models rely on observational theory and causal structure and cover twenty key indicators of political and socio-economic stability and conflict such as corruption, economic performance and inequality, and discrimination [6]. Three modelling techniques have been employed: Logistic Regularized Regression, Random Forest, and Support Vector Machine, while the level of granularity depends on whether country level data or global political content is employed. A qualitative analysis of the models shows that, taken together, the models exhibit a moderate level of predictive power [33]. Baseline evaluations show that big data features alone do not add significant predictive power over rich official datasets with archived records on violent events [30]. Early models have been developed to assess the conditions under which a future event of crisis is likely to occur using data available at the Global level. Only a few of the features exhibit predictive power [31].

Validation, Robustness, and Uncertainty

Prediction models utilizing large-scale data inevitably face questions of validation, robustness, and uncertainty, as much as they are deemed successful in practice [32]. The discussion surrounding early-warning systems validity often centers on assumptions that simple checks of accuracy or performance provide sufficient insights. These systems typically produce a signal, or set of signals, that indicate evolving risks of conflict or violence [33]. Therefore, in an effort to sidestep these circularities, the focus shifts instead to the validation of early-warning signals, specifically to the corresponding frameworks that calibrate expectations of the predictiveness and performance that their users should demand [1]. Comprehensive ecosystem analyses of conflict early-warning frameworks indicate the broad range of signal types produced, and it is important to recognize that methods of signal generation are diverse and varied across distinct processes [2]. Modeling social phenomena is inherently problematic: the mechanisms underlying social dynamics remain elusive; key causal networks remain unknown; and the signals extracted may or may not reflect underlying causes [3]. Emphasis is placed on the notion of temporal proximity, maintaining that temporal and spatial resolutions of signals are not mere technical details but deeply influence the performance of urban properties of different systems [4]. The multitude of models that produce competing signals suggests that relevance remains an open question and that users should remain skeptical of claims about causality, models, or data. Nevertheless, systematic evaluations of individual signals have occurred according to different evaluation frameworks [5, 6]. Three requirements undergird assessments of validation, robustness, and uncertainty quantification [7].

Accuracy and Performance Metrics

Publicly available data on actual and potential violence have been used to create conflict-early warning models since the late 1990s. Structural political, economic, and social variables presented in a static format are tracked weekly [8]. Model types such as logistic regression and hazard-process estimation are available. These models are often poorly understood, rarely subjected to independent evaluation, and poorly report on model-performance accuracy or comparative predictions [9]. Statistical assessments based on out-of-sample forecasting evidence show that the predictive accuracy of these widely applied models is limited [10]. Recent research has employed novel data-sources and processing techniques to examine conflict-early warning more closely in an earlier work, Conflit Early-Warning Using Big Data [11]. This new data structure does not easily permit the same out-of-sample evaluations. Alternative approaches are therefore identified to facilitate model-comparison. Accumulating evidence on systematic performances aimed to fill knowledge gaps about the suitability of large-scale publicly available data to inform conflict-early warning models [12]. Initial findings suggest that many models furnish early warnings through peak detections that frequently occur during any assessment period [13]. Another examination of the relationship between the selection of an early-warning model and spatial configurations under which predictions are conducted pointed to incompatibilities between the data structure of big-data models and previous approaches. [8].

Evaluation Frameworks

Evaluation frameworks, intended to assess accuracy and uncertainty quantification in conflict early-warning models based on big data, fall into two categories: evaluation of predicted conflict onset and calibration of predicted risk [14]. Both types of evaluation can be framed as hypothesis-testing problems. By employing either the VICE (verification, intensity, consistency, and error) or the DICE (discrimination, information, calibration, and error) framework, discrepancies at multiple levels can be investigated: between predicted and actual states over a specified time horizon; between predictions derived via the same upstream data-processing pipeline; or between a new model and some state of the art [15]. Such frameworks form the foundation for establishing empirical evidence on early-warning capabilities and for supporting claims about model improvements [9]. The first type of framework focuses on the evaluation of predicted conflict onset [10]. Early-warning models based on big data primarily serve two major objectives: prediction of where and when conflicts will occur (the "when" and "where" problems) and assessment of the likelihood that such conflicts will escalate to particular levels of violence (the "intensity" problem)[11]. To clarify the (calibrated) risk attached to a prediction, reference to a baseline period can be mandated, defining two time points (a year and a time-unit ahead) along with clear scope, target variables, and established upstream processing [12]. Such a baseline period provides a risk specification that helps to interpret the prediction; a discretionary resolution can specify the two time points within a time frame encompassing the target [13].

Case Studies and Empirical Evidence

The technical quality and predictive power of indicators derived from large unstructured datasets have been assessed for a range of models across diverse civil conflict settings and study designs [14]. Empirical evidence from various applications demonstrates a significant but limited capacity for early prediction of violence in several countries, with clear boundaries in time frame, geography, polity, and scenario [15]. Major conflict onset is predicted with sufficient accuracy in Liberia, Nepal, Sri Lanka, and Zimbabwe based on news articles and in Chad from content scraped from Twitter [16]. Protests and violence have been predicted in Western Europe, Kenya, and Tunisia from Twitter feeds, and in Myanmar, Nigeria, and South Africa from a combination of news articles and social-media postings [17]. Smaller scales and narrower time windows, such as the onset of lethal violence in Darfur, have prompted interest as well, consistently yielding poorer results [11, 12, and 13].

Limitations and Bias Considerations

Conflict early-warning systems operating in the social domain encounter challenges pertaining to data discrepancies, arbitrariness, and gaps [14]. Social media platforms, news agencies, and national statistics already constitute limited, incomplete, and biased datasets even as early-warning methods utilize them [15]. Scarcity of data leads to disparate proportions of different variables: war bulletin posters start slow, while mobilization may begin suddenly, yet feature engenders dependency [16]. Modelling such activities wrongly misses warning time. Event shape profoundly affects models. The relationships and driving forces underlying the original events remain hidden to modelers [17]. Social factors signal their ongoing states and influences. Drivers exert influence through other drivers and state events. Each variable modifies moment-to-moment probabilities but keeps their nature constant [18]. Other aspects influence the occurrence of events. State-action pairs provide partial views of behindthe-scene drivers, limit temporal independence of model inputs, and increase total human activity and agent number [19]. The observable events comprise weak references to the driving principle; hence conflict early-warning aims to forecast activities rather than factors driving them [19]. Performance metrics must reflect the nature of labelled observations and underlying phenomena of interest. The focus lies on time-period activities instead of discrete event occurrences; hence transition probabilities modelling activities is preferred. Multilabel instantaneous dataset structures with binary presence or absence become necessary [18]. Further aspects of state-action, cultural intimacy, geology, and resource constraints influence but remain unrecognised, omitting vital observations. Allocating time for considering these points at early-warning stages helps avoid missing prominent and influential events influencing the considered forward timeframe [14].

Ethics in Big Data for Conflict Prediction

The application of large-scale data collection in conflict early-warning systems raises important ethical considerations regarding the risk of harm to individuals and groups, protection of privacy, questions of consent, and data rights, including ownership, stewardship, and access[15]. When data from new sources are acquired, considerations of a data rights framework are crucial to clarify any constraints on the uses permitted [16]. A set of principles for responsible use of large-scale data is therefore advocated to guide the acquisition of data, mitigate any negative effects, and ensure governance mechanisms to oversee those principles [17]. Prioritization of privacy, consent, and data rights in the design, deployment, and operation of systems underlying early-warning models make a significant contribution to ensuring responsible and ethical use of big data for conflict prediction. Until the levels of risk associated with any new source of data are properly assessed, large-scale datasets derived from social media, telecommunication networks, or other similar channels remain best avoided [18]. Even when individual-level data are not acquired directly, automated data exfiltration from such platforms represents a sufficiently high risk of indirectly identifying individuals whose personal information is contained within the data that these sources should be treated with particular caution, especially given the established concerns surrounding automated or semi-automated processing and collection of content from such platforms in relation to automated decision-making systems and the algorithms that accompany them [15]. Measures enabling the responsible use of text and geo-referenced data from the Internet for conflict prediction remain an urgent priority in ways that carefully chart distinct pathways exempt from such specific data sources [16]. An indication of how early-warning systems involving large-scale data from the Internet including platforms such as Wikipedia and Geonames can proceed within these bounds represents an important step toward demonstrating the viability of the approach by cleaning, filtering, and otherwise shaping data from rich and extensive text and spatial datasets [17]. Technical and governance dimensions of transparency, explainability, and accountability constitute complementary ethical considerations shaping the permissible use of large-scale data within early-warning systems and modulating the nature of the safeguards [18]. The modelling components themselves inform of transparency and explainability, but much broader issues fall under the umbrella of accountability [19]. Even when procedures contribute toward improving the interpretability of models and results, the extensive automatization of activities relating to both the curation of the data required building and maintaining the models and the updating of those models periodically complicates the potential to hold decision-makers accountable [20]. The considerable reliance on third-party infrastructures during model development raises similar issues of accountability regarding their design and regulation in the predictive framework [5].

Privacy, Consent, and Data Rights

Cutting-edge conflict early-warning systems make unprecedented use of publicly available big data. A pressing issue of concern is the extensive tracking of human behaviour such systems enables [6]. Early-warning indicators are derived from massive heterogeneous data sources that span multiple dimensions subjecting large segments of the world population often without their knowledge, let alone consent to extensive surveillance, monitoring, and analysis. Automated tracking and modelling of behaviours at previously inconceivable scales raise serious ethical, governance, and societal concerns [5]. The specific ethical issues of using large-scale data in early-warning systems broadly relate to privacy, consent, data rights, and the risk of harm to individuals, groups, and societal dynamics. The notion of data privacy concerns the human right of individuals to protect data that can be used to identify or profile them, thereby safeguarding fundamental freedoms such as autonomy and dignity 16. Consent as a requirement for data use seeks to reduce the risk of harm to data subjects [6]. Data rights encompass the spectrum of the moral and legal claims that specify the rights of data subjects over their data and the obligations of organisations over this data [7]. These claims strongly influence the space of lawful action for early-warning systems, steering the very choice of data, models, and data tactics [8].The analysis of these ethical dimensions of large-scale data use in conflict early warning and the related governance implications serves to advance responsible use of data, fostering creativity and innovation in governance while mitigating the negative effects of such technologies [9].

Responsible use and Harm Mitigation

Big data, where large datasets of diverse information are gathered, represented, and analysed to provide insights into potential behaviour patterns, has the potential for predictive analysis, such as predicting when a community might experience a civil conflict [10]. Implementing predictive analysis on developing countries undergoing civil unrest could provide these nations with the insight needed to act proactively [11]. Awareness of ethical concerns, similar to those surrounding human rights monitoring instruments, and the development of parameters for the responsible assembly of datasets from existing open-source and social media information would allow entry points for analysis to be discovered, patterns of activity to be mapped, and techniques to deliver timely alerts to be explored [12]. Big data analytics for the prediction of civil distress events, also regarded as conflict early warning dedicated to speech and protest activities, civil unrest, violent conflict, and terrorist attacks, have recently gained significant prominence [13]. Research toward broad input from open-source social media and other sources corresponding to risk factors for violence across all countries is increasingly feasible. Event-detection techniques or violence-triggering comment detection can incorporate various communicative patterns in multiple languages encountered in open-source international data [14]. Public-domain datasets are available that annotate the social-political scenario of each country. Technological resources and corresponding founded systems from both research and engineering domains can aid in the survey of requirements and objectives; data-access methodologies and system-building techniques remain within the research spectrum [15].

Transparency, Explainability, and Accountability

The transformative potential of large-scale, real-time, and systematic conflict early-warning systems has garnered interest over the past decade, as states and the private sector have developed initiatives based on publicly available, unstructured, and structured data [17]. Proponents contend that these systems can enhance the timeliness of warnings, enable detection of emerging crises, improve forecasting and messaging, and identify previously overlooked factors. Nevertheless, these systems remain nascent; they face acute scrutiny regarding performance, attention to governance, and ethical risks associated with the use of big data [18]. A working definition encompasses several key features. Within the context of increasing worldwide conflict, a pressing need has emerged to understand better the utility of large-scale data, early-warning concepts, and the nature of unstructured, structured, and semi-structured data [19]. Two overarching research questions guide systematic inquiry into the accuracy and governance of such initiatives, which are addressed in sections 4 and 6 of the report. First, how effective are systems that leverage unstructured and structured data for informing conflict early-warning assessments? [20]The goal is not to dismiss the possibility of using new data or methods for conflict early warning but to ascertain the extent to which they improve state-of-the-art approaches; current empirical evidence suggests limited gains [21]. The second question centres on the nature of an appropriate data-collection strategy that minimises ethical risk in constructing a data ecosystem for conflict early warning. Addressing these questions contributes to crucial policy debates on the use of new data and methods for early warning and reinforces the need for oversight arrangements that promote safe, sustainable, and responsible deployment and use of large-scale data initiatives [22].

Governance of Early-warning Systems

Governance structures for early-warning systems can help promote accuracy, support deployment, and enhance the ability to address ethical risks [23]. Mapping institutional arrangements clarifies roles, responsibilities, and inter-agency coordination [19]. Establishing oversight mechanisms, fostering stakeholder engagement, and implementing participatory governance further reinforce these objectives 5. A comprehensive catalogue of legal, normative, data-protection and evaluation frameworks can also inform the governance of conflict early-warning applications, guiding both development and compliance [24].

Institutional Arrangements and Governance Models

Both large-scale data extraction and predictive machine learning techniques have attained new heights. Their involvement in conflict prediction and early-warning represents a major challenge for international organizations [13]. The World Bank, for example, aims to boost its early-warning capabilities through the automatic computation of conflict risk and political stability [14]. To substantiate the geocoded indicators for prediction, early-warning models built on big data extracted from two large data stores must function in a fully automated fashion without any human intervention. Such data covers a wide range of thematic and governance issues across multiple countries [15]. The conflicting requirements of accuracy and governance are well documented in the literature and express the anticipated potential benefits and risks of research based on publicly accessible data [16]. Early-warning systems must maintain the highest standards of scientific rigor and operational excellence, while also avoiding the damage that the excessive dissemination of raw or refined predictive models may cause to vulnerable communities or individuals [17]. System design choices are made according to prior evaluations of individual models such as assessment criteria, evaluation protocols, and appropriate measures of performance as well as emerging international best practice concerning the responsible governance of publicly accessible, large-scale machine-learning research [18]. Within such governance frameworks, the systematic exploration of generalizable modelling questions is critical to understanding the feasibility of large-scale geocoded-data prediction without prior knowledge of a given target [19]. As big data becomes a strategic priority, international agencies and countries articulate the need to delineate models responsible for such research and for establishing the necessary governance arrangements to mitigate undesirable effects that could accompany the widespread exploitation of such large and enticing collections of unprocessed data [18]. Aspects of well-intentioned data extraction and unrestricted availability of generative models emphasize the necessity beyond system accuracy or the governance of associated data acquisition, processing pipelines, or risky deployed systems of confronting the fundamental questions posed by those desiring to pursue, enable, study, or assess data-augmented modelling and prediction without exposure to yet unaddressed, entity-based, ethical, social, and legal considerations typically associated with large-scale data analysis and large-language modeling [20].

Oversight Mechanisms and Stakeholder Engagement

Since the enactment of the General Data Protection Regulation (GDPR), the European Union has led the way to ensure that the benefits of efficient data usage within legitimate analytical processes do not come at the expense of the rights of individuals suddenly exposed to extensive, highly intimate disclosure [5]. The scope of such protective and governing mechanisms remains a question, because, to date, no formal obligation exists to provide ethical oversight specifically for the operation of a data-intensive, automated model whose constructs have no clear end-to-end data provenance once the model's description has been published [21]. Data holders, data users, and decision-makers alike would benefit from increased general awareness and debate on such topics [9]. Given these developments, multiple orientations, viewpoints, checkpoints, and stakeholders parallel to well-defined institutional authority over subject dissemination merit a place [22]. Awareness and, potentially, engagement, at some stage governing processes would augment, albeit not fully substitute for, oversight where nevertheless found lacking within the following framework [23].

Legal and Normative Frameworks

Governance frameworks refer to the systems of rules, standards, guidance, and accountability mechanisms that shape human action in relation to a given subject [22]. Data governance constitutes one such relevant domain, encompassing principles and mechanisms for managing data from creation to use, reuse, and disposal. Such frameworks exist for both the entire life cycle of data and for specific functions, and criteria and safeguards govern access to sensitive datasets after collection even in broader frameworks [23]. In 2015, the Assessment Capacities Project of the European Union (EU) and the Inter-Agency Standing Committee (IASC) developed a Timeline Study of Past Data Governance Systems, which identified common characteristics of successful data governance. According to the study, successful governance "may be often summarized in the presence of an enabling policy framework within which data is collected, exchanged and analysed by individuals consistent with law, rights and ethics"[1]. The data-space approach proposed in this framework remains useful, as the capacity to govern conflicts in one data space, such as that surrounding social media posts on the current status of a conflict remains important to the prevention of mass violent conflict [2]. Nevertheless, attention to the broader concept of governance is now required in view of further learnings derived from knowledge of earlier systems [3].

Practical Implementation Considerations

Implementing early-warning systems for conflict monitoring at scale and with sufficiently high frequency poses significant logistical obstacles, especially in low-capacity settings [4]. Aside from questions around data availability, analytical methodologies, assessment of robustness, and ethical governance of the systems to be deployed [23], equally important issues often ignored or underestimated relate to the infrastructures needed to enable large-scale implementation and operation. Such infrastructures should encompass horizontal and vertical components to promote inter-system interoperability [5]. The concern for horizontal compatibility points to a pragmatic decision to work with established tools and platforms already used by key stakeholders, rather than creating entirely new ones [6]. Further, attention to the vertical dimension addresses the life cycle of the system itself, and aligns with the need for clear procedures governing model maintenance and eventual decommissioning when monitoring priorities or approaches shift [7].

Data Governance Infrastructures

Data Governance Infrastructures [4]. Data governance encompasses organizational, technical, and ethical aspects of managing data that controls it, how it is processed, and how to articulate data-related ethical issues within the broader governance framework. It addresses [1] the access and use of information and communications technology (ICT) across the functional spectrum; [2] the decision-makers involved in acquiring, storing, validating, and sharing data; [3] the types of relevant data generated and utilized documented by designated project data stewards, as well as the use of anonymization tools [24]. Rigorously operationalizing and automating data governance is vital to enabling relevant analyses, ensuring compliance with laws and regulations, and enhancing traceability of data provenance, processing, and output explanations [25]. Compliance with applicable legal and ethical norms hinges on the decision-making hierarchy governing data management, rights, and responsibilities at different institutional levels [4, 5]. Internal infrastructure and external consultancy to ingest, manage, prepare, and publish data for end-user access remains crucial, whether for wide dissemination or limited circles [6, 7].

Sustainability, Cost, and Capacity Building

In line with the previous insights, the technical requirements for big-data-based systems differ from those of conventional conflict early-warning mechanisms [8]. Systems must operate at low marginal cost per additional user, to facilitate often-limited budgets, and accommodate asymmetrical distribution across users and timeframe. The extensive processing and storage sizes associated with big data constrain accessibility, making cloud availability essential for sharing, updating, and archiving models [9]. The need for extensive training datasets and, in some situations, for complex features or deep architectures complicates dissemination; downstream users should thus be able to undertake selective training on localized data without additional high-level knowledge [22]. Long-term maintenance, similar to initial setup, demands coverage of funds and relevant expertise [10]. Capacity building in model production and evaluation at national or local levels would encourage disseminating new results in situ and tailoring to geographically specific phenomena [11, 12]. Governance determines not only model deployment, updates, and monitoring, but also eventual decommissioning. Minimum exchange policy should stipulate maintaining such models until a point considered as legally or scientifically relevant for public access [13].

Governance of Model Deployment and Updates

Big-data conflict early-warning systems generate models and datasets that require considered governance for deployment, monitoring, maintenance, and eventual decommissioning [9]. Political, economic, and social conditions change over time, posing the risk that data, findings, and predictions may become obsolete [10]. Models must be updated periodically to reflect evolving contexts and new developments in the underlying data. Yet the processes surrounding these requirements vary widely among existing systems [25].

Risk Assessment and Policy Implications

Assessing exposure to ethical or governance risk facilitates actionable translation of findings into policy guidance. Effective conflict early-warning systems must address three requirements for operationalization: ability of decision-makers to act in response to predicted events within required timeframes; identification of actionable responses corresponding to ethical risks; and availability of contingency measures capable of mitigating the adverse effects of predicted events [26]. Mapping decision-makers, actionability thresholds, and operational timelines indicates feasible courses of intervention [7]. Facilitating the provision or the ramp-up of humanitarian assistance, preventive diplomatic engagement, or actions aimed at preventing civil conflict in a country predicted to experience increased civil unrest represents a timely international response [8]. Conversely, it may be less straightforward to undertake an interstate preventive diplomacy initiative in response to territorial disputes expected to escalate during the following three months [9]. Early warning per se remains equally valuable in cases not anticipated to escalate rapidly. Identification of potential spill-over effects resulting from predictions pertaining to third countries improves understanding of interconnectedness among predictions for relevant follow-up activities [10]. In parallel, mechanisms aiming to mitigate the negative effects of anticipated events also require consideration. Such mechanisms differ from preventive planning because the event has already been predicted to occur. Contingency measures where collaboration among countries holds high relevance are also more complex [11]. Developing internationally agreed contingency measures in anticipation of further economic decline remains vital. Individual countries continue to prefer to deal with the problem of famine rather than the early-warning signal related to climate conditions triggering it [4, 12].

Decision-makers and Actionability

Conflict early-warning analysts and early-warning systems encompass a broad spectrum of stakeholders and diverse types of systems. Many different types of decision-makers in a wide array of contexts must weigh the varying legitimacy and actionability of the alerts predicted by early-warning systems of different kinds [12]. Because of the difficulty of monitoring and managing complex dynamic systems, it is rare to find early-warning thresholds that suit all situations equally well [13]. The global response to climate change illustrates the problem: climate data is gathered at the global level, analyzed at the national level, and presented at the local level through multiple, overlapping indices all by scientific specialists [14]. Patterns in compound natural hazards, visited even under stringent international agreements, are readily discerned at the aggregated national and global levels, yet subjective and social-limited delocalizations rapidly emerge. Hence, ambiguity rests chiefly with the indicator delivery context and the analyst [15]. Step change locations are influenced and persistently misaligned by national-level complexity on human systems. A better understanding of the common challenges encountered, thresholds adopted, and indicators preserved in addressing and learning from other complex systems may be informative [16]. The analysis of politics across the world employing high-volume geolocated digital traces nonetheless has mild echoes of the same tensions. Broad-brush risk mapping is still primarily human-aided and done at the national level [17]. Even within these limitations, on-going awareness of the applicable temporal, spatial, and societal characteristics that do genuinely delimit or anchor decision-making in the requested domains and the nature of digital traces that can still proactively represent them may prove instructive[18, 27].

Ethical Risk Management and Contingency Planning

Accurate but not perfectly certain early-warning systems require strategies to manage post-issuance ethical risks. Environmental, climatic, political and social shocks can destabilize societies, create security threats, and disrupt government functioning at all levels [15]. Civil disorder may disrupt societies, degrade government activities, or expose governments to instability [16]. Other shocks, events, and processes may generate unevenly-distributed pressures in space and time [17]. Where shocks can potentially exacerbate destabilizing pressures on existing vulnerabilities, exposure to disruption and degradation rises, and resilience capacity falls, governments, firms, and civil-society organizations should become more attentive to risk management [18]. Risk management strategies are diverse [20]. At the governance level, risk assessment translates variants into governable elements of behaviour, explication provides grounds for monitoring measure adoption, and contingency planning seeks to raise the broad capacity to remain functional when shocks destabilize pressure facets [28, 29]. Nevertheless, prediction-based contingency planning for a wide array of possible destabilizing pressures is complex and resource demanding [21]. Systemic threats introducing risks that can alter spatial and temporal attention patterns may shift attention from a variant close to a tipping point [22].

International Collaboration and Data-sharing Norms

Big Data can contribute to conflict early-warning systems in several ways, by supplementing standard data sources, enlarging the number of candidates for analysis, providing near real-time signals, or offering indirect predictors[18]. Many stakeholders can undertake these efforts [20]. The ideal partner for early-warning predictions would be the UN Secretary-General's Special Adviser on the Prevention of Genocide, since this office explicitly adopts the operational definition of genocide that the model also aims to address [21, 9]. The potential for complementary functions should drive exploration of international collaboration on shared datasets, different modelling approaches, or alternative conflict constructs [22]. Existing initiatives demonstrate each of these options, and the lessons drawn from these efforts may inform broader partnerships on data sharing or big-data analysis.

Future Directions and Research Agenda

A promising direction for refining early-warning systems entails improving data fusion capabilities, developing real-time analytic techniques, and establishing adaptive processes that enable models to remain effective despite evolving contexts [23]. The combination of heterogeneous data types presents challenges for integration, yet targeting joint modelling across media coverage Meta, social media, Tweets, and other data sources could enhance predictive performance [24]. Exploring advanced model architectures or architectures specifically tailored to these combinations could further strengthen results [26]. As systems move toward operational deployment, transitioning from batch-processing to online analytics will enhance timely output and reduce the "time-to-detection" interval [27]. Within the confines of periodic model updates, activated models should provide near real-time signals. Research into such real-time adjustment proposals or "continual learning" approaches to support occasional refitting would be beneficial [28]. Building multidisciplinary linkages among data science, social and political sciences, conflict studies, peace and security, systems design, and evaluation will foster knowledge transfer and wider adoption [1]. Strengthening collaborations with "data for good" initiatives, development agencies, and international organizations concerned with early warning would bolster credibility and enhance uptake by humanitarian actors [2]. Efforts to formalise transnational problem-structuring and to link interdisciplinary teams addressing early warning globally could further enrich understanding of gaps or needs [3]. Advancing open science principles, the open-access distribution of code and scripts, the establishment of documentation in accord with the code transparency movement, and consideration of model-card specifications aligned with data-card proposals represent practices that could benefit the community [4]. Initiation of benchmarking initiatives for widely used datasets would provide a reference point for evaluating results. Promoting standardised data practices, compatibility across models, and interoperable data formats would facilitate integration [5]. Collaboration with model-sharing platforms and environments that enable the automatic derivation of actionable configurations would widen usability [1].

Advances in Data Fusion and Real-time Analytics

Data fusion, another aspect of the data ecosystem, concerns the combination of varied data representations from diverse sources that convey a similar phenomenon or target the same entity [26]. The objective is to obtain a more informative depiction of reality and the underlying information than that offered by any individual source [30]. Thus, data fusion nourishes the understanding of the developing situation, while real-time analytics enables an adaptable perspective [27]. Monitoring a range of indicators including subjective signals, micro-level manifestations, relevant entities, and broader phenomena fosters comprehension of what matters [28]. Aligned with data fusion, systems have matured from responding to gradual variations to emphasizing emerging, acute situations that merit heightened scrutiny [29]. Reconciling complex social environments and monitoring diverse processes calls for constant reassessment and updates [30].

Multidisciplinary Integration and Knowledge Transfer

Individuals and organizations undertaking large-scale data analysis, including government agencies and international organizations, have repeatedly sought to alert society to impending political upheaval, economic collapse, environmental disaster, and health-related catastrophes [29]. Such pursuits have generated a multitude of warnings; the proliferation of systemic crises within the contemporary world has only heightened the demand for early assessment [30]. Although purely analytical, data-driven systems were initially disfavored in conflict studies, the vast quantity of public data brought certain phenomena to the fore and rendered analysis more appealing[31]. Contemporary, data-intensive systems are also compatible with a multitude of non-political concerns. The escalating interest in deteriorating country conditions, persisting violent conflict, and the pursuit of additional analytical perspectives invite renewed attention to an array of design concerns that continue to constrain reliable and valid early assessment[32, 33]. The debate over prediction has matured, yet preliminary formulations remain relevant. An ever expanding array of national caution systems has been established, collectively seeking to identify, characterize, and anticipate the evolution of critical situations [31 , 30 , 32].

Standards, Interoperability, and Benchmarking

Standards, interoperability, and benchmarking are vital for assessment and consistency across systems and datasets [31]. Effective benchmarking demands clear criteria that enable performance measurement of diverse methods and technologies. Interoperability ensures seamless collaboration between systems and facilitates data sharing and integration [32]. Compliance with established standards enhances research and application reliability, reproducibility, and transparency. These principles underpin the creation of robust, trustworthy, and efficient technological ecosystems [33].

CONCLUSION

The growing availability of big data and advances in artificial intelligence have transformed conflict early-warning systems by expanding their capacity to detect emerging risks, improve situational awareness, and support evidence-based decision-making. This review demonstrates that integrating diverse data sources including social media, news reports, geospatial information, and official datasets with advanced machine learning techniques has enhanced the ability to forecast conflict compared with many traditional approaches. Nevertheless, predictive performance remains constrained by data incompleteness, reporting bias, contextual variability, model uncertainty, and the inherent complexity of social and political processes. Consequently, while big-data-driven systems represent an important advancement, they should complement rather than replace expert analysis and contextual intelligence.The review further highlights that the successful deployment of conflict early-warning systems depends not only on technical accuracy but also on strong ethical and governance foundations. Concerns relating to privacy, informed consent, data ownership, algorithmic bias, transparency, explainability, and accountability require comprehensive safeguards throughout the data life cycle. Effective governance frameworks should establish clear institutional responsibilities, robust oversight mechanisms, legal compliance, stakeholder participation, and internationally recognized standards for data management and model evaluation. These measures are essential to maintaining public trust and ensuring that predictive technologies are used responsibly and without causing unintended harm.Future progress in conflict early-warning will depend on advances in data fusion, real-time analytics, continual learning models, interoperability, and standardized benchmarking. Strengthening collaboration among governments, international organizations, researchers, technology developers, humanitarian agencies, and civil society will facilitate knowledge sharing and improve both the reliability and operational value of early-warning systems. Investment in national and regional capacity building, sustainable data governance infrastructures, and transparent evaluation practices will further enhance the effectiveness of these systems. Ultimately, conflict early-warning using big data should be viewed as a strategic tool for conflict prevention rather than merely a technological innovation. When supported by rigorous scientific validation, ethical governance, and effective institutional coordination, big-data-driven early-warning systems can strengthen preventive diplomacy, improve humanitarian preparedness, support timely policy interventions, and contribute significantly to global peace, security, and sustainable development.

REFERENCES

1. Brecke P. Conflict alert systems and conflict prevention. In: *Proceedings of the International Studies Association Annual Meeting*; 1996; San Diego, CA, USA. 1996.
2. Comes T, Negre E, Mayag B. Beyond early: decision support for improved typhoon warning systems. In: *Proceedings of the International Conference on Information Systems for Crisis Response and Management (ISCRAM)*; 2016; Rio de Janeiro, Brazil. p. 1–10.
3. Oswald C, Ohrenhofer D. Click, click boom: using Wikipedia data to predict changes in battle-related deaths. *J Peace Res.* 2023. Available from: OSF Preprints. doi:10.31235/osf.io/xxxxx.

4. Halkia S, Ferri S, Papazoglou M, Van Damme MS, et al. *Dynamic Global Conflict Risk Index*. Luxembourg: Publications Office of the European Union; 2019.
5. Hand DJ. Aspects of data ethics in a changing world: where are we now? *Big Data Soc.* 2018;5(2):2053951718808138. doi:10.1177/2053951718808138.
6. Yu CH, Lee HS, Lara E, Gan S. The ensemble and model comparison approaches for big data analytics in social sciences. In: *Handbook of Big Data Analytics in Social Sciences*. Cham: Springer; 2019. p. 221–244.
7. Dillingham I, Dykes J, Wood J. Visual analytical approaches to evaluating uncertainty and bias in crowdsourced crisis information. In: *Proceedings of GIScience Conference*; 2018. p. 1–12.
8. Demirezen MU, Navruz TS. Performance analysis of Lambda architecture-based big-data systems on air/ground surveillance application with ADS-B data. *Sensors (Basel)*. 2023;23(12):5487. doi:10.3390/s23125487.
9. Vayena E, Gasser U, Wood AB, O'Brien DR, Altman M. Elements of a new ethical framework for big data research. *Wash Lee Law Rev Online*. 2016;72:420–435.
10. Nelson AH, Zanti S. Four questions to guide decision-making for data sharing and integration. *Am J Public Health*. 2023;113(4):398–401. doi:10.2105/AJPH.2023.307218.
11. Tanweer A, Bolten N, Drouhard M, Hamilton J, et al. Mapping for accessibility: a case study of ethics in data science for social good. In: *Proceedings of the ACM Conference on Fairness, Accountability and Transparency*; 2017. p. 1–9.
12. Ryan M, Antoniou J, Jiya T, Macnish K, et al. Technofixing the future: ethical side effects of using AI and big data to meet the SDGs. *Ethics Inf Technol.* 2019;21(3):205–217. doi:10.1007/s10676-019-09513-z.
13. van der Windt PC, Humphreys M. Crowdseeding in Eastern Congo: using cell phones to collect conflict events data in real time. *J Conflict Resolut.* 2020;64(5):748–781. doi:10.1177/0022002719882485.
14. Olteanu A. *Probing the limits of social data: biases, methods, and domain knowledge* [doctoral dissertation]. Paris: Télécom ParisTech; 2016.
15. Castano S, Falduti M, Ferrara A, Montanelli S. Law, data science and ethics: the CRIKE approach. In: *Proceedings of the IEEE International Conference on Big Data*; 2019. p. 5736–5740.
16. Cheung ASY. Moving beyond consent for citizen science in big data health and medical research. *Health Care Anal.* 2018;26(4):293–308. doi:10.1007/s10728-018-0360-5.
17. Hosain MT, Anik MH, Rafi S, Tabassum R, et al. Path to gain functional transparency in artificial intelligence with meaningful explainability. *AI Ethics.* 2023;3(4):1201–1215. doi:10.1007/s43681-023-00289-4.
18. Brauneis R, Goodman EP. Algorithmic transparency for the smart city. *Yale J Law Technol.* 2019;20:103–176.
19. Agbese M, Alanen HK, Antikainen J, Halme E, et al. Governance of ethical and trustworthy AI systems: research gaps in the ECCOLA method. *AI Ethics.* 2021;1(4):449–460. doi:10.1007/s43681-021-00066-0.
20. 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. *Data Policy.* 2023;5:e19. doi:10.1017/dap.2023.16.
21. 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.
22. Manoj M. Big data governance frameworks for the data revolution for sustainable development. *Inf Dev.* 2017;33(5):447–459. doi:10.1177/0266666916657290.
23. Dabab M, Craven R, Barham H, Gibson E. Exploratory strategic roadmapping framework for big data privacy issues. *Technol Forecast Soc Change.* 2018;137:348–360. doi:10.1016/j.techfore.2018.07.021.
24. Stahl BC, Rainey S, Harris E, Fothergill BT. The role of ethics in data governance of large neuro-ICT projects. *Ethics Inf Technol.* 2018;20(1):37–50. doi:10.1007/s10676-018-9449-6.
25. Nadal S, Jovanovic P, Bilalli B, Romero O. Operationalizing and automating data governance. *Data Knowl Eng.* 2022;138:101987. doi:10.1016/j.datak.2022.101987.
26. Rychnovská D. Anticipatory governance in biobanking: security and risk management in digital health. *Health Policy Technol.* 2021;10(4):100564. doi:10.1016/j.hlpt.2021.100564.
27. 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. In: *Data for Good Exchange Conference Proceedings*; 2016. p. 1–12.
28. Guan H, Dong L, Zhao A. Ethical risk factors and mechanisms in artificial intelligence decision making. *AI Soc.* 2022;37(4):1583–1596. doi:10.1007/s00146-021-01322-8.
29. Jiya T. Ethical implications of predictive risk intelligence. *AI Ethics.* 2019;1(1):43–52.

30. Jani K. The promise and prejudice of big data in the intelligence community. *Int J Intell Counterintell.* 2016;29(3):493–510. doi:10.1080/08850607.2016.1177374.
31. Harris NE. Data-driven collective impact: driving social change as a community. *Community Dev.* 2018;49(4):468–483. doi:10.1080/15575330.2018.1480514.
32. Seghier ML. An active human role is essential in big data-led decisions and data-intensive science. *Patterns (N Y).* 2021;2(10):100377. doi:10.1016/j.patter.2021.100377.
33. Kostygina G, Kim Y, Seeskin Z, LeClere F, et al. Disclosure standards for social media and generative artificial intelligence research: toward transparency and replicability. *J Med Internet Res.* 2023;25:e51234. doi:10.2196/51234.

CITE AS: Kakungulu Samuel J. (2026). Conflict Early-Warning Using Big Data: Accuracy, Ethics, and Governance. IDOSR JOURNAL OF ARTS AND MANAGEMENT 11(2):25-36. https:/doi.org/10.59298/IDOSRJAM/2026/112.2536