



Research Output Journal of Arts and Management 5(1):26-32, 2026

ROJAM Publications

PRINT ISSN: 1115-6112

<https://rojournals.org/roj-art-and-management/>

ONLINE ISSN: 1115-9065

Page | 26

<https://doi.org/10.59298/ROJAM/2026/512632>

Humanitarian Innovation: Drones, Biometrics, and Unintended Harms

Asiimwe Kyomugisha T.

Faculty of Business, Kampala International University, Uganda

ABSTRACT

Humanitarian innovation increasingly relies on advanced technologies such as drones and biometric systems to enhance the efficiency and effectiveness of aid delivery. While these tools offer significant operational benefits including improved logistics, real-time data collection, and secure identification of beneficiaries they also introduce complex ethical, legal, and social challenges. This study examines the interplay between drones, biometrics, and unintended harms within humanitarian contexts. Drawing on existing literature and case-based insights, it highlights how technological interventions may inadvertently generate risks related to privacy violations, surveillance, bias, dependency, and the erosion of humanitarian principles such as neutrality and independence. The analysis further explores how these technologies reshape power dynamics between humanitarian actors and affected populations, raising concerns about accountability, consent, and governance. While drones facilitate rapid response and access to remote areas, and biometrics improve aid targeting and fraud prevention, both systems carry the potential for misuse and long-term harm if inadequately regulated. The study concludes that humanitarian innovation must be guided by robust ethical frameworks, participatory governance, and context-sensitive implementation strategies to balance technological benefits with the protection of human dignity and rights.

Keywords: Humanitarian Innovation, Drones in Humanitarian Action, Biometric Technologies, Unintended Harms and Data Ethics and Governance.

INTRODUCTION

Humanitarian action increasingly engages newer digital and technological interventions to solve emerging operational needs and risks [1]. Such humanitarian innovation generates new opportunities, carries associated risks, and entails the possibility of unrecoverable, unintended harm [2]. Within this context, this study examines how drones, biometrics, and unintended harms relate within humanitarian innovation. The drone domain encompasses diverse uses, operational challenges, and relevant ethical and legal debates. The biometrics domain spans aid delivery, data protection, empowerment, governance, privacy, social custom, and bias. Unintended harms cover security, dependence, social dynamics, and accountability [3]. General understanding of humanitarian action drives consideration of the narrower notion of humanitarian innovation. Humanitarian action denotes “the response to... human suffering” [1]. Humanitarian grounded “in the promotion and protection of human life and health and the preservation of human dignity derives its contours from the principles of humanity, neutrality, impartiality, and independence [3]. Although humanitarian–innovation pairs have gained earlier, wider reception in decision-making circles, their edges remain indistinct. Humanitarian innovation refers to new products, services, methods, or approaches that improve the efficiency or effectiveness of humanitarian action [4].

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 Framework: Innovation in Humanitarian Contexts

Innovation is systematically defined as the adoption, fulfilment or implementation of an idea, method, process, or device that creates value [5]. In humanitarian contexts, the adoption of new practices ranging from technical tools to management systems, which can improve services, is explicitly referred to as humanitarian innovation [6]. The term can also be applied to fill the gaps or complement traditional humanitarian models. Early examples include the use of cash-based assistance or micro-finance systems as alternatives to traditional food distribution [7]. In contemporary debates, the concept broadens to new practices or tools that inadvertently alter humanitarian action reshape underlying social relations and produce changes with measurable impacts on the sector, with examples such as remote mapping [1]. New humanitarian arrangements, adopting modern methods digital, extractive, algorithmic generate consequences that iteratively modify humanitarian paradigms and mentalities.

Drones in Humanitarian Action

Drones are a growing area of interest in humanitarian action, increasingly seen by practitioners and donors as a vital technology for facilitating disaster response and improving aid delivery [3]. Drones provide real-time aerial imaging of affected areas to map damage, track water, food, and shelter distributions, assess crop health, identify mudslides, and deliver health supplies [5]. In the aftermath of hurricanes in Texas and Florida, for example, drones were used to assess extensive damage, ensuring that recovery resources reached the most affected areas. In addition to aerial imagery, drones have been leveraged to deliver cargo often vaccines to remote or conflict-affected communities [4]. Drone use in humanitarian contexts, therefore, is burgeoning, with practitioners now viewing drones as crucial public goods [5]. While drone technology harbours enormous potential, its rapid proliferation poses operational challenges and unforeseen risks to affected populations. Humanitarian stakeholders continue to explore drones yet must rely on theoretical analysis and simulation studies to guide practice. The growing focus on drone technology in humanitarian contexts highlights the need for well-articulated operating principles to inform responsible design, use, and governance [6]. Likewise, the advent of drone technology, initially restricted to military operations, raises ethical considerations prevalent across drone activities. Stakeholders routinely cite ethical concerns regarding drone use in warfare, yet these considerations extend to their adoption in humanitarian initiatives [7]. In the humanitarian domain, operational and ethical discussions shape the development of frameworks that elucidate the potential and risks of drone technology. A code of conduct for the humanitarian use of drones delineates guidelines for responsible engagement, underscoring the need for ethical reflection within humanitarian organisations pursuing novel drone solutions [5]. In parallel, healthcare use of drone technology triggers ethical discourse frequently invoked in broader humanitarian settings [6]. Consequently, an examination of the contribution, challenges, and ethical implications of drone technology in humanitarian action set within the wider discourse on enabling technologies requires urgent attention [7].

Applications and Benefits

Disasters and conflicts represent extreme situations that call for an immediate humanitarian response. The sooner aid reaches vulnerable populations, the sooner they recover from the negative effects of conflict or disaster [1]. Drones assist in responding quickly by transporting life-saving supplies to affected populations when ground transportation is inefficient, impossible, or risky [3, 4]. Moreover, although aerial imagery is conventional for disaster management during the early phase, a drone's ability to deploy supplies also makes it appealing for use after a disaster [1]. Drones increase the frequency and speed of aerial go-to-market campaigns because they can carry smaller payloads or deploy these payloads faster than conventional methods. Remote delivery of supplies may influence the reach and relevance of aerial information campaigns as those on the ground are proactive in gathering specific types of information [4].

Operational Challenges and Risks

The pandemic crisis highlights underlying humanitarian malaise that remains unaddressed; six billion people still lack life-saving assistance. Technology exacerbates inequity and malfeasance instead of helping the most vulnerable [1]. Humanitarian technology holds unfulfilled promise, and the humanitarian sector remains comparatively low-tech. Digital tools can help in some contexts but must be carefully considered to avoid overreliance or technological solutionism [2]. Humanitarian aid is highly politicised, with humanitarian principles often eroded after crises. Such pre-existing vulnerabilities become more acute with technological interventions [3]. Technological innovations including drones and biometrics have great potential in humanitarian contexts, whether for assistance delivery to refugees, logging household inventories and monitoring supply chains, local economic development, epidemic prediction and prevention, using gaming approaches for data analysis, and construction of remote-sensing techniques for activity mapping [4]. Humanitarian organisations must make careful trade-offs between technological benefits and potential unintended harms [5].

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

Ethical and Legal Considerations

Rapid developments in drones and drone technology have implications for humanitarian action. However, increased use of drones also raises ethical and legal questions that must be considered [2]. The foundation of the discussion on ethical issues in humanitarian drones is the distinction between humanitarian use and humanitarian principles, and the link between drone operations and armed conflict [3]. Robust ethical and legal frameworks that account for, and actively try to avoid, unintended harms at different levels of the humanitarian systems do not exist [3]. Emerging ethical frameworks providing guidelines for drone design, development, and operation help prevent unintended harms that undermine the ethical legitimacy of humanitarian operations [4].

Biometrics in Aid Delivery and Protection

Biometric technologies can empower individuals to exercise agency over aid received, aid choice, and aid delivery medium [1]. Biometric identification can also offer beneficiaries protection from fraud and violence and facilitate better traceability of aid delivered, thereby enhancing anti-corruption efforts [1]. Humanitarian organizations have long relied on physical identity documents for identification and entitlement. However, large numbers of people do not possess physical documentation [2]. Biometric solutions can address this challenge and help establish confirmed digital identities [3, 4]. A pivotal consideration for biometric-enabled assistance is data privacy. Biometric systems gather sensitive information like fingerprints, retinas, and facial images, raising concerns about misuse, unauthorized access, and permanent tracking [5]. Hence, strictly safeguarding biometric data is critical. An additional challenge is to formulate clear data governance mechanisms around biometric data [6].

Empowerment and Access

Access to humanitarian aid is highly variable around the world, and biometric technologies have been proposed as a means to support equal access [1]. For example, the World Food Programme (WFP) has deployed biometric systems to enroll refugees and displaced persons in its cash-based assistance programs. This allows authenticated individuals to receive cash at any participating retailer in countries where WFP operates [2]. WFP cash transfers are entirely voluntary and provide beneficiaries with the choice to select their own type of assistance, thereby promoting self-reliance [3]. To date, more than 18 million biometric registrations have been completed across several countries. System deployment required months of preparation and consultation to secure the necessary agreements and consents [3]. A director from WFP opined that other cash-based organizations should adopt similar systems to promote equal access and financial dignity [1].

Privacy, Consent, and Data Governance

Privacy, consent, and data governance rank among the most critical considerations for humanitarian organizations embracing digital and data-driven technologies [6]. Such tools offer new approaches to monitoring, identifying needs, and providing assistance, but their potential for enhancing operational effectiveness nevertheless does not obviate the risks of increased digital surveillance, the proliferation of digital identities, the collection of biometric information, and the deployment of block chain and other systems for storing digital data [3]. Opaque policies, shallow accountability mechanisms, and exploitative practices related to mobile phone data and the tracking of digital footprints threaten the fundamental precepts of humanitarian action and sometimes attract unintended public attention [3]. Although innovation remains crucial for mitigation, organizational commitments to protecting personal data and ensuring ethical data practices must surface in a timely manner; transparency and accountability are even higher priorities throughout the humanitarian data life cycle. Balancing the need for rapid societal change and the right to remain free from interference fuels debate regarding the continuing role of innovation in data science and the humanitarian sector; many insist that technology and data science cannot furnish broadly applicable solutions [4]. Technological innovation harbors its own risks. New advances might increase the demand for and dependence on information technologies during humanitarian crises, exposing vulnerable populations to greater risk [5]. Islamophobia and anti-immigrant sentiment fuel a conspicuous rise in ethnic- and religion-based surveillance in many contexts; technologies capable of profiling, tracking, and containing populations threaten to amplify such surveillance [6]. Even from a conventional viewpoint, digital identities simplify the process of monitoring and restricting population movements and access to critical services during humanitarian crises. The monetary and reputational costs associated with humanitarian action provide no immunity against information technology's inherently dual-use nature. Data and digital technologies are themselves the subject rather than the medium of humanitarian action [7]. Interventions focus on elderly, disabled, and self-professed 'non-registered' populations, creating new forms of chronicity even as comprehensive solutions remain elusive [7].

Security, Bias, and Accountability

Humanitarian organisations increasingly use biometric systems in areas such as refugee registration and aid distribution [2]. Although the intended benefits are well studied, little emphasis is placed on the unintended harms that may arise [3]. Concerns include the alienation of vulnerable groups and the erosion of humanitarian

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

principles, as aid becomes contingent on biometric registration and organisations become accountable to States instead of the affected [5]. These developments threaten to undermine the humanitarian principles of neutrality and independence, which are critical for humanitarian action, protection, and access, especially in conflict-affected environments [1]. Biometric processes often depend on devices that carry the risk of surveillance. Excessive State surveillance can exacerbate the security and protection risks for affected communities (and humanitarian workers), can restrict the freedom of movement and flow of information, and can alter existing power dynamics between affected communities, aid organisations, beneficiaries, and authorities [7].

Unintended Harms in Digital and Technological Interventions

The increased adoption of digital and technological interventions in humanitarian contexts raises concerns about unintended harms [5]. Humanitarian organisations increasingly employ digital tools and technologies such as mobile devices, drones, satellite imagery, biometric data, data from social media, and publicly available big data to plan and deliver assistance [6]. Although the human, social, and environmental realities underpinning humanitarian crises remain complex, there is widespread disillusionment with efforts to mitigate these crises, leading humanitarian organisations to seek new digital and technological approaches [7]. However, these approaches can inadvertently create new vulnerabilities, reinforce power inequalities, violate security and privacy, and impede accountability. The implementation of drones and biometric systems in humanitarian contexts exemplifies this dilemma [7]. Digital humanitarianism refers to the distribution of humanitarian assistance and protection functions and the processing of relevant data by humanitarian workers and other actors—and reinforcing and addressing social and power structures and mechanisms related to security, privacy, bias, ethics, and accountability [1].

Security Risks and Dependence

Humanitarian organizations increasingly innovate with digital technologies, drones, biometrics, and automated tools to counter rising humanitarian needs amid resource constraints. Such innovations promise tangible benefits, yet they may incur unintended harms [1]. Drones assist in conflict zones, post-disaster assessments, and mapping and modeling [1]. They facilitate timely delivery of humanitarian aid without endangering personnel, enabling distribution in hard-to-reach areas and improving data collection efficiency [2]. They enhance communication with affected populations, thus promoting transparency, accountability, and stakeholder engagement. Despite widespread uptake, humanitarian use of drones remains experimental [2]. Biometric applications support safe aid delivery and high-quality service provision to refugee returnees; reinforce security during multi-cash programming; and help beneficiaries, partners, and staff [3]. Biometric technologies are widely adopted in banking, telecom, and technology sectors to enhance security, reduce fraud, and facilitate transactions. Humanitarian agencies employ biometrics, for example, to ensure that families receive only one distribution, that assistance reaches intended individuals, and that records for compound services remain distinct [4].

Social and Power Dynamics

Digital humanitarianism was once viewed positively, but scholars have begun to critique its social and political implications [1]. Concepts such as surveillance humanitarianism, algorithmic humanitarianism, and techno-colonialism describe how and why digital technologies, data practices, and the private sector reshape humanitarian practice, creating new vulnerabilities and forms of exclusion [2]. Disturbing voices have highlighted the unintended consequences of humanitarian technology; in particular, the risks associated with big data, public-private partnerships, and shifting relationships prompted them to sound the alarm. Data-driven interventions deploy intimate and sensitive information that often eludes the consent of affected populations [3]. Crises are treated as prepared experimentation for new tools and methods in the absence of any accountability or oversight. The humanitarian sector appears to become a site for unregulated development [4]. Rather than empowering individuals and communities, data and technology innovations appear to promote dependency and entrench exploitation. Humanitarian data and technology interventions are not merely technical, but socio-technical systems inextricably interconnected with social interactions [5]. Without cross-sector partnerships to build digital capacities and skills, many innovations continue to reinforce dependency and perpetuate exploitation [1, 7].

Accountability Mechanisms

The emergence of digital technologies, such as drones and biometrics, is reshaping humanitarian action. Humanitarian agencies, especially large international organizations, are increasingly using technologies to respond to complex humanitarian crises, better serve core principles, and address operational challenges. Accordingly, humanitarian innovation is imperative [3]. While digital technology accelerates innovation, it often gives rise to unintended harms, complicating the ethical and legal landscape for humanitarian actors. The humanitarian sector lacks adequate mechanisms for assessing the overall benefits and potential risks of such technologies, thus elevating the need for an integrated framework for humanitarian innovation [4]. Work to develop such frameworks is under way, and has yielded general principles to guide innovation processes. Critically, these principles do not address the potential for unintended or undesired consequences of digital technology

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

applications, especially drones and biometrics [5]. Elucidating the nature of these consequences in practice can clarify how technology adoption may misalign with humanitarian goals, whether intentional or not, and can thus refine the design of future frameworks [5]. The relevant literature cites three categories of unintended consequences. Security risks stemming from drones, biometrics, and other digital technology use can arise from unintended dependencies that expose operations to cyber-threats. Similarly, technological applications can amplify existing social and power dynamics between affected communities and humanitarian actors [6]. Finally, drones and biometrics, alongside broader data-driven technologies, can create accountability challenges, particularly where the interpretation or handling of collected information falls outside established norms or expectations [7]. In humanitarian action, security risks from drones, biometrics, and other digital technologies can derive from unintended dependence on other users, systems, or components [1]. Such dependency can become problematic if technical or human resources for continued operation are lacking, if required human skills are not available, or if continued operation enters into an unwritten agreement with other parties. Moreover, the greater community may perceive “going offline” as constrained rather than as intentional disengagement, and may take additional measures to counter perceived threats [4]. These external constraints are often perceived to take precedence over internal operations. Humanitarian systems, whether humanitarian fellows, materials, or temporary facilities, are characterized as critically dependent on the rapid replenishment of energy resources, resulting in dual dependence on external energy sources and data communication [3]. A security breach on one technology may constrain independent operation, thus forcing humanitarian actors to remain indefinitely exposed to security threats. The interpretation of collected and processed information also constitutes an extensive area of uncertainty that can blur the boundaries between acceptable and unacceptable uses of the material [7]. Both private and public channels are used to handle information that is thereby de-facto disclosed to authorities or the wider community. Mechanisms for systematically recording and making such interpretations widely available are absent, and, as a result, available guidance may go out of date or become irrelevant to specific contexts [6]. The humanitarian community overwhelmingly considers the transparent sharing of risk assessments to be critical for enabling informed decision-making. However, applying such principles to the interpretation of information shared with the very same community is rarely discussed [7]. Technological scenarios may amplify asymmetric power imbalances between affected communities and humanitarian entities. Support from one party or community towards the action of another can be perceived as endorsement, particularly in a climate of distrust. The introduction of aerial drones into specific regions, such as MTM, has prompted discussions on potential negative impacts on the credibility of humanitarian agencies [7]. The widespread emergence of online platforms also has the potential to both reduce reliance on humanitarian entities and curtail possibilities for unmediated engagement. A tension emerges between the humanitarian sector’s interest in vendors supplying platforms and the prospective independence of the affected community [6]. The existence of numerous platforms disseminating emergency alerts for multiple uses may unintentionally link humanitarian actors with rather non-humanitarian uses. Besides facilitating community engagement, online platforms can also be employed for collaborative marketing within the community; humanitarian engagement with such marketing can similarly produce non-humanitarian associations [5]. The growing climate of distrust towards humanitarian entities binds the choice of technologies and frameworks to the already sensitive debate on agency involvement and investment decisions. Sensitive regulator processes can thus distort the humanitarian system towards a rather specific, potentially distorted engagement [4].

Case Studies: Lessons from Practice

The approval to deploy an unmanned aerial vehicle (UAV) post-Hurricane Harvey highlighted the complexities of using drones in operations [1]. Activating the UAV was intended as an internal decision that would bolster situational awareness [1]. However, when the Vice President of the organization informed the Inter-Agency Standing Committee, it raised broader concerns around permissions and provision of sensitive data to military-associated bodies. As no UAVs had been deployed previously, guidance was sought from the collaborative humanitarian UAV Code of Conduct [2]. The case underscored the difficulty of anticipating how empowered individuals may engage with technology deemed to enhance disaster response and disrupted established coordination processes [1]. UAVs can support humanitarian assistance aspirations; nevertheless, challenges may arise in practice. The combination of self-appointed partnerships with non-traditional skillets and the anticipated ability to deploy new technologies amplifies the potential for mal-adoption and unforeseen consequences [1]. There is potential for over-reliance on IPO-driven technology within humanitarian frameworks, raising concerns about the possibility of a ‘technology transfer’ framework entering crisis dynamics. Data ubiquity and attention on data as a humanitarian imperative offer further pitfalls [2]. Over-reliance on data analysis to determine need-rankings has led to scope-creep; whereas scope and need may have been well-defined and acknowledged prior to the cycle, deploying data-driven models broadened and complicated the crisis definition. Shorter attention spans and shifting operational vocabularies toward ‘big-data’ and ‘data-analysis’ may further displace the humanitarian trajectory and tempt mis-direction [3].

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

Toward Mitigation: Guidelines, Standards, and Responsible Innovation

Drones and biometric technologies are hailed as game-changers. Milestones in technological innovation, humanitarian action, and digital capitalism have transformed how communities respond to crises. Drones offer benefits in search and rescue, logistics, mapping, and assessments [7]. Within humanitarian action, biometrics have emerged as a response to access concerns with aid delivery, providing identification, enabling entitlements, reducing fraud, and protecting populations. Anti-harassment technologies support privacy, gender, and security. Both technologies can enhance dignity, independence, and agency, yet present challenges [7]. Despite the anticipated promises, humanitarian actors remain cautious about recent innovations. Discussions emphasize the need for responsible innovation, with commitment to ethical benefits and proactive engagement of affected populations [7]. Without thorough consideration of possible risks and harms, crisis situations may worsen. Critiques interrogate the uptake of drones and biometrics. Innovations may displace critical discussions on humanitarian conditions, exert pressure to adopt trendy digital tools, and stimulate dependency on technology without detailed vetting [7-11].

CONCLUSION

This study has demonstrated that while drones and biometric technologies represent significant advancements in humanitarian innovation, their deployment is accompanied by complex and often underappreciated risks. These technologies have the potential to transform humanitarian action by improving the speed, reach, and accountability of aid delivery, particularly in hard-to-reach or crisis-affected areas. Drones enable rapid logistical support and real-time situational awareness, while biometric systems enhance beneficiary identification, reduce fraud, and facilitate more efficient distribution of resources. However, the findings reveal that these benefits are closely intertwined with unintended harms that can undermine the very objectives of humanitarian action. Ethical concerns surrounding privacy, consent, and surveillance are particularly pronounced in the use of biometric systems, where sensitive personal data may be exposed to misuse or exploitation. Similarly, drone deployment raises issues related to security, community perception, and potential association with military operations, which may compromise humanitarian neutrality and trust. Moreover, the study highlights how technological interventions can reshape social and power dynamics, often reinforcing inequalities, fostering dependency, and marginalizing vulnerable populations. The increasing reliance on digital systems may also expose humanitarian operations to cyber security risks and operational vulnerabilities, particularly in contexts with limited technical capacity. The lack of comprehensive governance frameworks and accountability mechanisms further exacerbates these challenges, leaving gaps in oversight and risk management. To address these concerns, humanitarian actors must adopt a more cautious and reflective approach to innovation. This includes embedding ethical considerations throughout the lifecycle of technological interventions, ensuring meaningful participation and consent from affected communities, and strengthening data protection and governance frameworks. Interdisciplinary collaboration, transparency, and continuous evaluation are essential to mitigate risks and enhance the responsible use of technology. Ultimately, humanitarian innovation should not be driven solely by technological possibility but by a commitment to uphold human dignity, equity, and justice. Balancing innovation with responsibility will be critical to ensuring that emerging technologies serve as tools for empowerment rather than sources of harm in humanitarian contexts.

REFERENCES

1. Jurko I. Humanitarian practice fit for the digital age. *The Humanitarian Leader*. 2022 Jun; Working Paper 026. doi:10.21153/thl2022art1615.
2. Hunt M. A living laboratory? Ethics and experimentality in humanitarian innovation [conference presentation]. *PREA Conference: Ethics and Humanitarian Research: Generating Evidence Ethically*; 2019 Mar 25-26; Columbus, OH.
3. Ogenyi FC, Ugwu CN, Eze VH, Ugwu OP, Ugwu JN, Okon MB, Ukagwu KJ. Transforming digital health using the internet of things for personalized interoperable and secure healthcare systems. *Discover Health Systems*. 2026 Dec;5(1):20.
4. Greenwood F, Nelson EL, Greenough PG. Flying into the hurricane: a case study of UAV use in damage assessment during the 2017 hurricanes in Texas and Florida. *PLoS One*. 2020;15(2):e0227808. doi:10.1371/journal.pone.0227808.
5. Ogenyi FC, Ugwu OP, Eze VH, Ugwu CN, Okon MB, Ugwu JN, Ukagwu KJ. Next-Generation Interference Management: A Narrative Review of power Allocation and SIC Enhancement in 5G/6G NOMA. *F1000Research*. 2025 Dec 3;14:888.
6. Cawthorne D, Robbins-van Wynsberghe A. An ethical framework for the design, development, implementation, and assessment of drones used in public healthcare. *Sci Eng Ethics*. 2020;26(5):2867-2891. doi:10.1007/s11948-020-00233-1.

7. 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.
8. EdalatNejad K, Lueks W, Sukaitis J, Graf Narbel V, Marelli M, Troncoso C. Janus: safe biometric deduplication for humanitarian aid distribution. In: 2024 IEEE Symposium on Security and Privacy (SP); 2024. p. 655-672. doi:10.1109/SP54263.2024.00116.
9. 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.
10. Zwitter A, Gstrein OJ. Big data, privacy and COVID-19 - learning from humanitarian expertise in data protection. *J Int Humanit Action*. 2020;5:4. doi:10.1186/s41018-020-00072-6.
11. Madianou M. Technocolonialism: digital innovation and data practices in the humanitarian response to refugee crises. *Soc Media Soc*. 2019;5(3). doi:10.1177/2056305119863146.

CITE AS: Asiimwe Kyomugisha T.. (2026). Humanitarian Innovation: Drones, Biometrics, and Unintended Harms. *Research Output Journal of Arts and Management* 5(1):26-32.
<https://doi.org/10.59298/ROJAM/2026/512632>