AGENCY FOR PEACEBUILDING

October 2026

FOREIGN POLICY AND THE REORDERING OF CONFLICT IN EASTERN AFRICA

PeaceTech in a securitised digital order

Naomi Mwelu Kilungu

AP Policy Papers
Issue 3/2026 ISSN 3103-1668

ABOUT THE AGENCY FOR PEACEBUILDING

The Agency for Peacebuilding (AP) is a think-and-do organisation committed to bridging the gap between research and practice in peacebuilding.

AP aims to contribute to more peaceful and just societies by preventing and transforming violent conflict and creating spaces for dialogue and cooperation across sectors and divides. AP's vision is of a world where conflicts can be transformed without violence and where peace can be promoted through inclusive, innovative sustainable means.

ABOUT THE AUTHOR

Naomi Mwelu Kilungu is a researcher, artist, and consultant specialising in localisation and decolonisation across African contexts. Her work bridges creative practice and policy research, with focus areas that covers Artificial Intelligence applications for peace and post-conflict reconstruction, African security architectures, child protection in war zones, and peace finance.

ACKNOWLEDGMENTS

This Policy Paper has been realised under the project “Foreign policy and peace processes: the role of cyberspace” cofinanced by Fondazione Compagnia di San Paolo.

The author is solely responsible for the content of the paper.

AP would like to thank Logan Uhlig for the final revisions and comments.

INDEX

GLOSSARY 4

AT A GLANCE 5

INTRODUCTION 6

DIGITAL GEOPOLITICS 8

DIGITAL FINANCE AND THE NEW GEOPGRAPHY OF ARMED CONCLICT 11

DIGITAL TECHNOLOGY AND DIPLOMACY 13

PEACETECH IN THE REGION 15

MAINSTREAMING PEACETECH THROUGH PEACE ARCHITECTURES 19

RECOMMENDATIONS 20

GLOSSARY

AI – Artificial Intelligence

AU – African Union

CEWARN – Intergovernmental Authority on Development Conflict Early Warning and Early Response Mechanism

CEWS – Africa Union Conflict Early Warning System

DRC – Democratic Republic of the Congo

EAC – East African Community

EU – European Union

GIS – Geographic Information Systems

GPS – Global Positioning System

IGAD – Intergovernmental Authority on Development

NCEWERS – National Conflict Early Warning and Early Response System (Kenya)

NDVI – Normalised Difference Vegetation Index

NEWIS – National Early Warning Information System (Kenya)

NLP – Natural Language Processing

RSF – Rapid Support Forces

SMS – Short Message Service

UN – United Nations

AT A GLANCE

The Rise of "Digital Geopolitics"

Connectivity, digital finance and infrastructure have become instruments of power in Eastern Africa. China, the United States, the Gulf, Russia, and the EU and other powers compete for influence, while regional states practise "polyalignment".

This hedging preserves room for manoeuvre but produces "polydependence", and no enforceable continental framework yet compels convergence on data governance and cybersecurity.

The Digital Paradox: Control versus Engagement

The infrastructure that enables civic engagement, mobile finance, and digital diplomacy also enables shutdowns, information warfare, and new channels for financing armed groups.

Ethiopia's blackouts, the diaspora influencers of Sudan's war and al-Shabaab's use of the mobile-money ecosystem show the same infrastructure serving both control and conflict.

The Expanding Frontiers of PeaceTech

Eastern Africa possesses a mature institutional tradition (IGAD's CEWARN, Kenya's NCEWERS) and a vigorous citizen-led one (Ushahidi, #defyhatenow, Sudan's Emergency Response Rooms).

Digital tools can broaden participation and provide early warning, but they cannot resolve the land, territorial and political disputes that drive violence.

Structural Barriers and New Digital Risks

PeaceTech is marginal to foreign and security policy, and dependent on external platforms, data infrastructure and short-term funding. The attendant risks include bias, threats to data sovereignty and the safety of participants.

An Eastern Africa Digital Peace Platform, anchored by the AU and endorsed by IGAD and the EAC, could connect peacebuilders, diplomats and security actors.

INTRODUCTION

In recent years, the nature of war in Eastern Africa[1] has changed. Connectivity, no less than weaponry, has become a decisive factor, which is perhaps best illustrated by Ethiopia. From November 2020, the government severely restricted telephone and internet services in Tigray for more than two years. Its aim went beyond suppressing dissent. It sought to create an information vacuum, where abuses could occur without journalists, humanitarian workers or foreign observers to bear witness.[2]

While the Ethiopian government aimed to cut the flow of information, in Sudan, competition centers on control over it. After fighting began in 2023, the most influential voices were not always those of the generals who started the war. It was the diaspora influencers in Paris, Toronto and the Gulf who held livestreams with armed commanders. In doing so, they shaped narratives and mobilisation almost in real time.[3]

A third case concerns dependence on infrastructure. For instance, in 2018 Le Monde alleged that data from the African Union (AU) headquarters in Addis Ababa, financed by China, had been sent to servers in Shanghai from 2012 to 2017. However, the allegation remains contested because the Chinese officials and AU representatives rejected or disputed key parts of the report. Even so, it points to wider concerns as reliance on foreign digital infrastructure becomes a frontline of geopolitical competition.[4] Therefore, Ethiopia, Sudan and the African Union headquarters are symptomatic of a deeper structural shift in the conduct of war.

This article contends that digital technologies are no longer supplementary instruments of war. They have altered its underlying conditions. First, new technologies change who controls the flow of information through shutdowns, platforms and disinformation. Second, they change how money reaches armed actors through mobile money and fintech. Third, the ownership structure around information has shifted with modern communications technologies, which rely on vendors, networks, and

clouds, which are oftentimes foreign owned. Each shift redistributes power among states, armed groups, external powers and civilians. Each, in turn, narrows or widens what peacebuilders can do. While recognizing this shift is necessary, it is insufficient to fully grasp a situation, as in various contexts the same technologies can serve as a tool of control in one setting and of civic engagement engagement in another.

Against this background, the article examines digital tools used to prevent violence and support peacebuilding, known as PeaceTech. How East African states interact through their foreign policy, in different terms, with "core" states dictates their experience in geopolitical relations, security and peace. It is worth noting a citizen-led tradition of digital peacebuilding has emerged across Eastern Africa, yet it remains largely detached from the region's foreign and security policy debates, and policymakers continue to treat PeaceTech and digital geopolitics as separate domains. This article argues instead that they are two expressions of a single structural change, and that closing the gap between them is a policy goal in its own right.

The term "security" is used in this paper to denote the state-centred and regional policy sphere of defence, intelligence, cyber and counter-terrorism, distinct from the human security concerns of communities. Collaboration between peacebuilders and security actors is not always feasible or desirable. Where governments are themselves parties to conflict, or order shutdowns, as in Ethiopia, civil society may rightly keep its distance. Data shared with security services can also place people at risk. This article therefore does not assume convergence. It argues instead for structured and selective contact. Such contact should rest on clear data-protection safeguards and be confined to

[1] For the purposes of this article, "Eastern Africa" denotes, for the most part, the member states of the Intergovernmental Authority on Development (IGAD) and the East African Community (EAC. Nigeria and Cameroon, examined later in relation to fintech-facilitated conflict financing and mobile-enabled mobilisation respectively, fall outside this regional core, but they serve as comparative examples of dynamics that may also be observed in Eastern Africa.

[2] Aemro Ayalew, "Ethiopia's Digital Blackouts are an Attempt to Turn Off Accountability", Africa at LSE, 19 January 2026.

[3] O. Hamad, "The Weaponization of Social Media in Sudan's War", SWP Megatrends Spotlight 70, 2026.

[4] Le Monde Afrique, "À Addis-Abeba, le siège de l'Union africaine espionné par Pékin", 26 January 2018; Reuters, "African Union says has no secret dossiers after China spying report", 8 February 2018; DW, "China calls AU spying report 'preposterous'", 29 January 2018.

areas where interests genuinely overlap, such as monitoring hate speech or protecting civic data.

Hence, an Eastern Africa Digital Peace Platform could help to build these points of contact. It would also support regional data-sharing and capacity-building. Its applications would be locally designed, rather than imported or donor-driven. Donor-driven, thereby bringing PeaceTech into the region's security equation. It would also offer a practical alternative to unregulated rivalry over security and infrastructure. A comparable proposal has been made by Emiliano Alessandri for the Middle East and North Africa, which this piece builds upon. The article proceeds as follows: it first maps the region's digital geopolitics, including the role of digital finance in armed conflict; it then examines digital engagement, digital control and the PeaceTech toolkit, before turning to six country cases. It closes with the case for mainstreaming PeaceTech through the region's peace architecture, together with recommendations for specific actors.

DIGITAL GEOPOLITICS

Most African states have adopted what one recent study of Kenyan foreign policy terms "polyalignment": utilising competition between external powers and being careful not to bind themselves to a single patron.[5] This strategy is a genuine expression of African agency; it also, however, produces socio-economic contradictions and a form of "polydependence" that leaves individual states more, not less, geopolitically exposed as rivalries intensify. This hedging should not be interpreted as weakness, according to relevant work on African agency in cyberspace. It contends that even from a position of material weakness, low costs and quick dissemination provide African players genuine, if limited, flexibility to restrict foreign influence and pursue local political goals.[6]

Each alignment brings something different to the table. For example, China offers finance and equipment, whereas the United States offers security cooperation, cloud services and its platform firms. Gulf states contribute capital, and Russia operates chiefly through information operations. It would be mistake, however, to read this behaviour as improvisation by weak states. Research on African agency in cyberspace observes that digital communication is inexpensive and information travels rapidly. These conditions afford African governments a degree of latitude to resist foreign influence and pursue their own aims, even when they lack financial resources and advanced technology.[7]

It is therefore evident that these agreements rarely decide how wide the digital divide is. They decide the shape of the network that crosses it: whose equipment is used, whose standards prevail and whose rules govern data. Capacity-building assistance plays a quiet but important role here, because it draws "digital peripheries" into a donor's system without any formal alliance.[8]

Kenya's polyalignment

Kenya has so far declined to choose between Washington and Beijing. What is being bargained over is not access to the internet as such, but control of its foundations: the cables, exchanges, servers and standards on which connectivity depends. Kenya's geography makes control over this infrastructure particularly consequential, as the country serves as the region's principal data hub, and its international cables make landfall on the Indian Ocean coast.

In fact, Kenya's foreign policy and polyalignment can be interpreted through the geography of its strategic infrastructure. Manda Bay, on the northern coast near the Somali border, represents Kenya's security partnership with the United States and the United Kingdom. In 2024, the United States designated Kenya as its first Major Non-NATO Ally in sub-Saharan Africa. The designation provides defence-trade and security-cooperation benefits and formally recognises Kenya as one of Washington's principal counter-terrorism partners in the region.[9] The facility is located in Lamu County, close to Somalia and the western Indian Ocean. Its position allows the United States and Kenya to support operations against al-Shabaab and to respond rapidly to security developments in the Horn of Africa. The base's strategic importance became clear in January 2020, when al-Shabaab attacked the installation. In January 2026, Kenya and the United States began a $71 million expansion of the military airfield, including the construction of a 10,000-foot runway. [10] The expansion enables the United States to support

[5] T. Zajontz, "Locating Africa in the Second Cold War: the Geopolitical Economy of Kenyan Polyalignment", Third World Quarterly, 2025.
[6] N. Allen et al., "New Technology, Old Strategy: Cyberspace and the International Politics of African Agency", Journal of Strategic Studies, 2024.
[7] N. Allen et al., "New Technology, Old Strategy: Cyberspace and the International Politics of African Agency", Journal of Strategic Studies, 2024.
[8] J. Carver, "Developing Digital 'Peripheries' for Strategic Advantage: Capacity Building Assistance and Strategic Competition in Africa", Contemporary Security Policy, 2024.

[9] The White House, "United States–Kenya Joint Leaders' Statement", 23 May 2024; U.S. Department of State, "Designation of Kenya as a Major Non-NATO Ally", Federal Register, 12 July 2024. The designation made Kenya the first Major Non-NATO Ally in sub-Saharan Africa.
[10] *Stars and Stripes*, "$71 Million Upgrade Starts at Kenyan Airfield That Plays Key Role in Counterterrorism", 30 January 2026. The report states that the expansion includes a 10,000-foot runway. The 2020 attack killed one U.S. service member and two U.S. contractors.

operations from Kenyan territory without relying exclusively on facilities in Djibouti, where China has maintained a military base since 2017. The security partnership also goes beyond military infrastructure.[11] The latest known involvement was on 18 September 2026, when Kenya unveiled a counter-terrorism hotline and online reporting portal, built with British and American help but owned and run by Kenya's own Counter Terrorism Bureau.[12]

Another significant example is the Mau Summit, in the Rift Valley. It lies on the Northern Corridor, which links Mombasa to Nairobi, Uganda and the Great Lakes and it represents the continuing importance of Chinese contractors, infrastructure finance and transport connectivity. Its relevance follows from Kenya's turn to Beijing in April 2025. After President Ruto's visit, the two governments raised their relationship to a Comprehensive Strategic Partnership in the New Era. They signed about twenty agreements covering infrastructure, trade, digital technology, energy and finance. These included support for extending the Standard Gauge Railway towards Malaba and for expanding the Nairobi–Nakuru–Mau Summit–Malaba corridor.[13]

There are two major considerations which may help explai Kenya's polyalignment. First, Kenya needs foreign capital, technology and security cover, but foreign partnerships are rarely unconditioned. External actors consistently attach specific terms to their support, ranging from preferred supplier status and proprietary standards to data rights and the exclusion of rival powers. As a result, resource inflows are bound by external dictates that systematically shape and restrict Kenya's policy discretion. The second issue involves data sovereignty. High-value security assets, including intelligence gathered at Manda Bay and counter-terrorism case files, are managed across different foreign-backed platforms. However, distributed financing does not determine legal jurisdiction over sensitive information. Relying on multiple external security partners ultimately trades immediate operational gains for long-term legal exposure and regulatory risk. Polyalignment gives Nairobi leverage, since no single suitor can dictate terms. On the other hand, polydependence removes its exit, since no single supplier can easily be dropped. The critical test is whether Kenya can court many allies and still command its own infrastructure, data and policy.

Digital control

Infrastructure dependence determines that whoever supplies and runs networks shapes what governments and armed actors can do with them, and Ethiopia shows this most clearly. The government has repeatedly used connectivity restrictions as an instrument of political control during hostilities. A good example is the Tigray blackout, among the largest communication shutdowns on record, which began in November 2020 and lasted more than two years in its most severe form. After a partial and uneven restoration, another shutdown followed in Amhara from 2023, linked to fighting between the Fano militia and federal authorities.[14] Shutdown orders are executed through Ethio Telecom, whose network was supplied by Chinese contractors; infrastructure built for growth thus becomes a tool of political control.[15]

In this framework, Beijing's contribution is mainly infrastructural. Its guiding framework is the Digital Silk Road, which Chinese firms and banks bring to fruition through supplying networks, data systems and the hardware that links them, something which Beijing and Addis Ababa describe the result as a partnership. Western critics describe it as capture and a mechanism of surveillance. It is also seen as reduced competition and long-term dependence on Chinese vendors and credit.[16] The disagreement is therefore less about who builds the infrastructure than about what it connects to: Chinese equipment, Chinese standards and, in the critics' view, Chinese methods of governance, considered by some scholars call the this rivalry a digital cold war.[17]

[11] Congressional Research Service, Kenya: Current Issues and U.S. Relations, 6 March 2026. The United States has supported Kenyan capacity to counter terrorist attacks, secure borders and contribute to regional stabilisation operations.
[12] Mudavadi Unveils New Counter-Terrorism Hotline, Ministry of Foreign and Diaspora Affairs, Kenya; 18 September 2026.
[13] Permanent Mission of the People's Republic of China to the United Nations, "Joint Statement between the People's Republic of China and the Republic of Kenya on Creating an Inspiring Example in the All-Weather China–Africa Community with a Shared Future for the New Era", 24 April 2025; Kenya Broadcasting Corporation, "Kenya Strikes Significant Deals during Ruto's State Visit to China", 24 April 2025.

[14] Ayalew, "Ethiopia's Digital Blackouts are an Attempt to Turn Off Accountability", 2026; Access Now, "Two years of internet shutdowns: people in Tigray, Ethiopia, deserve to be reconnected", 4 November 2022; Access Now, "After years under a shutdown, Tigray is slowly coming back online", 1 February 2023.
[15] Binding Hook, "How African States Challenge Cyber Superpowers", 2024.
[16] S. van der Lugt, "Exploring the Political, Economic, and Social Implications of the Digital Silk Road into East Africa: The Case of Ethiopia", 2021.
[17] J. Åberg et al., "A Digital Cold War in Africa? Capitalist Multiplicity, Digital Transformation, and Shifting Dependencies amid US–China Tech Rivalry", Third World Quarterly, 2025; S.

Washington has responded with initiatives such as the Digital Connectivity and Cybersecurity Partnership, though it has not matched Chinese lending at scale.

Ethiopia is far from unique in digital tools of political control. Monitoring indicates that the number of internet shutdowns in Africa has roughly doubled since 2016, with Ethiopia and Sudan among the most frequently affected countries. [18] In eastern DRC, digital disruption extends from the information domain into navigation and logistics: UN experts and aviation authorities have documented GPS jamming and spoofing affecting UN, humanitarian and commercial flights, with the interference attributed to non-government conflict actors operating in and around North Kivu. [19] Cyber-espionage allegations, such as the Le Monde report on the AU headquarters, add a further layer, since they suggest that the very institutions meant to coordinate a common African position may themselves depend on foreign-built systemss, encouraging states to seek bilateral engagements independently to try to negotiate the best terms for themselves.

Policy incoherence?

Polyalignment also carries a governance implication. Because security requirements differ across vendors and no legally enforceable continental framework compels convergence, hedging produces policy incoherence. [20] The AU Data Policy Framework (2022) and the Malabo Convention (2014) both aim to strengthen data governance and cybersecurity, yet neither yields a comprehensive, uniformly enforceable continental framework. The Malabo Convention entered into force in June 2023, once the required fifteen ratifications had been secured, but it binds only the states that have ratified it, a minority of AU members. Regional integration compounds the problem. Digital-market integration in East Africa, examined through the cases of Rwanda and Tanzania, is driven more by external actors and firms than by coordinated regional policy, so that Eastern African states retain only a limited ability to set common terms for digital infrastructure. [21] The greatest impediment to advancing the continent's cyber-governance agenda is thus the gap between the aspiration to digital sovereignty and the people and technical resources needed to achieve it. The next subsection shows the same gap at work in digital finance, where infrastructure is spreading faster than the capacity to secure it

Kumar, "China's Digital Expansionism in Africa and the US Counter-Strategies", Insight on Africa, 2024.

[18] Paradigm HQ, "Internet Shutdowns in Africa Double Since 2016", 2025.

[19] United Nations Security Council, Midterm Report of the Group of Experts on the Democratic Republic of the Congo, December 2024 (cited in U.S. State Department statement, 16 January 2025); ICAO ESAF APIRG, "GPS Spoofing/Jamming in the Democratic Republic of the Congo", Working Paper, 2024.

[20] N. Ifeanyi-Ajufo, "Cyber Governance in Africa: at the Crossroads of Politics, Sovereignty and Cooperation", Policy Design and Practice, 2023; N.G. Adams, "Cybersecurity and Geopolitical Rivalry: Why Africa Needs a Digital Defence Strategy Now", T20 South Africa, 2025.

[21] S. Arnold, "Drivers and Barriers of Digital Market Integration in East Africa: A Case Study of Rwanda and Tanzania", Politics and Governance, 2022.

DIGITAL FINANCE AND THE NEW GEOPGRAPHY OF ARMED CONCLICT

Eastern Africa's digital financial revolution is one of the continent's most celebrated achievements. Kenya's M-Pesa pioneered mobile money, Somalia's informal economy runs substantially on mobile transfers, and Ethiopia's telebirr has extended financial access to millions.[22] Yet the infrastructure that enables financial inclusion also perpetuates new pathways for armed groups to move, launder and distribute funds.

In Somalia, for example, mobile money is ubiquitous, and Al-Shabaab, an al-Qaeda aligned Islamist group, al-Shabaab has exploited aspects of this ecosystem for taxation and logistics, often through coercive collection rather than direct use of formal mobile-money accounts.[23] In Sudan, the RSF, the primary faction currently fighting the Sudanese government in the ongoing civil war, controls of gold mining and smuggling routes potentially benefits from mobile financial channels that enable the movement of funds across regions.[24] In the DRC, M23, a rebel paramilitary group, extracts taxes and revenues from occupied territory is facilitated by informal financial channels and mobile transactions that complicate tracking, although there is limited public evidence of systematic use of more advanced digital-payment technologies such as blockchain.[25]

Nigeria's experience, though geographically distant, offers an indicative model that depicts ransom payments and insurgent revenue collection increasingly using mobile-money platforms and fintech wallets, and fragmented transfers help to avoid bulk cash movement.[26] Cameroon's Ambazonian war offers a second comparison. Mobile technology enabled mass mobilisation and diaspora coordination among separatist sympathisers, but as conflict financing spread through the same networks, it also exposed weaknesses in institutional cohesion and political legitimacy, illustrating how digital mobilisation and conflict finance can reinforce one another.[27]

As is evident, digital-finance infrastructure is expanding more quickly than security and regulatory frameworks can keep pace with it. Mobile-money penetration is highest in Africa, yet the continent's cybersecurity workforce is chronically understaffed relative to the size of the sector.[28] Blockchain analytics firms have also identified substantial flows of illicit virtual assets involving Africa-linked wallets, although estimates vary considerably by methodology and year.

The implications for Eastern Africa are seen as an increased likelihood for exploitation by armed groups and non-state actors, which is likely to grow unless cybersecurity and regulation keep pace, as mobile-money and fintech platforms spread into

[22] William Jack and Tavneet Suri, "Mobile Money: The Economics of M-PESA," *National Bureau of Economic Research Working Paper* No. 16721, 2011. The World Bank also records that Safaricom launched M-Pesa commercially in Kenya in March 2007. See World Bank, "Mobile Payments Go Viral: M-PESA in Kenya," *World Bank Working Paper*, 2009. Central Bank of Kenya, *Kenya's Payments Journey*, 2023. The report identifies the launch of M-Pesa in March 2007 and records the growth of active mobile-money customers to more than 28 million by July 2022. It also reports an increase in formal financial inclusion from 26.7 per cent in 2006 to 83.7 per cent in 2021.
World Bank, *Somalia Economic Update: Rapid Growth in Mobile Money and Digital Financial Services*, World Bank Documents and Reports. The report describes mobile money as an essential part of Somalia's economic ecosystem and identifies its use for retail payments, salary transfers, bill payments, remittances and cash transfers.
Ethio Telecom, "Ethio Telecom 2025/26 Fiscal Year First Half-Year Business Performance Report," 30 January 2026. The report states that telebirr registered 4.69 million additional customers during the first half of the financial year, bringing total users to 58.61 million.

[23] Peter Chonka, "Digital Governance and Security in the Horn of Africa", Rift Valley Institute (XCEPT programme), March 2025.
[24] Suliman Baldo, *Gold and the War in Sudan*, Chatham House, March 2025. The report examines the RSF's involvement in gold production, smuggling networks and military financing in Sudan. Available at: Chatham House.
[25] United Nations Security Council, Final Report of the Group of Experts on the Democratic Republic of the Congo, 2024. The report documents M23's control of Rubaya, its taxation of mineral production and trade, and the movement of minerals through regional smuggling networks.
[26] A. Mustapha, "Nigerian Jihadists and Bandits Exploit Emerging Fintech", Terrorism Monitor 23(10), Jamestown Foundation, 2025.
[27] J. Asongu, "Mobile Technology and the Ambazonian Conflict: Digital Mobilization, Cyber Exposure, Conflict Finance and the Limits of Networked Resistance", International Journal of Scientific Research and Modern Technology, 2026.
[28] Carnegie Endowment for International Peace, "Security and Trust in Africa's Digital Financial Inclusion Landscape", 2024.

rural and conflict-affected areas. Peacebuilders and PeaceTech practitioners therefore have a case for developing tools that divert attention from illicit channels, reduce their consequences and strengthen peace-finance portfolios. This dimension of digital geopolitics is probably as important to the region's conflict economies as shutdowns or disinformation, yet it receives far less policy attention.

DIGITAL TECHNOLOGY AND DIPLOMACY

Scholarship on digital diplomacy suggests that states can project influence and manage relations by integrating digital technologies into foreign policy and that there are risks in ignoring the trend or in embracing it unevenly. [29] In Africa, the same literature finds that digital diplomacy remains uneven and often ad hoc. Unfortunately, the practice is outpacing the research, policy, and institutional development needed to support it.[30]

Across Eastern Africa, diplomats and international organisations increasingly use social media to engage with publics and partners. These tools have also improved advocacy and mobilisation by non-governmental organisations. [31] The platforms are open to everyone, however, and they also carry provocation and false information, particularly around elections. This is a feature of the platforms themselves and not a consequence of diplomatic engagement, but it means that diplomats work in the same information space as the actors they are trying to counter.

Kenya has been a pioneer, and a comparatively reliable regional user, of digital tools in foreign policy. Research finds that digital technologies have remarkably amplified the effectiveness and visibility of Kenyan foreign policy, in addition to increasing its responsiveness. However, the cybersecurity weaknesses, coupled with a lack of institutional alignment and capacity-building, limit the extent to which these gains can be sustained.[32] A longer view of Kenya's digital diplomatic communication across the region since 2013 reaches a similar conclusion: institutional gaps and evolving legal/regulatory frameworks persist; nonetheless, the trajectory is one of steady, if uneven, progress.[33] Other assessments show that Kenyan digital diplomacy has depended heavily on internet connectivity and political leadership. It is also evident that public diplomacy runs largely through social media and not formal institutional channels. [34] Further, comparative work on Kenya and South Africa concludes that digital diplomacy has become a genuine instrument for advancing African states' foreign-policy goals. However, its institutionalisation lags well behind its use in practice.[35]

Ethiopia presents a completely different scenario. The government that shuts down networks also courts digital diplomacy when it serves the national interest. Research on Ethiopia's use of e-tools in diplomacy finds that digital diplomacy has helped Addis Ababa to articulate and pursue foreign-policy objectives around democratisation, development and national prestige. [36] Shutdown and digital engagement are therefore two settings of the same infrastructure, deployed selectively according to the government's calculation of what connectivity threatens and what it can be made to serve.

Institutional gaps and risks

Institutionally, PeaceTech and diplomacy remain separate. The literature reviewed documents digital tools in Eastern African foreign ministries mainly as instruments of communication and public diplomacy. Thus, it does not document dedicated PeaceTech units that bring together diplomats, technologists, data analysts and mediation experts to apply digital tools to conflict prevention. Kenya, the region's most advanced case, illustrates this pattern: its civic and institutional early-warning tools are well developed, but their integration with the ministry's digital work remains limited.

Accordingly, the digital-diplomacy literature is

[29] O.S. Adesina, "Foreign Policy in an Era of Digital Diplomacy", Cogent Social Sciences, 2016; Corneliu Bjola and Ilan Manor (eds.), The Oxford Handbook of Digital Diplomacy (Oxford: Oxford University Press, 2024).
[30] B. Wekesa et al., "Introduction to the Special Issue: Digital Diplomacy in Africa", South African Journal of International Affairs, 2021.
[31] Muaka, "The Role of Social Media in Facilitating Diplomatic Engagements in East Africa: A Comparative Study of Kenya and Rwanda", University of Nairobi, 2022.
[32] H.W. Njiru et al., "The Effect of Digital Technologies on Kenya's Foreign Policy", International Journal of Research and Innovation in Social Science, 2026.
[33] W.A. Kimathi et al., "The Nature and Scope of Kenya's Digital Diplomatic Communication within the Eastern African Region, 2013–2025", International Journal of Research and Scientific Innovation, 2026.
[34] K.K. Ian et al., "Kenya's Foreign Policy and Diplomacy in Digital Space", EPRA International Journal of Research & Development, 2025.
[35] Mutisya, M., P. Maluki and K. G. Adar, "The Role of Digital Diplomacy in Advancing Foreign Policy in Africa: The Case of Kenya and South Africa," Journal of African Foreign Affairs 11, no. 3 (2024).
[36] M.Y. Ayenew, "Relevance of Digital Diplomacy in Promoting the National Interest of States: Reflection on the Ethiopian Case", Cogent Social Sciences, 2024.

concerned largely with visibility and responsiveness. It therefore says little about using these tools to link diplomacy with conflict prevention. Hence a noteworthy lacuna, because diplomacy is also where norms for security technologies are set. Yet artificial intelligence (AI) is progressively being embedded in security practice in parts of the region, such as drone operations and counter-terrorism targeting in Somalia or wider Horn to AI-enabled surveillance and predictive policing. Therefore, regional oversight and normative frameworks remain underdeveloped and only partly reflect the wider international debate on appropriate military AI. The applications with the highest stakes are then left in a governance vacuum, which foreign ministries and regional organisations are well placed to help fill.

PEACETECH IN THE REGION

This section sets out what PeaceTech looks like in Eastern Africa today. It moves from institutional early-warning systems at regional and national levels to citizen-led tools and analysis at country level and assesses what each does well and where each fall short. The argument is that the toolkit is broad and effective, but that it sits largely outside diplomatic and security policy.

IGAD and the African Union: institutional early warning

Early-warning systems are among the most developed examples in the field. Intergovernmental Authority on Development (IGAD)'s Conflict Early Warning and Early Response Mechanism (CEWARN) gathers field data through National Research Institutions and processes it into conflict scenarios. Its value at the working level therefore depends on the quality of local reporting and on whether analysis reaches those who can act on it. In 2025, an IGAD CEWARN-commissioned study found that a 0.2 increase in the Normalised Difference Vegetation Index (NDVI) corresponds to a 12 per cent decrease in the probability of physical conflict in the following month. [37] This reflects an associated research analysis as opposed to CEWARN's routine operational alerts, and the distinction matters for policy. Thus, the studies of this kind show what climate and conflict data can reveal, but not the routine, trusted alerts that can change the decisions of diplomats and security actors.

At the continental level, the AU's Conflict Early Warning System (CEWS) handbook sets out best-case, worst-case and most-likely-case scenario construction as a key analytical stage.[38] The method is simple and transferable, which is its strength. Its weakness, as the Kenyan case below suggests, is that scenarios are only as useful as the channels that carry them to decision-makers.

Citizen-led and research-based tools

Alongside these institutional systems, civil society and research organisations have built tools for tracking online harm. Policy's Byte Bullies study analysed online activity around Kenya's 2022 elections and developed a machine-learning model able to identify online violence and hate speech in English and Swahili, even though the tool was a research output, not a platform deployed for real-time detection.[39] ISD Global monitored divisive content ahead of the same elections by combining natural language processing with skilled manual analysis.[40]

Therefore, the quality and scope of these tools vary considerably, and taken together they form the region's PeaceTech toolkit. What stands out is who owns and operates each part of it. Institutional early warning sits with regional organisations and states, sentiment analysis with research organisations, and crowdsourcing with civic groups. Few of these tools are designed to speak to one another, and fewer still to foreign or security policy. Kenya is the clearest case of layering, and even there the layers are only loosely connected to the foreign ministry's digital work described above.

Kenya: disinformation, verification and election integrity

Kenya exemplifies both the potential and the institutional depth of digital peacebuilding in the region. Ushahidi, founded in Nairobi during the 2007–2008 post-election violence, pioneered the crowdsourcing of crisis information by SMS and web. Its first prototype was created within days, and it enabled any mobile phone user to report an incident and have it appeared on a live public map.[41] Its legacy has shaped a generation of civic-technology tools across the continent. More recent initiatives build on this foundation, including Maskani Commons, which has established online debate spaces in Kenya's informal settlements, extending participation to populations often excluded from formal engagement. The Sentinel Project's Una

[37] IGAD CEWARN, "Climate-Conflict Nexus in the IGAD Region", 2025.
[38] African Union, "Conflict Early Warning System Handbook".
[39] Pollicy, "Byte Bullies", 2023.
[40] ISD Global, "Polarising Content and Hate Speech Ahead of Kenya's Elections".
[41] "Inter-Ethnic Cooperation Revisited: Why Mobile Phones Can Help Prevent Discrete Events of Violence, Using the Kenyan Case Study", Stability: International Journal of Security and Development, 2013; The Guardian, "Ushahidi: crowdmapping collective that exposed Kenyan election killings", 7 April 2011.

Hakika, an established SMS-based rumour-tracking effort in the Tana Delta, forms part of a wider fact-checking and content-integrity ecosystem (including PesaCheck and various parliamentary-monitoring tools) that works to counter disinformation before it inflames local disputes.[42]

The state subsequently developed its own institutional capacity, domesticating the IGAD system into a National Conflict Early Warning and Early Response System (NCEWERS). Today, NCEWERS uses an online platform, the National Early Warning Information System (NEWIS), to relay situation reports, media monitoring and SMS-based alerts, drawing on geographic information systems (GIS) and the Swiss Peace Foundation's FAST analytical model. Kenya's National Steering Committee applied the scenario method in 2013, combining statistical research, field monitoring and GIS modelling to map potential electoral-violence hotspots.[43]

The Kenyan case shows that locally created infrastructure, sustained over more than a decade, can deliver lasting benefits across communities. It also shows the limits of such tools. Verification can identify falsehoods, but it cannot resolve the land, resource and political grievances that misinformation exploits. This points to the breadth of what PeaceTech can be. Tools can advance economic security, education for peace and many other fields. Yet Kenya's PeaceTech remains concentrated in early warning and verification, which leaves a diversification gap. Closing it requires rethinking peacebuilding beyond reactive mechanisms and towards sustainability, so that technology addresses the conditions that produce conflict as well as the crises that follow. Finally, it illustrates the disconnect with which this article is concerned. Kenya's civic-tech achievements in election monitoring and verification have outpaced the institutionalisation of digital tools in its own foreign ministry, and the two are rarely examined together.

Ethiopia: platforms, incitement and shutdown

Ethiopia is the most striking example of what might be called the dual-use continuum in Eastern African PeaceTech and one of the countries where digital freedom is unpredictable. Algorithmic amplification of hate speech accompanied the fighting in Tigray and Amhara, while the government's blocking of networks prevented independent reporting for months at a time.[44] To the extent that Freedom House's 2024 assessment classifies Ethiopia's internet as "Not Free", such actions by state agencies curtail innovation and even slow down economic activities.[45]

Shutdowns also have humanitarian costs that extend beyond censorship. Without connectivity, relief organisations cannot arrange logistics, hospitals cannot access medical data or reporting networks, and families cannot locate one another. Because shutdowns also make documentation harder, the damage in affected areas is probably far greater than what has been recorded.

Within this constrained space, Ethiopian civil society has nevertheless built verification capacity. HaqCheck, an Ethiopia-based fact-checking organisation set up around 2020, has debunked thousands of misleading posts and trains others in verification. Much of the misinformation it handles concerns internal conflict, border disputes and the diplomatic tension with Somalia over the Somaliland port deal.[46] Ethiopia Check, supported by Internews, works in a similarly sensitive environment and has stressed the need for care in language and verification if it is to remain unbiased.[47] When seems like a salient trend in Africa, the legal framework is a further constraint. For example, the proclamation No. 1185/2020 on hate speech and disinformation, in force since March 2020, has been criticised by ARTICLE 19 for its broad definitions and its potential use against critics of the government.[48] Ethiopian PeaceTech thus operates between shutdowns on one side and restrictive regulation on the other, while the state's own digital diplomacy, described above, presents a more open face abroad.

[42] Sheila Akinyi Owino, "Becoming a Maskani Digital Peacebuilder" Knowledge Platform Security & Rule of Law, 17 November 2020. Maskani Commons was established through a collaboration between Rongo University's Centre for Media, Democracy, Peace and Security and the organisation Build Up. It brought together approximately sixty students from six public universities in western Kenya and trained them to address polarising political, ethnic and COVID-19-related narratives through their own social-media networks.

[43] IGAD Resilience, "Taifa Lango, Jukumu Langu", 2013.
[44] Freedom House, "Ethiopia: Freedom on the Net 2024 Country Report", 2024.
[45] Ibidem
[46] "Ethiopia: Fact-Checkers in Ethiopia Take On Disinformation Amid Rising Tensions", allAfrica, 31 January 2025,
[47] Internews, "Ethiopia Check".
[48] ARTICLE 19, "Ethiopia: Hate speech and disinformation law must not be used to suppress the criticism of the Government".

Somalia: countering violent extremism and mobile stabilisation

In Somalia, mobile money plays an equivocal role. The formal banking sector remains limited outside the main urban centres, so mobile money is both essential to financial inclusion and a channel that al-Shabaab has used for logistics and taxation.[49] Chonka's 2025 study for the Rift Valley Institute also examines how social media governance and online misinformation and disinformation, including the role of digital diasporas, cut across security in Somalia, which reinforces the point that finance, information and security cannot be treated separately.

Counter-narrative work has centred on radio and SMS. Local NGOs have experimented with chatbot-style tools to educate young people on rights and dispute resolution and to reach across polarised media silos, although thorough evaluations of these tools are still scarce.[50] Taken as a whole, the Somali case shows how PeaceTech operates where sovereignty is legitimately disputed and no single actor, whether state, clan or international organisation, has full control over the physical or digital environment.

South Sudan: hate-speech reduction and civic dialogue

South Sudan's digital peacebuilding grew out of the way in which social media was used to fan the war that blew up in December 2013 and again in July 2016. The #defyhatenow initiative was launched in early 2014 by the Berlin-based r0g_agency for open culture and critical transformation, working with South Sudanese partners including the Community Empowerment for Progress Organisation (CEPO) in Juba. It was supported from 2015 to 2018 by the German Federal Foreign Office through the ifa/zivik programme and, from 2016, extended to Kenya, Uganda and Sudan. Its outputs included a social media hate-speech mitigation field guide, media-literacy training, and campaigns such as #PeaceJam and #ThinkB4UClick.[51] Locally created monitoring of peace-agreement implementation has followed a similar logic, and women-led WhatsApp networks have used encrypted messaging and digital storytelling to amplify women's voices in a peace process from which they have often been formally excluded.

The South Sudanese case also underlines that data protection is a precondition for digital peacebuilding, not an afterthought. Identifying people who report hate speech or share testimony can expose them to real physical risk in a context of continuing armed mobilisation. It is also a reminder that much of this work was donor-funded and time-bound, which is the structural dependence to which the conclusion returns.

Sudan: diaspora mobilisation and emergency response rooms

Since the Sudanese civil war began in April 2023, social media platforms including Facebook, X and TikTok have become what one observer describes as a "central operational environment". They shape the political and security trajectory of the war.[52] Diaspora-based influencers operating from France, Canada, the Gulf and the Netherlands have built large followings and held live interviews with field commanders, shaping the narrative. Specific instances of direct influence on military decisions remain difficult to verify and should be treated with caution.

Against this backdrop, technologically coordinated mutual aid has also grown. Since 2023, Local Emergency Response Rooms have organised soup kitchens and evacuation routes and documented abuses using open sources, coordinating through social media and encrypted chat. The Sudanese case therefore shows that digitally mediated solidarity can be remarkably resilient, sustaining aid delivery where formal humanitarian access has collapsed. However, they can remain brittle and exposed to the same platform outages, surveillance and disinformation that shape the military side of the war.

---

[49] Chonka, "Digital Governance and Security in the Horn of Africa", 2025.

[50] Sara Zeiger, "Undermining Violent Extremist Narratives in East Africa: A How-To Guide" (Hedayah and IGAD Centre of Excellence for Preventing and Countering Violent Extremism, 2018), documenting the use of community radio, WhatsApp and peer-to-peer messaging by Kenyan initiatives, including SaSaa Media, to circulate alternative narratives and facilitate youth-focused discussions on human rights, livelihoods, conflict resolution and the prevention of violent extremism,

[51] #defyhatenow, "#defyhatenow South Sudan" and project history, and; UNMISS, "CEPO launches social media campaign #PeaceJam against online hate speech".

[52] Hamad, "The Weaponization of Social Media in Sudan's War", 2026; EUAA, "Members of the Resistance Committees (RCs) and Emergency Response Rooms (ERRs)"; The Guardian, "'You sneak in and hope you make it back': the Sudanese volunteers risking it all to bring care to millions", 24 December 2025.

Eastern DRC: mapping violence in the Great Lakes

Eastern DRC is a laboratory of information warfare in its own right. Research describes how social media has augmented the reach of "Xerox soldiers, YouTube commanders and Twitter brigades", condensing the distance and time of propaganda and, for better and worse, democratizing who can shape the narrative, from armed groups to ordinary residents with a smartphone.[53] There are conflict-tracking programmes that combine satellite imagery with mobile reporting and have tried to record territorial control, abuses and displacement in near real time during the M23 crisis. Broader research on digital mapping in territorial disputes suggests that such tools can significantly inform negotiations, sometimes by producing a shared evidentiary picture and sometimes by creating new problems when the parties dispute the map itself.[54]

Further, the DRC belongs to the EAC and sits close to IGAD and other regional mechanisms, which creates coordination challenges for data-sharing and response. Violence, mineral flows and refugee movements do not respect the borders that divide national reporting systems, nor does the digital mapping infrastructure designed to monitor them. The eastern DRC case therefore points to the need for regional, cross-border data-sharing agreements, a point taken up in the conclusion. Also, PeaceTech must also be understood through culture, which shapes how data is produced, shared and governed. The Democratic Republic of the Congo is francophone, whereas most of its Eastern African neighbours operate in English. This difference strains collaboration and synchrony, and it limits the fluidity of innovation, application and governance across borders. Tools, data and standards developed in one language do not transfer easily to the other. These issues must be weighed in any assessment of the DRC's regional dynamics, security and prospects for peace.

Risks and perspectives

Given this context, practitioners identify a distinct set of risks for PeaceTech tools in the region, each with a working-level consequence. The first is bias. AI models trained mostly outside the region perform unevenly in local languages and contexts, and AI-generated outputs are often hard to trace to their original sources, making it difficult for an analyst to verify them before they feed into an alert. The second is data sovereignty and privacy. Commercial digital platforms are frequently hosted outside the region, so data on hate speech, incidents and participants may fall under foreign jurisdiction and be governed by terms that peacebuilders do not control. The third, and possibly the most pernicious, is the "dehumanisation" of mediation. Procedures that are AI-mediated may appear efficient, but their impersonality can marginalise the face-to-face communication and empathy on which mediation depends. The fourth is a cross-cutting gap in exchange between peacebuilders and the region's security and cyber communities. PeaceTech remains little appreciated in diplomatic and military circles, while digital peacebuilders and cybersecurity experts do not systematically share knowledge, data or approaches, even where their subject matter overlaps directly, as in the monitoring of hate speech or the security of civic data.

Overall, it emerges that Eastern Africa already has regional early-warning mechanisms, national systems and a vigorous civic tradition. Its weakness lies in the connections between them. PeaceTech remains detached from diplomacy and peacebuilders rarely work alongside security and cyber experts, except for a few young start-ups like AI for Peace Africa. Locally owned tools stay disconnected from the platforms and data infrastructure on which they rely. The country cases that follow test this argument. Each sets out the current situation, what works, what does not, and where the links to diplomacy and security break down.

[53] C.N. Vogel and J. Musamba, "Xerox Soldiers, YouTube Commanders and Twitter Brigades: Information Warfare in Eastern Congo", International Affairs 100(4), July 2024, 1381–1404.

[54] J. Branch, "Territorial Conflict in the Digital Age: Mapping Technologies and Negotiation", International Studies Quarterly, 2017.

MAINSTREAMING PEACETECH THROUGH PEACE ARCHITECTURES

Research on the limits of digital peacebuilding offers a useful caution. Despite their promise, digital initiatives cannot address the older, analogue dynamics of state formation, territorial control and contested legitimacy that continue to fuel conflict across the region.[55] The cases above show this consistently. In Sudan, diaspora solidarity networks cannot replace humanitarian access or a negotiated end to the war; in the DRC, mapping technology cannot on its own resolve disputed territorial claims; and in Kenya, verification tools cannot resolve underlying land conflicts. Digital peacebuilding makes a genuine but limited contribution. It must therefore be connected to the region's wider peace and security architecture through a working mechanism that allows information and action to move fluidly between the two. The same applies across the full spectrum of PeaceTech. As geopolitics, peace and security structures converge, many factors must be weighed together. Stakeholders must therefore be drawn from every sphere of the state and the region, not only from the peace and security sectors. Climate and natural resources show why. They are among the main causes of conflict in the Horn, and they are bound up with how states relate to one another and to non-state actors under their foreign policies. The argument is one of convergence. Technology, climate, resources, diplomacy and security must meet, and they must rest on the regional peace and security architecture already in place. That architecture is the backbone on which any lasting peace depends.

This article has argued that digital technologies do more than add new tools to old conflicts in Eastern Africa. They remould who controls information, how armed actors are financed and who owns the infrastructure on which both depend. Shutdowns turn connectivity from a public good into an instrument of war, as in Tigray and Amhara. Social media platforms have become operational environments in which diaspora influencers inform the course of the fighting, as in Sudan. Mobile money and fintech open new channels through which armed groups can move funds faster than regulators can adapt. Foreign-built infrastructure and cyber-espionage allegations show how dependence erodes sovereignty, and polyalignment, though an expression of African agency, leaves states more exposed to that dependence, not less.

In light of these considerations, the article showed how the region has a vigorous PeaceTech ecosystem spanning from Ushahidi and #defyhatenow to Sudan's Emergency Response Rooms and the early-warning systems of IGAD and Kenya. Yet that ecosystem is peripheral in two ways: it is marginal to state and regional security frameworks. We see it is mostly dependent on externally owned platforms, data infrastructure and short-term donor funding. This double peripherality limits the legitimacy and impact of digital peacebuilding. The recommendations below follow directly from the gaps identified in the article.

[55] O.P. Richmond et al., "Analogue Crisis, Digital Renewal? Current Dilemmas of Peacebuilding", Globalizations, 2020.

RECOMMENDATIONS

RECOMMENDATIONS	
1	**The African Union** should anchor the proposed Digital Peace Platform and link the Conflict Early Warning System with its own digital and cyber work. It should also press for ratification and implementation of the Malabo Convention, so that the Convention's data-protection and cybersecurity obligations bind more states.
2	**IGAD** should build on CEWARN by opening a regular channel between its analysts and the region's cyber and security communities. It should also distinguish clearly between research analyses and routine operational alerts, because decision-makers will then trust the alerts.
3	**The East African Community** should develop cross-border data-sharing arrangements to monitor violence, mineral flows and displacement. It should begin with eastern DRC, where national reporting systems stop at borders that violence ignores.
4	**National governments** should bring PeaceTech into foreign-ministry digital strategies and cybersecurity capacity-building, since the Kenyan case suggests this is still needed. They should also refrain from network shutdowns, because the Ethiopian case shows their humanitarian costs and their damage.
5	**The EU, Italy and other external partners** should support capacity-building and sustained core funding for locally rooted tools, rather than relying on project-based grants. At the same time, they should not displace local ownership of the tools and data, and they should reconcile security and defense priorities with the peace-promotion agenda (digital geopolitics section).
6	**Technology companies** should protect the data of people who report hate speech or give testimony, as the South Sudanese case shows to be essential. They should also improve moderation and detection tools in regional languages such as Swahili, so that harmful content is caught where it actually circulates.
7	**Civil society and peacebuilders** should adopt shared data-protection standards, and they should engage security actors selectively, where interests overlap and safeguards exist.

A PLEA FOR AN EASTERN AFRICA DIGITAL PEACE PLATFORM

The Platform would be a lightweight, primarily digital mechanism. It would give peacebuilders, diplomats, and security and cyber experts a dedicated space to exchange information, lessons and practices on PeaceTech in specific Eastern African contexts, a space that is currently missing.

The African Union could anchor the Platform, and IGAD and the EAC could endorse it. Meanwhile, the EU, Italy and other partners could support capacity-building without displacing local ownership of tools and data. The design would need to guarantee participants' independence and enforce strict data-protection safeguards. Each state would also decide whether and how to take part.

Its objectives could include:

- Building a regional network that links peacebuilders with security and cyber communities;
- Connecting early-warning systems such as CEWARN and NCEWERS with digital and cyber expertise;
- Supporting the cross-border data-sharing arrangements that eastern DRC requires;
- Developing tools tailored to regional languages and contexts, rather than imported models;
- Channeling sustained support, in place of project-based funding, to locally rooted initiatives.

At a strategic level, the Platform could shift the region's digital agenda. That agenda now leans towards unchecked securitisation and great-power competition, whereas the Platform would move it towards a fuller account of technology's contribution to peace. As a result, PeaceTech would enter national strategies and the regional security equation, instead of remaining a promising but marginal field of practice.



AGENCY FOR
PEACEBUILDING

www.peaceagency.org