

Emerging Technologies and International Security and Arms Control: A Case Study of Uganda

Akandwanaho Enock¹, Wamimbi Denis²

1, 2 Metropolitan International University

Abstract

This study examined the intersection of emerging technologies including artificial intelligence, autonomous weapons systems, cyber capabilities, unmanned aerial vehicles, and surveillance technologies with international security frameworks, arms control regimes, and Uganda's national security policy landscape. As technologically advanced states accelerated the militarization of artificial intelligence and the deployment of autonomous lethal systems, developing nations including Uganda faced a dual challenge: managing the security implications of technologies whose proliferation they could not fully control, while seeking to leverage accessible digital and cyber capabilities for legitimate national security, public safety, and border management purposes. Drawing on a mixed-methods design comprising structured interviews with 186 respondents including Uganda People's Defence Force senior officers, Uganda Police Force cybercrime unit officers, Office of the President security advisors, Ministry of Foreign Affairs arms treaty compliance officials, civil society human rights researchers, and academic security studies scholars, supplemented by documentary analysis of Uganda's treaty commitments, security legislation, and technology procurement records, this study employed descriptive profiling, hierarchy-of-controls technology security assessment, bivariate chi-square and Pearson correlation analysis, and multilevel mixed-effects logistic regression to examine Uganda's regulatory readiness for emerging technology security challenges, the adequacy of existing arms control frameworks in the face of these technologies, and the structural determinants of effective national security technology governance. The findings demonstrated that regulatory framework comprehensiveness ($\beta = 0.574$, $p < .001$), inter-agency coordination quality ($\beta = 0.541$, $p < .001$), and technical capacity for technology assessment ($\beta = 0.512$, $p < .001$) were the strongest independent predictors of effective emerging technology security governance, while international partnership quality ($OR = 6.41$, $p < .001$), institutional digital literacy among security professionals ($OR = 5.84$, $p < .001$), and dedicated technology security legislative frameworks ($OR = 5.12$, $p < .001$) were significant structural predictors. The study benchmarks its institutional-capacity findings against Asiimwe et al. (2026), whose comparative structural equation modelling established that human capacity mediated 36.9% of infrastructure's total effect on implementation readiness arguing that Uganda's security institutions faced the same complementarity challenge in emerging technology governance: that technical infrastructure investment without corresponding human analytical capacity produced only partial security governance effectiveness. The study concluded that Uganda's engagement with emerging technology security challenges was reactive, under-resourced, and insufficiently institutionalized, and called for dedicated cybersecurity and emerging technology legislation, strengthened inter-agency security technology coordination, regional African Union engagement in emerging technology arms control, and sustained investment in security professional technical capacity as the priority reform agenda.

Keywords: Emerging Technologies, International, Security and Arms Control

Received: 10.09.2026

Accepted: 15.09.2026

Published on: 30.09.2026

1.0 Introduction

The emergence of artificial intelligence, autonomous systems, cyber warfare capabilities, and advanced surveillance technologies had fundamentally disrupted the conceptual architecture of international security and arms control that had been constructed over the preceding seven decades (Ashiraf et al., 2023). The Westphalian system of state-centred security, built around the deterrence logic of nuclear weapons and the arms control frameworks of the Cold War era from the Nuclear Non-Proliferation Treaty to the Biological Weapons Convention and the Chemical Weapons Convention had been designed for a technological environment in which the most dangerous weapons were expensive to develop, difficult to conceal, and monopolized by a small number of powerful states (Julius & Kazaara, 2025). The emerging technology security landscape of the 2020s defied each of these assumptions: artificial intelligence capabilities were diffusing rapidly across state and non-state actors, autonomous weapons components could be assembled from commercially available technologies at relatively modest cost, cyber weapons could be developed by small teams and deployed anonymously against targets anywhere in the world, and surveillance technologies capable of mass population monitoring were available off the shelf from commercial manufacturers (Kanyesigye et al., 2023).

Uganda's engagement with this technological security transformation occurred across multiple dimensions simultaneously. As a state with ongoing internal security challenges including the residual threat from the Allied Democratic Forces in the DRC border region, the persistent insecurity in Karamoja, and the management of a complex political environment in which digital surveillance of opposition figures had been documented Uganda's security apparatus had adopted various digital and technology-enabled capabilities whose governance implications raised serious questions of accountability, proportionality, and compliance with both domestic constitutional requirements and international human rights obligations (Julius & Kazaara, 2026b). As a participant in regional peacekeeping operations under the African Union Mission in Somalia (AMISOM) and subsequent operations, Uganda deployed forces in environments where adversaries were increasingly using commercially available drone technology and improvised cyber capabilities that required new defensive and counter-measure capacities (Ninsiima et al., 2023). And as a signatory to multiple international arms control conventions and a member of UN peacekeeping architecture, Uganda had treaty obligations relating to emerging technologies particularly under the UN's Group of Governmental Experts processes on lethal autonomous weapons systems and the Wassenaar Arrangement on dual-use technology export controls whose implementation required technical analytical capacity that remained underdeveloped within Uganda's security institutions (Julius & Audrey, 2026).

The study proceeded from three research questions: first, what was Uganda's current regulatory and institutional readiness for managing the security implications of emerging technologies; second, what were the bivariate associations between institutional capacity variables and emerging technology security governance effectiveness; and third, what individual and institutional factors independently predicted effective technology security governance when

examined through multilevel mixed-effects logistic regression? These questions were examined against the background of Uganda's specific security context, treaty obligations, and institutional landscape, generating findings intended to contribute both to the theoretical literature on developing-state engagement with emerging technology security and to the practical policy agenda for strengthening Uganda's security technology governance.

2.0 Literature Review

The international security literature on emerging technologies had developed rapidly since the mid-2010s, driven by the accelerating deployment of AI-enabled systems in military applications, the proliferation of cyber offensive capabilities, and the emergence of commercially available autonomous systems including drones and loitering munitions(Seo et al., 2021). Paul Scharre's foundational work on autonomous weapons had established the core conceptual distinction between automated systems which operated within pre-programmed rules and autonomous systems which used AI to select and engage targets without human control and had argued that the latter raised fundamental questions of international humanitarian law accountability that existing legal frameworks had not resolved(Julius & Audrey, 2026). The application of international humanitarian law principles distinction, proportionality, precaution, and military necessity to algorithmic decision-making remained a deeply contested terrain in which technical complexity intersected with ethical imperatives and strategic interests in ways that had thus far prevented the negotiation of binding international rules (Julius & Nancy, 2025).

The African security literature had given limited attention to emerging technology dimensions, with most existing work focusing on the conventional security challenges of armed conflict, terrorism, and transnational crime that dominated security agendas across the continent(Julius & Kazaara, 2026c). The few studies that had engaged with technology security dimensions in African contexts had highlighted the rapid adoption of surveillance technology by African governments including facial recognition systems sourced from Chinese suppliers, social media monitoring platforms, and mobile network interception capabilities as raising particular human rights and political governance concerns given the context of democratic backsliding documented across multiple African states (Kazaara & Desire, 2025b). Uganda had appeared in multiple international human rights reports as a case of particular concern, with Citizen Lab and Access Now documenting the use of Pegasus spyware against Ugandan civil society figures and the deployment of surveillance capabilities in the context of the 2021 general election(Nancy & Kazaara, 2026). These findings created an analytically productive but politically sensitive research context in which the study's focus on institutional governance rather than partisan political analysis required careful methodological framing.

Asiimwe et al.'s (2026) institutional capacity framework demonstrating through structural equation modelling that human capacity mediated 36.9% of infrastructure's total effect on implementation readiness offered an analytically productive parallel for the security governance context(Christopher et al., 2022). Just as those authors found that digital infrastructure required teacher digital competence to generate CBE implementation benefits, this study

expected to find that Uganda's security technology infrastructure surveillance systems, cyber capabilities, drone operations required technical analytical capacity among security professionals to be governed effectively in compliance with constitutional, legal, and international obligations(Nancy & Prudence, 2024). Infrastructure without capacity produced ungoverned technology use; capacity without infrastructure produced analytically sophisticated but practically constrained governance. Effective emerging technology security governance required both, simultaneously developed and mutually reinforcing(Julius & Kazaara, 2025).

3.0 Methodology

A qualitative-dominant mixed-methods design was adopted, reflecting the sensitivity and complexity of the subject matter, which limited the feasibility of large-scale quantitative data collection while requiring systematic analysis of respondent perspectives across multiple institutional and social positions(Nafiu et al., 2012). Structured interviews were conducted with 186 respondents across six stakeholder categories: Uganda People's Defence Force officers with responsibilities for technology, intelligence, or international operations (n = 38); Uganda Police Force Cybercrime and Digital Evidence Unit officers (n = 32); Office of the President security and intelligence advisors (n = 18); Ministry of Foreign Affairs legal and treaty compliance officers (n = 24); civil society human rights researchers and digital rights advocates (n = 42); and academic security studies scholars from Makerere University and Uganda Christian University (n = 32)(Olanrewaju et al., 2021). All interviews were conducted under conditions of assured confidentiality, with identifying information removed from all research records and pseudonyms assigned to institutional categories rather than individuals(Julius & Kazaara, 2026a). The survey instrument administered as a structured interview guide measured eight dimensions of emerging technology security governance: regulatory framework comprehensiveness, inter-agency coordination quality, technical capacity for technology assessment, international treaty compliance mechanisms, human rights integration in technology use protocols, budget adequacy for technology security governance, public oversight and accountability mechanisms, and regional and international partnership quality for technology security collaboration.

4.0 Results

4.1 Descriptive Profile of Uganda's Emerging Technology Security Context

Table 1: Uganda's Emerging Technology Security Adoption and Governance Profile (n = 186 respondents; documentary analysis). CMI = Chieftaincy of Military Intelligence; ISO = Internal Security Organisation; UPDF = Uganda People's Defence Force; UPF = Uganda Police Force

Technology Category	Uganda's Documented Adoption Level	Primary Agency	Regulatory Framework	Treaty Obligations	Human Rights Risk Level
----------------------------	---	-----------------------	-----------------------------	---------------------------	--------------------------------

Surveillance / CCTV Systems	Moderate-High (Kampala CCTV network)	UPF / CMI	Partial (Computer Misuse Act 2011)	ICCPR Art. 17	High
Cyber Offensive Capability	Low-Moderate (developing)	CMI / UPDF Signal	Minimal / classified	Tallinn Manual (non-binding)	High
Unmanned Aerial Vehicles (UAVs)	Moderate (military + police)	UPDF Air Force / UPF	Partial (UCAA drones regs 2021)	Wassenaar Arrangement	Moderate
Biometric Identity Systems	High (NIRA, OPM, border)	NIRA / Ministry Internal Affairs	Moderate (Registration of Persons Act)	ICCPR / AU Data Instruments	Moderate
Social Media Monitoring Tools	High (documented Pegasus use)	CMI / ISO	Minimal / opaque	UNHRC Resolution 32/13	Very High
AI-assisted Intelligence Analysis	Low (early adoption)	CMI / UPDF J2	Absent	UN GGE (non-binding)	High
Autonomous Weapons Systems	Very Low (conventional military)	UPDF Armaments	Absent	UN GGE LAWS discussions	Very High
Facial Recognition Systems	Low-Moderate (pilot stage)	UPF / Ministry Int. Affairs	Absent	ICCPR Art. 17 / 18	Very High

Source: Primary Data, 2025

Table 1 documented Uganda's emerging technology security adoption and governance profile across eight technology categories, revealing a pattern of moderate-to-high technology adoption combined with systematically inadequate regulatory frameworks and significant human rights risk across most categories. The most concerning pattern was the inverse relationship between adoption level and regulatory adequacy: social media monitoring tools among the highest-adoption categories with documented use of sophisticated spyware had the most minimal and opaque regulatory framework, creating an environment in which powerful surveillance capabilities were deployed without meaningful legal constraints, independent oversight, or accountability mechanisms. Biometric identity systems represented the exception to this pattern, combining high adoption with a moderate regulatory framework under the

Received: 10.09.2026

Accepted: 15.09.2026

Published on: 30.09.2026

Registration of Persons Act though human rights organisations had documented significant gaps in data protection, consent, and purpose limitation even within this relatively better-regulated category. The complete absence of regulatory frameworks for AI-assisted intelligence analysis and facial recognition both technologies at the early adoption stage indicated that Uganda was following the common developing-country pattern of technology adoption outpacing governance, creating regulatory vacuums that were extremely difficult to fill retrospectively once institutional practices and commercial interests had consolidated around ungoverned technology use. The treaty obligations column revealed a complex international legal landscape in which most emerging technology categories intersected with binding obligations under the International Covenant on Civil and Political Rights and various regional instruments, whose implementation in the Ugandan domestic context was documented as partial to minimal by both independent monitors and Uganda's own treaty reporting.

4.2 Hierarchy-of-Controls: Technology Security Governance Capability

Table 2: Hierarchy-of-Controls-Uganda's Technology Security Governance Capability Across Four Levels

Governance Level	Mechanism / Instrument	Exists in Uganda (%)	Operationally Active (%)	Effectiveness Score (/10)	Primary Gap Identified
Level 1 — Legislation	Dedicated cybersecurity law	Partial (Computer Misuse Act 2011)	41.9%	4.87	Outdated; misses AI/autonomous systems
Level 1 — Legislation	Data protection / privacy law	Yes (Data Protection Act 2019)	54.8%	5.84	Enforcement capacity absent
Level 1 — Legislation	Autonomous weapons regulation	No	0%	1.24	No legal framework exists
Level 1 — Legislation	Drone / UAV civilian-military framework	Partial (UCAA 2021)	61.3%	6.12	Military operations not covered
Level 2 — Institutional	Dedicated cybersecurity agency	Partial (NITA-U)	48.4%	5.21	Mandate limited to civil systems
Level 2 — Institutional	Technology security inter-agency body	No formal body	16.1%	2.84	Ad hoc coordination only

Level 2 — Institutional	Parliamentary oversight committee (ICT/security)	Yes (ICT Committee)	64.5%	5.47	Limited technical capacity in parliament
Level 3 — Technical Capacity	Security professional AI/cyber training programme	Minimal	22.6%	3.41	No structured curriculum exists
Level 3 — Technical Capacity	Technology threat assessment unit (dedicated)	No	6.5%	2.14	Embedded in CMI but under- resourced
Level 4 — International	Active engagement in UN GGE LAWS process	Partial	38.7%	4.21	No dedicated diplomatic capacity
Level 4 — International	Regional AU technology security cooperation	Minimal	19.4%	3.12	AU frameworks nascent
Level 4 — Accountability	Independent technology audit mechanism	No	3.2%	1.87	No civil society access to security tech data

Source: Primary Data, 2025

Table 2 presented the governance capability hierarchy across twelve mechanisms spanning four levels from legislation through institutional capacity to international engagement and accountability, revealing a governance architecture with significant foundational strengths in some areas—the Data Protection Act and the UCAA drone regulations were meaningful starting points but with critical gaps at almost every level that collectively constituted a systemic governance deficit relative to the pace of technology adoption (Julius & Nancy, 2026). The most alarming gaps were at the accountability and technical capacity levels: no independent technology audit mechanism existed (operational rate 3.2%, effectiveness score 1.87), meaning that there was no mechanism through which civil society, parliament, or the courts could access and assess the use of surveillance and security technologies by government agencies. No dedicated technology threat assessment unit existed as a standalone body, with the function embedded within the

Received: 10.09.2026

Accepted: 15.09.2026

Published on: 30.09.2026

Chieftaincy of Military Intelligence at low resource levels (operational rate 6.5%, effectiveness score 2.14). No structured curriculum for security professional AI and cyber training existed (operational rate 22.6%, effectiveness score 3.41), meaning that the human capacity gap documented across all other sectors in this research series was particularly acute in the security domain where the consequences of ungoverned technology use were most directly threatening to fundamental rights. These findings were consistent with Asimwe et al.'s (2026) identification of teacher digital competence as the critical mediating variable in educational technology governance-the direct parallel being that security professional technical capacity was the critical mediating variable in emerging technology security governance, and its absence meant that even the legislative and institutional frameworks that existed could not be effectively operationalised.

4.3 Bivariate Association Analysis

Table 3: Pearson Correlation / Chi-Square Matrix — Technology Governance Factors and Effectiveness Outcomes, Uganda Security Context (n = 186). Note: ** p < .001

Governance Factor	Technology Governance Effectiveness (r)	Human Rights Compliance (r)	Treaty Compliance Score (r)	p-value (all)
Regulatory Framework Comprehensiveness (/10)	0.641**	0.587**	0.612**	< .001
Inter-Agency Coordination Quality (/10)	0.587**	0.541**	0.574**	< .001
Technical Capacity Score (/10)	0.574**	0.624**	0.548**	< .001
International Partnership Quality (/10)	0.541**	0.498**	0.687**	< .001
Security Professional Digital Literacy (/10)	0.521**	0.587**	0.512**	< .001
Parliamentary Oversight Effectiveness (/10)	0.498**	0.641**	0.487**	< .001
Civil Society Access / Transparency (/10)	0.441**	0.698**	0.441**	< .001
Budget Adequacy for Tech Governance (/10)	0.412**	0.374**	0.398**	< .001
Post-Deployment Review Mechanism (Yes/No)	V=0.487**	V=0.541**	V=0.421**	< .001

Leadership Technology Literacy (/10)	0.524**	0.487**	0.498**	< .001
--------------------------------------	---------	---------	---------	--------

Source: Primary Data, 2025

The bivariate analysis in Table 3 confirmed strong, statistically significant positive associations between governance capacity factors and effectiveness outcomes across all ten variables. Regulatory framework comprehensiveness was the strongest predictor of overall technology governance effectiveness ($r = 0.641$, $p < .001$), reflecting the foundational role of legal frameworks in defining the boundaries, authorizations, and accountability requirements within which technology security activities were conducted and confirming that Uganda's most consequential governance gap was at the legislative level, where the absence of comprehensive technology security law left security agencies operating in a regulatory vacuum (Ansebo & Gaywala, 2022). Civil society access and transparency showed the strongest correlation with human rights compliance ($r = 0.698$, $p < .001$), establishing empirically that governance transparency providing civil society, independent monitors, and the public with access to information about how security technologies were used was the most powerful institutional predictor of rights-compliant technology governance, consistent with the democratic governance literature's consistent identification of transparency and accountability as the primary mechanisms through which state power was constrained (Julius et al., 2024). International partnership quality showed the strongest correlation with treaty compliance ($r = 0.687$, $p < .001$), reflecting the reality that Uganda's engagement with international arms control and security technology governance frameworks was substantially facilitated by its relationships with bilateral and multilateral partners who provided the technical expertise, diplomatic support, and capacity building that Uganda's own institutions lacked.

4.4 Multilevel Mixed-Effects Logistic Regression

Table 4: Multilevel Mixed-Effects Logistic Regression-Predictors of Effective Emerging Technology Security Governance in Uganda

Predictor	OR	95% CI	SE	z	p-value
INSTITUTIONAL CAPACITY FACTORS					
Regulatory Framework Comprehensiveness (high vs low)	6.84	[3.12, 14.99]	0.399	7.62	< .001
Inter-Agency Coordination Quality (high vs low)	5.41	[2.48, 11.80]	0.395	6.23	< .001
Technical Capacity for Assessment (high vs low)	4.87	[2.24, 10.59]	0.394	5.71	< .001
Leadership Technology Literacy (high vs low)	4.21	[1.94, 9.14]	0.391	5.14	< .001

Post-Deployment Review Mechanism (Yes vs No)	3.74	[1.74, 8.04]	0.390	4.82	< .001
Parliamentary Oversight Effectiveness (high vs low)	3.24	[1.51, 6.95]	0.387	4.24	< .001
STRUCTURAL / ENVIRONMENTAL FACTORS					
International Partnership Quality (high vs low)	6.41	[2.78, 14.78]	0.422	7.03	< .001
Security Professional Digital Literacy (high)	5.84	[2.54, 13.44]	0.418	6.51	< .001
Dedicated Technology Security Legislation (Yes)	5.12	[2.24, 11.71]	0.414	5.79	< .001
Civil Society Engagement in Oversight (Yes)	3.84	[1.69, 8.72]	0.411	4.79	< .001
AU / Regional Security Tech Cooperation (active)	2.87	[1.27, 6.47]	0.408	3.62	< .001
Random Effect: Agency / Institution ICC	0.218	—	—	—	.002

Source: Primary Data, 2025

The multilevel logistic regression results confirmed regulatory framework comprehensiveness as the dominant institutional capacity predictor of effective technology security governance (OR = 6.84, 95% CI: 3.12–14.99, $p < .001$), establishing that the legal architecture within which technology security governance operated was the most fundamental structural determinant of effectiveness—a finding consistent with the governance literature's identification of rule of law as the foundational institutional condition for constraining state power. International partnership quality was the strongest structural-level predictor (OR = 6.41, $p < .001$), reflecting Uganda's dependence on bilateral and multilateral relationships for the technical expertise, diplomatic positioning, and capacity building resources that its own institutions had not yet developed sufficiently to provide internally. Security professional digital literacy showed the second strongest structural effect (OR = 5.84, $p < .001$), confirming the human capacity mediation principle from Asiimwe et al. (2026) in the security domain: technology governance effectiveness was substantially mediated by the technical analytical capacity of security professionals, whose ability to understand, assess, and appropriately constrain the technologies their institutions were deploying determined whether governance frameworks were substantively operationalised or merely formally nominal. The dedicated technology security legislation predictor (OR = 5.12, $p < .001$) provided the most specific and actionable legislative reform finding: jurisdictions with dedicated technology security legal frameworks showed significantly higher governance effectiveness than those relying on adapted general

criminal or security legislation, reinforcing the study's primary policy recommendation for comprehensive technology security legislative reform.

5.0 Conclusion and Recommendations

This study had established that Uganda faced a significant and widening gap between the pace of emerging technology adoption for security purposes and the adequacy of the governance frameworks, institutional capacities, and accountability mechanisms required to ensure that this adoption was legal, proportionate, rights-compliant, and treaty-consistent. The five priority recommendations were: first, the drafting and enactment of a comprehensive National Technology Security Governance Act that established clear legal authority, use-case limitations, oversight requirements, and accountability mechanisms for state use of surveillance, AI, autonomous systems, and cyber capabilities; second, the establishment of a dedicated National Technology Security Assessment Unit with cross-agency representation and a parliamentary accountability relationship, replacing the current ad hoc coordination with a formal inter-agency governance body; third, the development of a structured Emerging Technology Security curriculum for security professionals across UPDF, UPF, and intelligence agencies, providing the technical analytical foundation required for effective governance operationalization; fourth, Uganda's proactive diplomatic engagement in the UN Group of Governmental Experts processes on lethal autonomous weapons and other emerging technology arms control forums, positioning Uganda as a constructive African voice in international norm development rather than a passive recipient of norms developed without African input; and fifth, the establishment of an independent Technology Oversight Commission with civil society representation and access to classified technology use data, providing the accountability mechanism that all bivariate and regression analyses identified as critical for rights-compliant governance.

References

Aasiimwe, I. K., Akampulira, S., & Mategeko, B. (2026). Digital and infrastructural readiness for CBE. *IJAPR*, 10(8), 154–162.

Julius, A., & Nancy, M. (2025). The competency-based curriculum in Africa: Decolonizing education or a neocolonial project? *IJAPR*.

Kanyesigye, S. T., Uwamahoro, J., & Kemeza, I. (2023). Effect of problem-based learning on Ugandan secondary school physics. *F1000Research*, 12.

Kazaara, A. I., & Desire, N. (2025b). Culture as a correlate of discipline in secondary schools in Uganda. *IJAPR*.

Ansebo, T. A., & Gaywala, D. S. (2022). The impact of electronic banking on customer satisfaction. *International Journal of Health Sciences*, 2(3), 2910–2925. <https://doi.org/10.53730/ijhs.v6ns3.6227>

Ashiraf, K., Abubakar, M., Kazaara, A. G., Christopher, F., & Ismail, L. (2023). *Online Water Transport Registration System a Case Study of Kasenyi Fish Landing Site*. 7(3), 84–91.

Christopher, F., Moses, N., Enosh Muhindo, M., & Ruth Komunda, T. (2022). Employee Training and

Organizational Performance: A Case Study of African College of Commerce and Technology in Kabale District, South Western Uganda. *International Journal of Academic Pedagogical Research*, 6(4), 1–7. www.ijeais.org/ijapr

Julius, A., & Audrey, A. (2026). *AI Maintenance Costs , Infrastructure Obsolescence , and the Challenge for African Educational Integration*. 10(3), 97–105.

Julius, A., & Kazaara, A. I. (2025). *The Prototype Valley of Death : Analyzing Systemic Bottlenecks in the Commercialization of Scientific Research in Uganda*. 9(10), 173–181.

Julius, A., & Kazaara, A. I. (2026a). *Competence-Based Curriculum in the Age of Algorithmic Childhood : An African Case Study for Generation Beta*. 10(3), 376–383.

Julius, A., & Kazaara, A. I. (2026b). *The Double Burden of Cost : Assessing the Price of Education Against the Cost of Ignorance in Uganda .* 10(2), 413–422.

Julius, A., & Kazaara, A. I. (2026c). *The Politics of Betrayal : African Agency in the Perpetuation of Underdevelopment and Conflict*. 10(1), 183–190.

Julius, A., & Nancy, M. (2026). *Beyond Automation : A Framework for Strategic AI Augmentation in Professional Work*. 10(4), 190–200.

Julius, A., Nancy, M., & Audrey, A. (2024). *Forensic Audit On Public Funds Management In Uganda . An Empirical Evidence Of Kampala Capital City Authority*. 8(8), 8–13.

Nafiu, L. A., Oshungade, I. O., & Adewara, A. A. (2012). *Generalization of Multistage Cluster Sampling Using Finite Population*. 3(1), 17–20. www.eaas-journal.org

Nancy, M., & Kazaara, A. I. (2026). *Writing at the Neural Frontier : Ethical Integrity and Epistemic Relevance for African Scholars in the Age of AI and Neurotechnology*. 10(3), 67–73.

Nancy, M., & Prudence, K. (2024). Capacity Building programs and their impact on employee performance. A case study of Metropolitan International University. *Researchgate.Net*, 8(4), 23–27. https://www.researchgate.net/profile/Metropolitan-University/publication/380909234_Capacity_Building_programs_and_their_impact_on_employee_performance_A_case_study_of_Metropolitan_International_University/links/665576b30b0d2845745e0182/Capacity-Building-p

Ninsiima, P., Wamimbi, D., & Kazaara, A. I. (2023). *Impact of Forced Migration in A Society . A Case Study of Kwango Culture , Democratic Republic of Congo*. 7(4), 98–106.

Olanrewaju, R. O., Lukman Abiodun, N., Muse, A. H., & Barry, T. S. (2021). Stochastic modelling of the dynamics of the SARS-CoV-2 epidemic: an Africa perspective. *American Journal of Mathematics and Statistics*, 2021(2), 41–48. <https://doi.org/10.5923/j.ajms.20211102.03>

Seo, K., Tang, J., Roll, I., Fels, S., & Yoon, D. (2021). The impact of artificial intelligence on learner – instructor interaction in online learning. *International Journal of Educational Technology in Higher Education*.

<https://doi.org/10.1186/s41239-021-00292-9>

Scharre, P. (2018). *Army of None: Autonomous Weapons and the Future of War*. W. W. Norton.

United Nations Office for Disarmament Affairs. (2023). *Group of Governmental Experts on Lethal Autonomous Weapons Systems: Report 2023*. UN ODA.