RESILIENCE
TECHNOLOGIES

2024 IN REVIEW

ADVANCING DIGITAL SAFETY AND RESILIENCE ACROSS AFRICAN CIVIL SOCIETY

A Comprehensive Report on Our Achievements, Milestones, and Impact in 2024.

Introduction

SPYWARE, SURVEILLANCE AND STATE-SPONSORED ATTACKS

The year kicked off with NSO Group famous for their spyware Pegasus trying to make a comeback through lobbying that positions the company as essential to global cybersecurity. In addition, several cases against the organisation were either dropped or dismissed. This year, we saw reports of persistent attacks and surveillance targeting journalists, civil society organisations and activists from as far back as 2019.

Governments around the world increasingly targeted civil society organisations for state-sponsored cyber actors, especially countries like Russia, China, Iran, and North Korea. U.S. cybersecurity agencies have issued warnings about these malicious actors focusing on NGOs, think tanks, and human rights activists. The primary goals of these attacks include intimidation, surveillance, and undermining democratic values.

ELECTION, MISINFORMATION AND FREE SPEECH

With national elections in over 50 countries and over half the global population eligible to vote, 2024 was a monumental year for democracy. The year saw the fundamental mechanisms of democratic discourse being reshaped by sophisticated digital technologies that churn out and amplify misinformation and hate speech faster than ever. In the buildup to the 2024 U.S. presidential election, there was a significant proliferation of deepfake videos using names and insignia of known individuals and organisations to spread misinformation about the election.

Platform governance also emerged as a critical battleground for digital rights. Major technology companies have demonstrated an inconsistent and often opportunistic approach to content moderation and user protection. While presenting themselves as neutral technological platforms, there have been documented patterns of undue removal and suppression of protected speech including peaceful expression in support of Palestine and other worn-torn countries as well as content related to elections.

SPYWARE, SURVEILLANCE AND STATE-SPONSORED ATTACKS

As of March 2024, there were 22 intentional internet shutdown events recorded across 12 countries, with India experiencing the highest number (9 events). Other countries affected include Ethiopia and Senegal, each with 2 events. As of December, there's been over 130 internet shutdowns across the world with India having the most at over 50 blackouts this year. These shutdowns happened for a variety of reasons including cable damage, natural disasters, government interruption and military action. These shutdowns are no longer blunt instruments but sophisticated operations that can target specific regions, platforms, or communication channels with remarkable precision. Governments employed multi-layered strategies that can include partial bandwidth throttling, selective platform blocking, mobile network interruptions and targeted platform restrictions.

Several African nations implemented internet shutdowns during elections and political tensions including Comoros, Mauritania, Mozambique and Mauritius. The Nigerian Government was alleged to have intentionally disrupted the internet amid the nationwide #EndBadGovernance protests.

At Resilience Technologies, 2024 was filled with growth, impact, and steadfast dedication to digital resilience. We strengthened our commitment to safeguarding African civil society organisations and at-risk communities, delivering innovative solutions tailored to their unique challenges.

From empowering media organisations and human rights defenders in Nigeria through our "Infrastructure Hardening and Digital Resilience" project to engaging with communities across the continent, we championed cybersecurity awareness, capacity building, and digital safety. We championed Africa's first homegrown Spyware Fellowship where we trained and equipped the next generation of digital defenders. We lent our voice to create change alongside other organisations under the leadership of the Committee to Protect Journalists (CPJ), to provide crucial feedback to the U.S. Commerce Department on the proposed rules aimed at strengthening regulations on the export of surveillance technologies. We also trained multiple organisations across Africa in various events.

We also achieved significant milestones, including a stronger online presence, impactful publications and resources, and active client and community engagement. As we look ahead, we remain steadfast in our mission to lead the charge in digital security solutions, ensuring a safer internet for civil society across Africa.

Together, we are building a resilient digital future!

State of the Industry

This year, we witnessed firsthand the mounting challenges Civil Society Organisations faced in navigating an increasingly hostile digital environment. The year 2024 has underscored the urgent need for comprehensive strategies to safeguard the digital ecosystems in which CSOs operate, as cyber threats continue to evolve and intensify.

One of the pressing issues is the prevalence of cybersecurity breaches. Our fieldwork revealed that malicious actors; ranging from opportunistic hackers to politically motivated entities , target CSOs and their sensitive data repositories. A recent survey conducted by West Africa Civil Society Institute (WACSI), also supports this, revealing that nearly a third of organisations in West Africa reported digital security breaches.

Exacerbating this problem is the widespread lack of digital security awareness among CSO staff. Many organisations struggle to implement even basic digital security protocols and policies such as multifactor authentication or regular system updates, due to knowledge gaps. In our training sessions, we have encountered instances where staff were unaware of how to identify phishing attempts or secure their communications. This lack of preparedness leaves organisations vulnerable to increasingly sophisticated cyber threats.

Further, resource constraints compound these vulnerabilities. Many CSOs operate on shoestring budgets or large budgets solely focused on programmatic activities rather than having dedicated resources for cybersecurity investments. This tradeoff leaves them exposed to potentially crippling attacks that may end up impacting even the programmatic activities. In our engagements, we have found that even those organisations that recognise the importance of digital security often lack the funding to implement necessary changes.

We also observed external challenges and pressures that pose significant barriers to CSOs operations in Africa. Restrictive legal frameworks, for example, continue to undermine digital freedoms. In April 2024, for instance, Malawian journalist Macmillan Mhone was arrested under cybercrimes charges for exposing corruption. State surveillance and the use of sophisticated spyware technologies also represent critical threats as they create an atmosphere of fear, erodes trust, stifles dissent and in many cases causes loss of lives.

On our radar, we are also monitoring the use of emerging technologies such as artificial intelligence and machine learning, to enable cyberattacks such as microtargeted phishing campaigns that exploit specific vulnerabilities in individuals or organisations.

Despite these existing and future challenges, we are optimistic that through continued collaborative efforts by stakeholders and innovative interventions, it is possible to build the resilience of CSOs and at-risk groups in Africa.

Innovation We've Championed:

In 2024, we spearheaded several initiatives to empower civil society organizations, activists, and innovators across Africa to strengthen their digital resilience. These projects not only addressed pressing digital security challenges but also laid the foundation for scalable, long-term solutions.

RT-10 PROJECT REPORT

In 2023, we initiated the RT-10 project which was a research-driven initiative aimed at developing a scalable framework for cybersecurity intervention for CSOs in Sub-Saharan Africa. Working with CSOs across Uganda, Zimbabwe, Kenya, Nigeria, Ethiopia, and Tanzania, we carried out robust security assessments, capacity training and infrastructure hardening. This project then culminated in the creation of the Resilience Model, a plug-and-play framework designed to address CSO-specific cybersecurity challenges. In 2024, we released a report on our findings during the project, as a valuable resource for the civil society.

KEY IMPACT:

01

The RT-10 Report is a comprehensive resource offering actionable insights & recommendations to enhance digital security practices for CSOs in Sub-Saharan Africa.

02

Highlighted the Resilience Model within the report, providing a scalable, plug-and-play framework tailored to CSO-specific cybersecurity challenges.

03

Presented findings from the RT-10 Report at DRIF24, with plans for broader dissemination at RightsCon25.

SPYWARE FELLOWSHIP 2024

The deployment of advanced spyware tools such as Pegasus and Predator by state actors has significantly impacted civil society across Africa. These surveillance technologies, ostensibly designed to combat crime and terrorism, have been repurposed to monitor and suppress journalists, activists, and political opponents, thereby undermining democratic processes and infringing upon human rights. Recognising this urgent threat, we launched Africa's first-ever Spyware Fellowship. This 4-month program equipped young cybersecurity professionals with skills in mobile forensics, OSINT, spyware mitigation, laws and policies and an introduction to the Civil Society space in Africa.

KEY IMPACT:

01

Fellows gained technical expertise to detect and respond to spyware attacks.

02

Collaborative mentorship and projects fostered community building among participants.

03

A standout capstone project, *"Spyware Governance in Africa and the Impact on Civil Liberties"*, paved the way for critical policy recommendations.

INFRASTRUCTURE HARDENING FOR MEDIA ORGANIZATIONS AND HUMAN RIGHTS DEFENDERS

We provided tailored solutions to help media organizations and human rights defenders in Nigeria combat escalating cyber threats. Over three months, Resilience Technologies conducted security assessments and training sessions, empowering organizations to protect their digital ecosystems.

KEY IMPACT:

01

Critical vulnerabilities in infrastructure were identified and mitigated.

02

Staff were trained to recognise and respond to digital threats.

03

Organizations are now equipped with sustainable security practices to continue their work without disruption.

DIGITAL SECURITY TRAINING FOR WOLE SOYINKA CENTRE FOR INVESTIGATIVE JOURNALISM

We delivered a tailored training program to Nigerian journalists at the Wole Soyinka Centre for Investigative Journalism. This training focused on mitigating sector-specific cyber risks while building capacity in secure data management.

KEY IMPACT:

01 Journalists gained a deeper understanding of sector-specific cyber risks and practical strategies to safeguard their digital presence and reduce online risks.

02 Participants developed the capacity to securely manage sensitive information, ensuring the confidentiality and integrity of their investigative work.

TRAINING PARTNERSHIP WITH WEST AFRICA CIVIL SOCIETY INSTITUTE (WACSI)

In collaboration with WACSI, we hosted a 5-day training program for CSOs in Nigeria, focusing on digital safety, data protection, and social engineering awareness. This initiative empowered civil society actors to safeguard their communities and promote digital rights.

WACSI
WEST AFRICA CIVIL SOCIETY INSTITUTE

KEY IMPACT:

01

Participants gained actionable knowledge to improve security practices.

02

The training fostered advocacy for safe and inclusive digital environments.

03

Organizations left equipped with policies to sustain digital resilience.

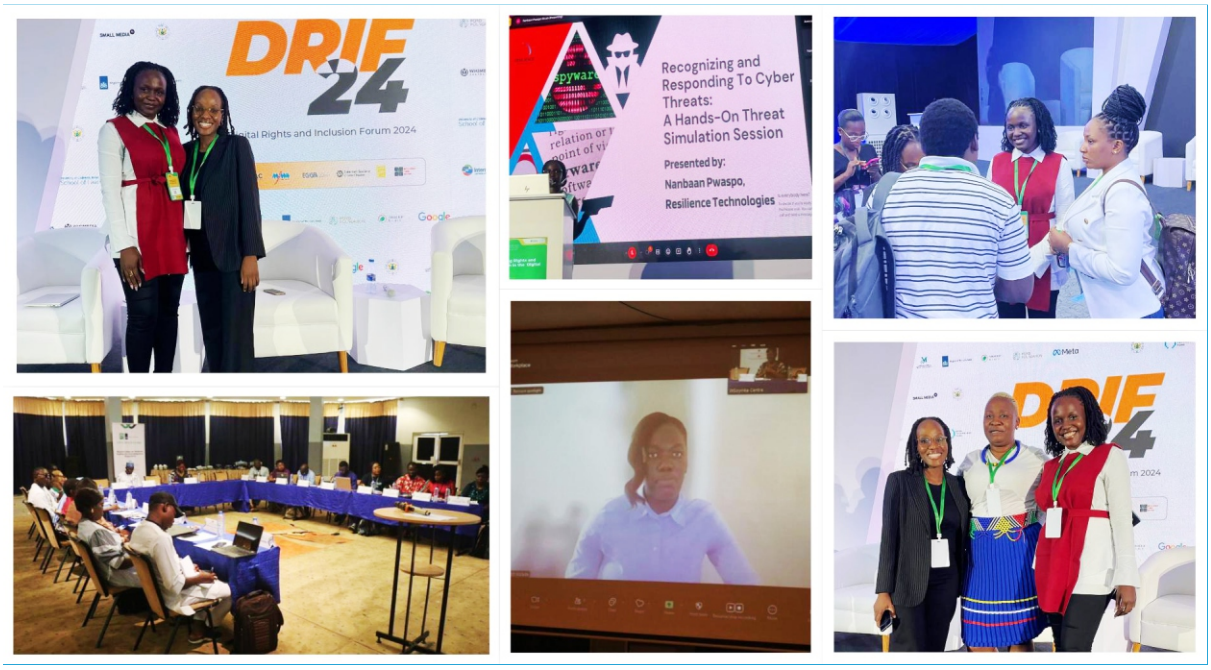
We Believe Dialogue is Crucial

In 2024, we lent our voices and participated in multiple external projects, and events where the future of digital resilience for Africa's Civil Society is being shaped. We believe that having pertinent conversations is key to creating the safe digital space that we want.

We facilitated two sessions at this year's **Digital Rights Inclusion Forum** (2024), speaking on how the Resilience Model is indeed a research-based model for cybersecurity intervention in Africa as well as a hands-on simulation of recognising and responding to digital threats. It was a pivotal platform where conversations on digital policy in Africa are shaped, policy directions debated and partnerships forged for action.

At the **Masterclass on Holistic Safety for Investigative Reporters** organised by the Wole Soyinka centre, we facilitated a digital security training with focus on how best to avoid and mitigate against threats and attacks. Sessions like these enable us to empower team members to fight against digital threats so that the great work of defending human rights can go without any hitches.

We were also live in Portugal for the Global Gathering that brought together over 1,000 digital rights defenders that work at the intersection of human rights and technology to have vital conversations on **Advancing Digital Rights Resilience through Community Building and Solidarity**. For us, it was a moment to lend our voice and expertise to the ongoing work, as well as network with hundreds of other organisations, and create collaborations that will shape the future of digital security for Civil Society Organisations.


DRIF 24
Digital Rights and Inclusion Forum 2024
Recognizing and Responding To Cyber Threats: A Hands-On Threat Simulation Session
Presented by:
Nanbaan Pwaspo,
Resilience Technologies
spyware

Expert Forecast

In this insightful series of interviews, Elizabeth Kolade (Executive Director), and Anthony Sule (Director of Security and Innovation) here at Resilience Technologies, discuss the evolving digital security landscape for African Civil Society Organizations (CSOs). They share their perspectives on emerging threats, strategic approaches to resilience, and the critical role of collaboration, innovation, and funding in safeguarding CSOs against an increasingly complex array of digital challenges. Their expert insights underscore the importance of adaptability and proactive measures in building a secure digital future for civil society in Africa.

INTERVIEW WITH ELIZABETH KOLADE

RT: How do you envision organisations like Resilience Technologies contributing to the broader digital resilience of CSOs in Africa by 2025 and beyond?

Elizabeth: By working with CSOs where they are, Resilience Technologies is taking a multidimensional approach that cuts across people, process and technology to develop sustainable and scalable strategies and solutions that align with their unique contexts. We are building an ecosystem that is resilient to emerging threats by leveraging threat intelligence sharing, capacity building, incident response readiness, and continuous feedback loops to ensure adaptability and drive long-term innovation.

RT: How do you encourage cross-departmental learning and sharing of best practices around digital security?

Elizabeth: Cross-departmental learning can be encouraged by integrating security into departmental goals, creating interdepartmental teams that leverage insights and expertise across departments, promote a culture of open communication on security challenges and solutions, regular table top exercises that promotes interaction and establishing knowledge sharing platforms,

RT: What role do funders play in enabling digital resilience for African CSOs, and how can they better support this area?

Elizabeth: Resource constraints, including limited finances, human resources, and technical capacity, significantly hinder the digital resilience of African CSOs. Funders play a vital role in addressing these challenges by supporting tailored initiatives that meet the specific needs of organizations in the region. This includes subsidizing access to secure and affordable technology, funding infrastructure, and prioritizing research into emerging digital threats like those posed by Artificial Intelligence. Capacity-building programs, such as training and mentorship, can help develop local expertise, enabling CSOs to build sustainable, in-house capabilities for managing these threats.

To maximize impact, funders should foster collaboration between CSOs, technology providers, and experts by supporting knowledge-sharing networks and co-creating solutions that are contextually relevant. Sustained, multi-year funding is crucial to ensure long-term planning and resilience. By taking these proactive steps, funders can significantly strengthen the ability of African CSOs to navigate an increasingly complex digital landscape.

RT: What are the most critical skills that managers and directors of Cybersecurity Social Enterprises in Africa need to improve advocacy and service delivery?

Elizabeth: Strategic advocacy, technical expertise, and a human-centered approach are essential for driving impact and delivering excellent services in cybersecurity social enterprises. Leaders must engage effectively with policymakers, governments, and stakeholders to advocate for inclusive cybersecurity frameworks while crafting compelling narratives that emphasize the societal importance of cybersecurity. Equally critical is an understanding of cybersecurity threats and emerging technologies to design informed and practical programs that address real-world challenges.

Cross-sector partnerships and collaborations are vital for amplifying advocacy efforts and achieving broader, sustainable impact. Leaders must also focus on building resilient operational models and nurturing teams that blend technical expertise with advocacy skills. By fostering a culture of excellence, accountability, and innovation, organizations can position themselves as leaders in delivering scalable, human-centered cybersecurity solutions that strengthen digital resilience across Africa.

INTERVIEW WITH ANTHONY SULE

RT: What are the top three digital security threats that you believe will dominate for African Civil Society Organizations (CSOs) by 2025 and beyond?

Anthony: I do not expect a lot to change from 2024. The common adversary of civil society organizations on the continent are state actors, and their primary goal is to silence and sideline dissidents.

For this reason, I strongly think that Surveillance and Spyware will continue to top the chart. Infrastructure and Platform Threats/Attacks (which includes websites, social media accounts, etc) will remain prevalent and Access-based Threats (which includes phishing, password attacks, account hijacking, etc) will be up there too.

RT: How do you assess the current level of preparedness of African CSOs to face digital security challenges, and where are the most significant gaps?

Anthony: The current level is not very good, and I say this based on what a threat actor attack vs civil society defense would look like. We have ample data in-house to show that if the average CSO is sufficiently targeted, they cannot withstand digital attacks. In simpler terms: the average organisation is not resilient. The gap mostly stems from approach; we have not really taken significant steps up from what has worked in the past -even in the face of ever-changing threat actor tactics and disruptive technologies. Security operators need to design and implement more impactful, futuristic, cheaper and sustainable solutions. CSOs themselves need to prioritize digital resilience in the boardrooms and on their budgets, and funders need to make sure of this, because I have seen successful attacks disrupt multi-year advocacy programs, uncovering the identities of operators and setting them up for attacks and incarceration.

RT: What specific challenges do you anticipate with the increasing integration of AI in both cyberattacks and defenses?

Anthony: I am quite worried about new attack types facilitated by AI technologies, especially as defenses in the internet freedom space often take longer to catch up. New malware samples, social engineering techniques and web-based attacks are being deployed with alarming sophistication. The cybersecurity defenses in our space are playing catch up, and this gap -between current AI-faciliated attacks and legacy defense techniques/solutions- is the main challenge we face. The solution is to embrace AI in our defense mechanisms. So, incorporating a lot of automation, data-backed, pattern and algorithm based solutions will help us bridge that gap.

RT: What are some innovative cybersecurity solutions or tools that you believe could be game-changers for African CSOs?

Anthony: This might be very biased, but the most relevant solution that comes to mind is Zeroth Cloud. With Zeroth Cloud, we are building a solution that completely revolutionizes how civil society organisations approach threat management, not just in Africa but in the entire Global South. From 2025 when we begin deployment, we will see a lot more threat detection and response with a key focus on automation, intelligence and reporting. Zeroth Cloud will change cybersecurity for African CSOs and that is my recommended solution.

Upcoming Projects

As we look ahead to 2025, Resilience Technologies is excited to introduce groundbreaking innovations and interventions that will redefine cybersecurity for civil society in Africa and the Global South.

ZEROTH CLOUD

This month, we launched Zeroth Cloud, a groundbreaking AI-enabled solution that transforms how civil society organizations in the Global South manage cybersecurity. We designed it to address the gaps in traditional threat management approaches. Zeroth Cloud provides autonomous and continuous protection by monitoring organisations' digital environments around the clock, automatically isolating threats, executing remediative actions, and generating detailed reports for further analysis.

This innovation comes at a critical time when the cybersecurity landscape for at-risk organizations is increasingly complex. Starting January 2025, we aim to deploy Zeroth Cloud to 100 organizations most at risk, prioritising African civil society groups. For medium-sized organizations, this year-round protection will be available at an affordable rate of $4,000 per year, with provisions for complimentary access for those unable to afford it.

Zeroth Cloud represents more than a technical solution, it is our contribution to democratising access to cybersecurity. Our goal has always been to provide accessible, scalable, and innovative solutions to organisations of all sizes without the need for extensive technical expertise. Our journey in 2025 marks the first phase of this ambitious project, as we lay the foundation for a future where cost-effective and impactful cybersecurity solutions are available to all.

Over the coming years, we will continue to scale and refine Zeroth Cloud, driving down costs while enhancing functionality to reach thousands of users. By 2026, the platform will expand to support help desks managing security for multiple organizations, further amplifying its impact. Ultimately, Zeroth Cloud will evolve into a fully democratized application - an all-in-one solution that organisations can download and deploy across their infrastructure with ease, managed from a single device.

SPYWARE FELLOWSHIP 2.0

Building on the success of our inaugural cohort to further address the escalating threat of spyware targeting civil society, activists, and journalists in Africa, we will be hosting another edition of the Spyware Fellowship. The program will continue to empower participants with the technical and investigative skills needed to detect, mitigate, and respond to advanced surveillance technologies. We will be deepening the impact and scope of this project next year. More information will be shared via our newsletter.

CATCH US AT RIGHTSCON25 AND OTHER CONVENINGS

Join us at RightsCon25 holding in Taipei, Taiwan where we will host an engaging virtual session on "**The Resilience Model: A Digital Resilience Intervention Model for Civil Society Organizations."** This session will unveil the model we developed through comprehensive research with a focus group of eight civil society organizations across six Sub-Saharan African countries. The Resilience Model represents a strategic and scalable framework for strengthening digital defenses, tailored to the unique challenges faced by civil society in the Global South and we are eager to share our insights, engage with experts, and collaborate with attendees to further refine and expand the reach of this impactful intervention. Please secure your spot here.

Beyond RightsCon, you'll find us at other key convenings throughout the year as we continue to drive innovation and build partnerships in the global digital rights space.

#RightsCon25

The Resilience Model:

A Digital Resilience Intervention Model for Civil Society Organizations.

How Can You Join Us to Build Resilience?

At Resilience Technologies, we're on a mission to empower civil society organisations across Africa to thrive in a secure digital world. These organisations are at the forefront of driving positive change, yet they remain vulnerable to cyber threats that can undermine their impact. You can key into our vision to help protect their critical work and ensure they can continue advocating for human rights, democracy, and social justice.

Your support can make a difference. Partner with us, share our mission (follow us, engage with our content) to reach more organisations in need, and attend our events to champion the cause of digital resilience. You can also contribute your expertise or partner with us on innovative projects to amplify our impact.

Together, we can build a stronger, more resilient digital ecosystem for African civil society. Join us in safeguarding the work that shapes the future of our continent.

CONTACT US

🌐 www.rtafrica.org

✉ info@rtafrica.org

𝕏 @rtafrica_

Published by:

RESILIENCE
TECHNOLOGIES

www.rtafrica.org