adf
AFRICA DEFENSE FORUM

DEFENDING AGAINST HYBRID THREATS

How African Countries are Endangered by High-Tech and Emerging Tactics

PLUS

Terror Groups Test Weaponized Drones

The Promise and Peril of Social Media

VISIT US AT ADF-MAGAZINE.COM

TABLE OF CONTENTS

features

44

departments

Africa Defense Forum is available online.

Please visit us at:
adf-magazine.com

ON THE COVER:
The continent faces a range of nontraditional threats including cyberattacks, drones and information warfare. Security professionals must prepare to face these hybrid threats.

ADF ILLUSTRATION

VIEWPOINT

Sometimes it's the unexpected threats that cause the most damage. A cyberattack can paralyze a nation's power grid. Disinformation can send protesters to the streets and fuel civil unrest. Small, off-the-shelf drones can deliver deadly bomb blasts.

Known as hybrid threats, these attacks are difficult to detect or attribute to a specific group. Often, proxy actors carry out the attacks to hide their origin. They appear to be the work of a small band of local criminals but, in reality, a foreign power or extremist group is calling the shots from a distance.

These nontraditional attacks are becoming the tool of choice for groups that want to make a big impact at a low cost. Security professionals must be prepared.

For example, with more than 500 million internet users, Africa is fertile ground for cybercriminals. These cyberattacks, often small in scale, cost the continent an estimated $4 billion in 2021 and reduced national gross domestic products by 10%.

But cyberattacks are more than just an economic concern. They're also a security issue.

During the past year, the computer system that operates South Africa's largest ports and commercial railways was attacked. Government agencies endured repeated ransomware attacks. Across the continent, hackers have put critical infrastructure and governmental data in their crosshairs.

Similarly, foreign powers use digitally driven disinformation campaigns to destabilize vulnerable countries. Russia, which has sent mercenaries to the Central African Republic, Libya and Sudan, is backing its fighters with radio, television and web campaigns. Typically, these campaigns are crafted to generate anger and confusion in targeted countries to benefit Russian interests.

Finally, the proliferation of cheap drone technology has countless valuable applications when used for science, surveillance and the delivery of goods. But extremist groups are intent on using drones to launch improvised explosive device attacks. Terrorists already use this tactic in the Middle East with devastating results. Observers believe it is only a matter of time before extremists use the same tactics in Africa.

African security professionals are racing to respond to these threats. Continuing military education and skills courses will be key to this effort, as will the ability to embrace new technology. A young, computer-savvy generation of Soldiers is eager to play a leading role in the fight.

The creativity and motivation of our adversaries to develop new modes of attack is boundless. But so is our resolve to defeat these threats. By relying on training, strong partnerships and the ability to adapt, there is no threat that we cannot anticipate and stop.

U.S. Africa Command Staff

Soldiers at the Nigerian Army School of Military Engineers in Makurdi practice detecting and disarming improvised explosive devices.

SOUTHERN EUROPEAN TASK FORCE, AFRICA

adf
AFRICA DEFENSE FORUM

Hybrid Threats
Volume 15, Quarter 2

U.S. AFRICA COMMAND

CONTACT US:

U.S. AFRICA COMMAND

Attn: J3/Africa Defense Forum
Unit 29951
APO-AE 09751 USA

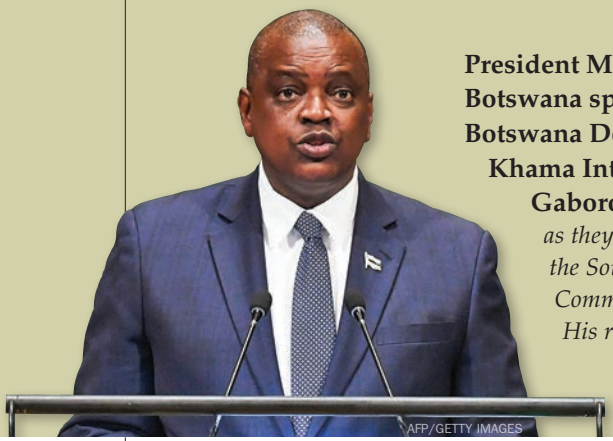
ADF.Editor@ADF-Magazine.com

HEADQUARTERS U.S. AFRICA COMMAND

Attn: J3/Africa Defense Forum
Geb 3315, Zimmer 53
Plieninger Strasse 289
70567 Stuttgart, Germany

ADF is a professional military magazine published quarterly by U.S. Africa Command to provide an international forum for African military personnel. The opinions expressed in this magazine do not necessarily represent the policies or points of view of either this command or any other U.S. government agency. Select articles are written by ADF staff, with credit for other content noted as needed. The secretary of defense has determined that publication of this magazine is necessary for conducting public business as required of the Department of Defense by law.

Ensuring Security Among Neighbors


AFP/GETTY IMAGES

President Mokgweetsi Masisi of Botswana spoke to Soldiers of the Botswana Defence Force at Sir Seretse Khama International Airport in Gaborone on July 26, 2021, *as they prepared to leave for service in the Southern African Development Community Mission in Mozambique. His remarks have been edited to fit this format.*

Members of the Botswana Defence Force listen to President Mokgweetsi Masisi at Sir Seretse Khama International Airport in Gaborone before they depart for Mozambique.
OFFICE OF THE PRESIDENT, REPUBLIC OF BOTSWANA

I stand here before you as the commander in chief of the Botswana Defence Force [BDF] and the current chairperson of the SADC [Southern African Development Community] Organ on Politics, Defence and Security. It is a formal institution of SADC, which was launched in June 1996 with a clear mandate to support the achievement and maintenance of security and the rule of law in the region.

Today this mandate is being put to a test by a geopolitical environment and security landscape not dissimilar to that of the formative years of our country during the years of the minority apartheid regime. As complex as the security situation in the SADC region may be, as in the past, Botswana's foreign policy goals have been, and remain, very clear. Botswana's security can never be attained without that of its neighbors. When Botswana took the leadership of the SADC Organ on Politics, Defence and Security troika, I laid out our country's role in leading our region's efforts to underpin stability in political, defense and security by applying our universal diplomatic and security capital to our region's vexing problems.

Today we witness yet another milestone in our objectives of propelling the peace agenda to our region in following through on the SADC mandate aimed at facilitating the peaceful conditions in the northern part of the Republic of Mozambique, in Cabo Delgado in particular. It is for this reason that I am here this morning to address members of the Botswana Defence Force who, as part of the SADC Standby Force, will be deployed to provide regional support to Mozambique to combat the looming threat of terrorism and acts of violent extremism in the Cabo Delgado region in the northern part of that country, as an element of the SADC Mission in Mozambique, SAMIM.

As stated earlier, our commitment to regional and international peace as a nation remains steadfast and undiminished, as evidenced by BDF's previous enviable involvement in peacekeeping operations in Operation Restore Hope in Somalia, in UNOMOZ I and II [United Nations Operation in Mozambique], as part of the U.N. observer mission in Rwanda, and Boleas in Lesotho.

Throughout these deployments, the BDF received very positive appraisal for their professional conduct in the execution of their military job and also as true and sincere ambassadors of Botswana's historical and enduring national values of being a rule-based society. That remains the historical legacy of your predecessors and the shoes you must now fill — all of you. I therefore implore all to emulate these predecessors, who were involved in previous peace missions, by exhibiting the highest level of professionalism during this deployment as Botswana's flag bearers in Mozambique.

As your commander in chief, I am alive to the fact that you will be facing a deceptive enemy, which is likely to use asymmetric warfare, unconventional and underhanded warfare tactics against yourselves and the population you will be protecting. As professionals, you stand for much more than they do and must avoid emulating them and sinking to their level. And yes, all your training will come into sharp focus.

I therefore demand nothing less from you than to observe the laws of armed conflict as prescribed internationally in your profession of arms, as well as the status of forces agreement, which establishes the framework under which SAMIM personnel will operate in Mozambique. I have full confidence that you will execute your task equitably and will do nothing that will taint the good image of the Defence Force of Botswana.

CAR'S PEANUT GROWERS FACE THREATS, THEFT

STORY AND PHOTOS BY AGENCE FRANCE-PRESSE

For many peanut growers in the Paoua region of the Central African Republic, life is a daily battle. They have to coax the plants from the ground, harvest the nuts and shell them. Then they have to survive theft, extortion or worse in a region where rebels and pro-government forces are at war.

"What is preventing us from developing further peanut farming in Paoua is insecurity," Jean-Paul Ndopaye, manager of a peanut store, told Africanews. "When we want to send our goods to Bangui, to Berberati, or even to Bouar, we might run into road bandits."

"There are too many threats and thefts," said Celestine Inforo, 33, shelling peanuts along with about a dozen others on the outskirts of Paoua, a town of 40,000. "We had to sell our production very quickly and at a low price."

Inforo and her co-workers each fill several sacks in a few hours, then a pair of oxen haul them to a secure storeroom loaned by the Oxfam nongovernmental organization. Outside the storeroom, each bag is weighed and recorded at between 35 and 45 kilograms.

In the town, a sack of shelled nuts fetches about 10,000 CFA francs, about $17. In the capital, Bangui, a sack sells for between 20,000 and 30,000 CFA francs, says Jean-Paul Ndopaye, president of the Paoua Rice Growers Union.

Production greatly exceeds demand in the region, bringing down prices, and 80% of the town's population works in the peanut industry.

The CAR has been in the grip of a civil war since 2013. The conflict has diminished in intensity in recent years, but it flared up again during the last presidential election in late 2020.

Men weigh a bag of peanuts in Paoua, Central African Republic. A bag weighing 35 to 45 kilograms will sell for about $17.

In the shade of a mango tree, women turn peanuts into oil, butter and "kuli-kuli" sticks, which have a high nutritional content. One roasts the nuts. Another kneads peanut butter on a wooden board.

"The problem is processing," said Mahoua Coulibaly, local manager of the World Food Programme. "This is what must be invested in for the well-being of the population, but for the moment the funds are lacking."

Ugandan Children Return to School After Nearly 2 Years

ADF STAFF

Uganda ended the world's longest school closure on January 10, 2022, by ordering millions of students back to the classroom nearly two years after learning was suspended because of COVID-19.

Students returned to schools closed since March 2020 when COVID-19 swept the globe.

"I am so happy because I was missing school, my teachers, my friends and my studies," 10-year-old Nawilah Senkungu told Agence France-Presse (AFP) at Nakasero Primary School in Kampala, where teachers encouraged students to wear masks and wash their hands.

Education Minister John Muyingo said all primary and secondary students would resume classes a year above where they left off.

"All schools have implemented guidelines and standard operating procedures to ensure the safe return of children to schools, and measures have been put in place to ensure those who don't comply do so," Muyingo said, according to Taarifa, a Rwandan news service.

Despite those assurances, some parents have been cautious in the wake of continuing infections. A week after the reopening, some schools were below 50% of regular enrollment, according to The Independent of Uganda.

Some administrators say parents held back to avoid paying school fees until they could be assured of their children's safety. Dovicko Kisembo, head teacher at Mubuku Valley Secondary School in Mubuku town, told The Independent that many parents were concerned that authorities would announce another lockdown because of rising COVID-19 cases.

Muyingo has said that any school demanding fees above prepandemic rates would be sanctioned.

The closures affected at least 10 million primary and secondary pupils and lasted 83 weeks, according to the United Nations' education and cultural body, UNESCO.

Nawilah spent the long closure tending chickens and digging the fields on her grandparents' small farm.

"I am very happy to see my children back to school," her father, Siraj Senkungu, told AFP. "They have been missing their teachers plus learning."

Students work on lessons in January 2022 at Sweswe Primary School in western Uganda after schools reopened. REUTERS

OLD HOTEL A PAINFUL *Memory of Liberia's Past*

AGENCE FRANCE-PRESSE

A brochure shows the hotel in all of its former splendor. AFP/GETTY IMAGES

When it opened in 1960, the Ducor hotel in Monrovia, Liberia, was one of the only five-star hotels in Africa, boasting a nightclub and air-conditioned rooms, according to travel guides.

It hosted VIPs such as former Ethiopian Emperor Haile Selassie. Guests would lounge by the swimming pool, sip cocktails and watch the sun set over the Atlantic Ocean.

The Ducor closed in 1989 at the outbreak of back-to-back civil wars, which ran from 1989 to 1997 and from 1999 to 2003. It swiftly fell into disrepair.

"It makes everybody sad," said Ambrose Yebea, a retired tourism ministry official who previously offered tours of the hotel.

Many of Africa's leaders stayed at the Ducor during the 1960s and '70s with several booking rooms during the 1979 conference of the Organisation of African Unity in Monrovia.

In 2011, then-President Ellen Johnson Sirleaf handed the Ducor to the Libyan African Investment Co. (LAICO), a subsidiary of Libya's sovereign wealth fund, as part of a renovation plan.

According to a 2011 government statement, the renovated hotel would have 151 rooms, restaurants, a shopping center, a tennis court and a casino, and provide jobs.

However, the project, which with another plan to develop a rubber-processing plant was priced at $65 million, fell apart. Liberia cut ties with Libya in 2011 as the country descended into civil war. Renovation work stopped.

"It came to us as a big shock," said Frank Williams, a laborer who said he'd been one of 150 people employed by LAICO. "Today we are jobless."

The project has been at a standstill since, and its future is unclear.

Some still hope to see the Ducor reborn. Yebea, the retired tourism official, said it could lure tourists and generate jobs.

"Every Liberian sees it the same way," he said. "They want it to be refurbished."

Defending the DIGITAL GATES

State-Backed Hacking Threatens National Infrastructure, Economies and Sovereignty

ADF STAFF

The cranes that unload containers from ships at two of South Africa's busiest ports slowed nearly to a halt in July 2021. Trucks waited in line for 14 hours or more to pick up cargo. Ships were forced to anchor outside the harbor for days and decide whether to skip the affected ports altogether. Shop owners and consumers worried about empty shelves as a prime shopping season approached.

"This could not have come at a worse time," Denys Hobson, logistics and pricing analyst at the South African bank Investec, said. "If nothing can move in and out the country, there will be serious economic ramifications."

The disruption was caused by a cyber-attack. Hackers had infiltrated the network of Transnet, the state-owned company that operates the ports at Durban, Cape Town and others, as well as South Africa's railway and pipeline network. Unable to fulfill contractual obligations for more than a week, the company was forced to break its contracts until the attack was resolved.

News reports stated that "Death Kitty," a group of hackers based in Eastern Europe or Russia, took credit for the attack, which used a technique commonly referred to as ransomware, because it freezes a computer system until a ransom is paid.

It was the most severe attack ever perpetrated on South Africa's critical infrastructure, but experts warn it will not be the last.

"Attacks on critical infrastructure, including maritime ports, are likely to increase in severity and quantity," wrote Denys Reva for the Institute for Security

"Attacks on critical infrastructure, including maritime ports, are likely to increase in severity and quantity."

~ Denys Reva, Institute for Security Studies

Studies. "The economic toll for African states will inevitably be high, which means that measures to boost cyber security and protect infrastructure are vital."

A Nation at Risk

In the first quarter of 2021, South Africa was hit harder by ransomware attacks than any country on the continent, according to Interpol's African Cyberthreat Assessment Report.

Government agencies are among those most at risk.

In September 2021, an attack forced South Africa's Department of Justice and Constitutional Development to shut down its information technology (IT) system, which stores information including personnel files. In a separate incident the same year, the National School of Government had to shut down its IT system for two months, which cost the government training institution about 2 million rand. Even the nation's president was affected by hackers who infiltrated his phone.

Cybersecurity experts warn that South Africa's government institutions are now squarely in the crosshairs of hackers.

"The combination of aging technology, inadequate funding, and lack of training, coupled with the high-value data these organisations hold, makes them a goldmine for bad actors," wrote Saurabh Prasad for South Africa's IT-Online.

Interpol found that African organizations saw a 34% jump in ransomware attacks in the first quarter of 2021, the highest recorded anywhere in the world. Government institutions have fallen behind in the race to protect their IT infrastructure and must catch up, Prasad said.

"The threat landscape is also evolving far faster than the ability of government organisations to keep up with technology, which makes it an easy, profitable and therefore very attractive target," Prasad wrote.

Trucks and cargo vessels line up at the Port of Durban harbor after the state-owned company Transnet was hit by a cyberattack in July 2021.

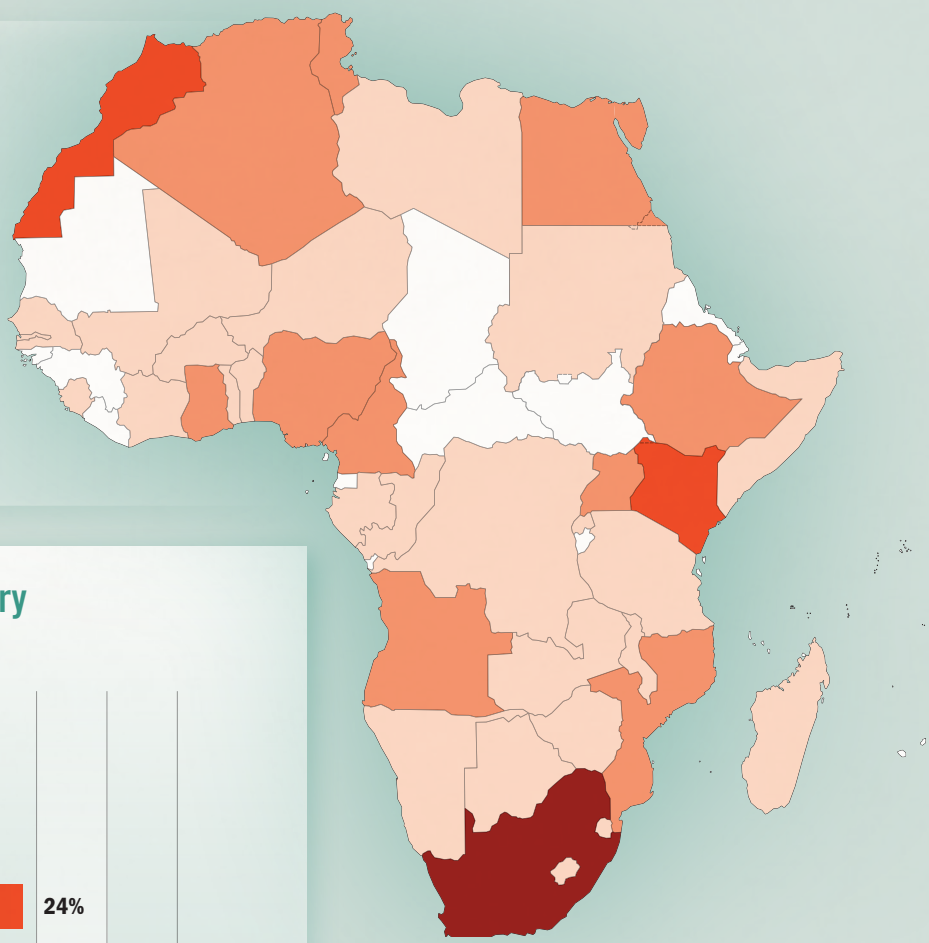
AFP/GETTY IMAGES

Threat Detection by Country*

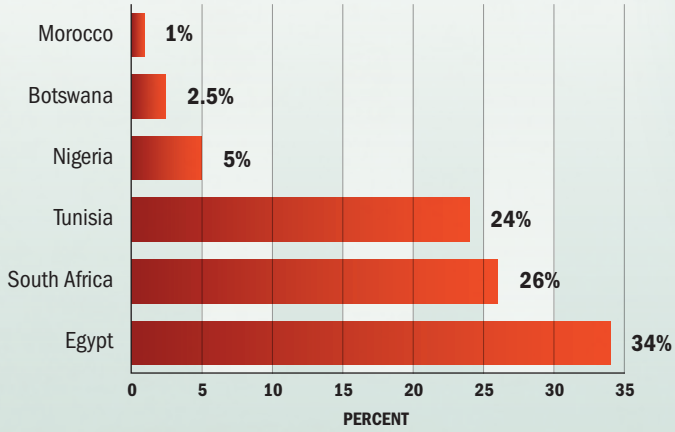
- less than 1 million
- 1 million – less than 10 million
- 10 million – less than 50 million
- 50 million – less than 100 million
- 100 million and above

Source: Trend Micro

*The number of threats detected in files, emails or URLs from January 2020 to February 2021 as recorded by Trend Micro, a cybersecurity software company that partners with Interpol.



Ransomware Detected by Country as a Percent of Africa's Total

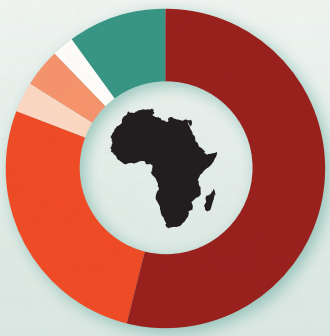


Source: Trend Micro, 2021

A ship moors outside Cape Town harbor after the port was hit by a cyberattack in 2021.

AFP/GETTY IMAGES

Most Common Threats Detected in Africa



- Malware..... **54%**
- Online scams..... **27%**
- Adware **4%**
- Command and control of server **3%**
- Phishing..... **2%**
- Others..... **10%**

Source: Trend Micro, 2021

A ship in Cape Town harbor unloads containers.

AFP/GETTY IMAGES

State-Backed Cyberwar

Although it is not known whether any nation or its proxies were behind the Transnet attack, state-backed hacking is a growing threat in Africa.

In 2018, Chinese-backed hackers stole emails and surveillance data from servers in the African Union headquarters in Addis Ababa, Ethiopia. In 2017, North Korea-backed hackers conducted a global attack known as Wannacry, which paralyzed businesses and public institutions in 150 countries. In 2020, Egyptian hackers hit Ethiopian businesses and governmental agencies in an attempt to disrupt construction of the Grand Ethiopian Renaissance Dam.

In 2021, Google sent more than 50,000 warnings to account holders worldwide telling them they had been the target of government-backed phishing or malware attempts. One of the most prolific perpetrators globally is a group known as APT35 or "Charming Kitten," which has links to Iran's Islamic Revolutionary Guard Corps.

African nations are particularly vulnerable to outside interference. Chinese companies built about 80% of the continent's telecommunications networks. The telecom company Huawei, which has strong ties to the Chinese Communist Party, is positioning itself to build much of the continent's 5G network. Additionally, Chinese companies have built IT systems in at least 186 government buildings in Africa, including presidential palaces, defense ministries and parliamentary buildings, according to a Heritage Foundation report.

Experts say this infrastructure means Chinese-aligned spies would have little trouble accessing sensitive government data.

"The Chinese government has a long history of all types of surveillance and espionage globally," said Joshua Meservey, senior policy analyst for Africa at the Heritage Foundation. "So we know this is the sort of thing they want to do, the sort of thing they have the capacity to do. And also, Africa is important enough to them to do it."

There are several strategic moves African countries can take to protect themselves from cyberattacks. Here are some:

Build Safeguards as You Go

As nations conduct more business online and sectors such as transportation, water and power are controlled digitally, hackers see openings to cause damage. Countries with the highest rates of internet penetration tend to be the most vulnerable. In one way, this is an advantage for African countries because many were relatively slow to adopt digital technology. This gives them the opportunity to build in safeguards as they develop their IT infrastructure.

Researchers Nathaniel Allen of the Africa Center for Strategic Studies and Noëlle van der Waag-Cowling of Stellenbosch University in South Africa said developing countries are not burdened by the older software architecture or "legacy code" that is easiest to attack.

By establishing good practices early on, countries that are less digitally advanced can "leapfrog" more cyber-mature countries, Allen and Waag-Cowling wrote.

Diversify Suppliers, Build Domestic Capacity

Countries that rely heavily on a single external service provider could be leaving the door open to state-backed hacking. By one estimate, Huawei manufactured 70% of the 4G base stations used on the continent. The company also is a leader in surveillance and facial recognition systems sold in Africa.

As Chinese-backed infrastructure projects have proliferated across the continent, they often are paired with IT development, which links control over multiple sectors, such as water, power and transportation.

"This could potentially create backdoors and vulnerability pathways," Waag-Cowling wrote in an article for the International Committee of the Red Cross (ICRC). "The net result is the possible future loss of de facto sovereign control of communication, energy, transport or water infrastructure."

Experts have encouraged African countries to cultivate relationships with a diverse range of IT service providers to avoid the single-provider pitfall. Competition not only challenges state-backed hacking; it also leads to better service for customers.

Many African countries also are trying to cultivate domestic capacity in the IT sector. Safaricom, the largest mobile phone company in Kenya, and South Africa's MTN are prime examples of this.

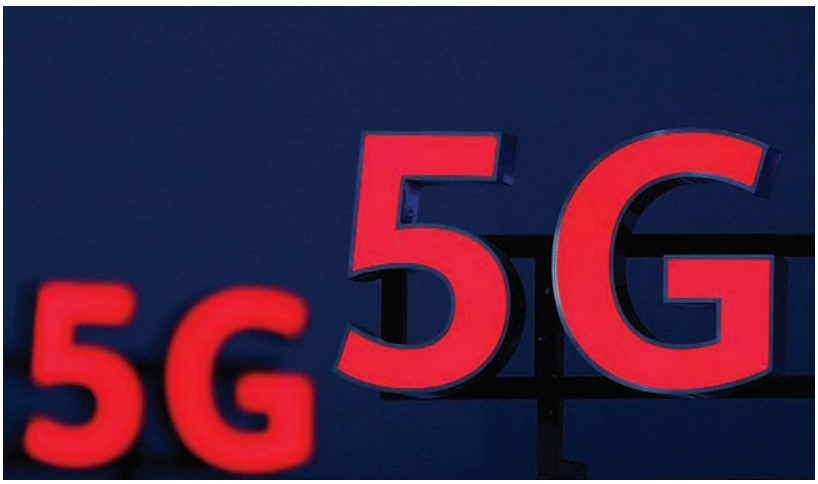
Eliminate Single Points of Failure

Cyber experts bemoan that too many IT systems controlling critical national infrastructure have a single point of failure. This means that if one server, one network or one plant is hit by an attack, an entire country can be left without a vital service, such as water or electricity. Advocates urge African countries to build in redundancies or backup systems to avoid catastrophic service loss in an attack.

"One attack on a single point of failure could lead to the disruption or destruction of multiple vital systems in the country directly affected, and a ripple effect worldwide," the United Nations and Interpol said in a "Compendium of Good Practices" to protect against cyberattacks. "This creates an appealing target to those intending to harm us. And as our cities and infrastructure evolve, so do their weapons."

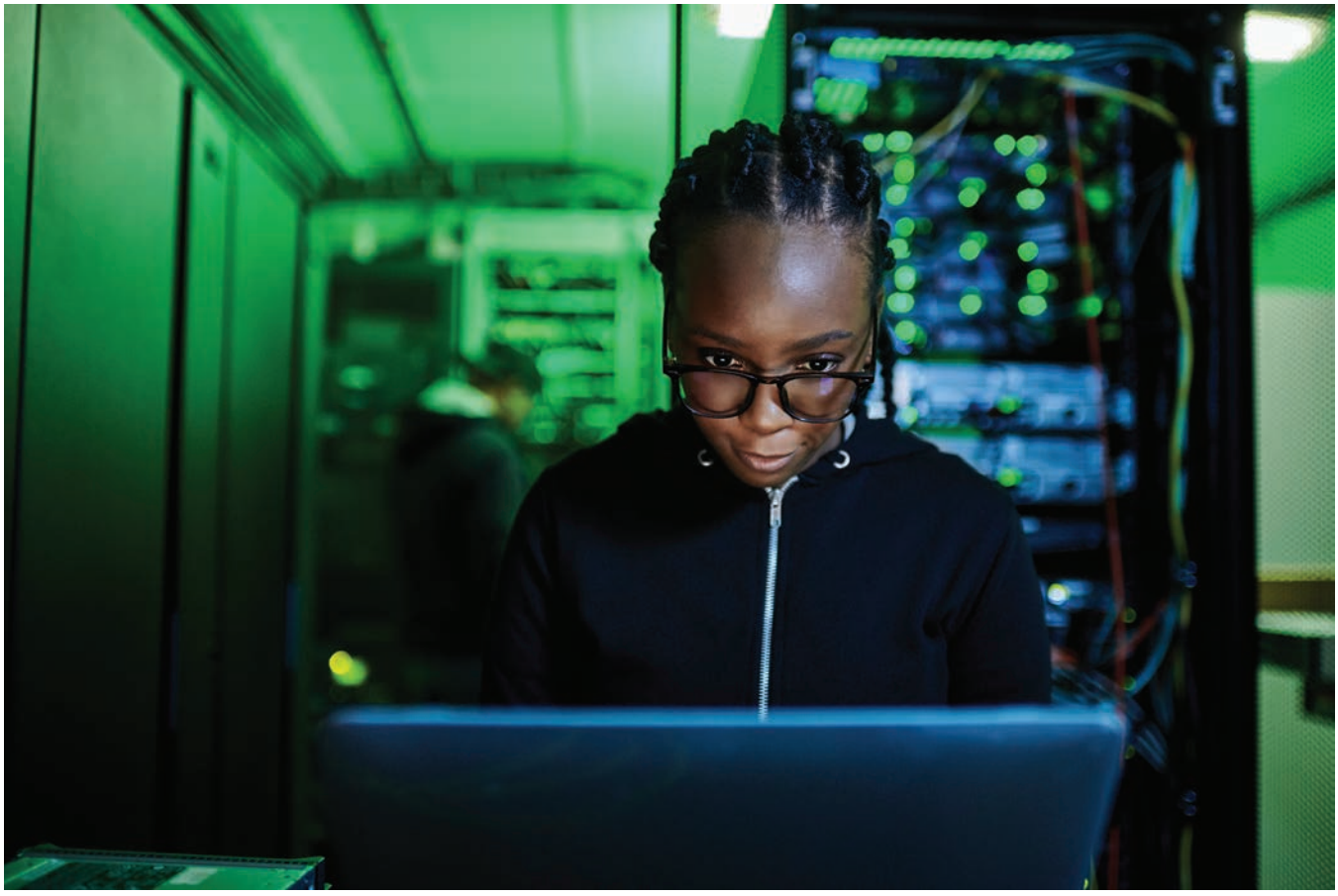
Chinese telecommunication giant Huawei manufactured most of the 4G base stations used in Africa. Experts say this dominance and the company's close ties to the Chinese government increase the risk of hacking and surveillance.

AFP/GETTY IMAGES



Huawei is positioning itself to build most of Africa's 5G infrastructure. 5G is the next generation of mobile phone, supporting towers and other technology being developed.

AFP/GETTY IMAGES



Invest in Detection/ Offensive Capabilities

Many nations are investing in computer emergency response teams that can monitor important national networks and critical infrastructure. These are sometimes called the nation's first responders in the event of a cyberattack.

Some countries, such as Nigeria, are launching cyber commands within the military. Experts say it is important for these commands to develop defensive and offensive capabilities that allow them to protect against attacks and degrade something that poses a threat before it can launch an attack.

The AU has taken a leadership role in encouraging cyber capacity with its Cybersecurity Expert Group, but observers are calling for more regional cooperation. Waag-Cowling said African countries could think of it like "cyber peacekeeping" through which nations work together to shore up cybersecurity at its weakest points. She believes the military, particularly its youngest, most educated cohorts, can play a lead role.

"African armed forces' ongoing experience with persistent irregular conflict could provide a platform for pivoting towards hybrid warfare threats," Waag-Cowling wrote for ICRC. "A young, urbanizing and tech-savvy population must complement future cyber defence strategies."

"African armed forces' ongoing experience with persistent irregular conflict could provide a platform for pivoting towards hybrid warfare threats."

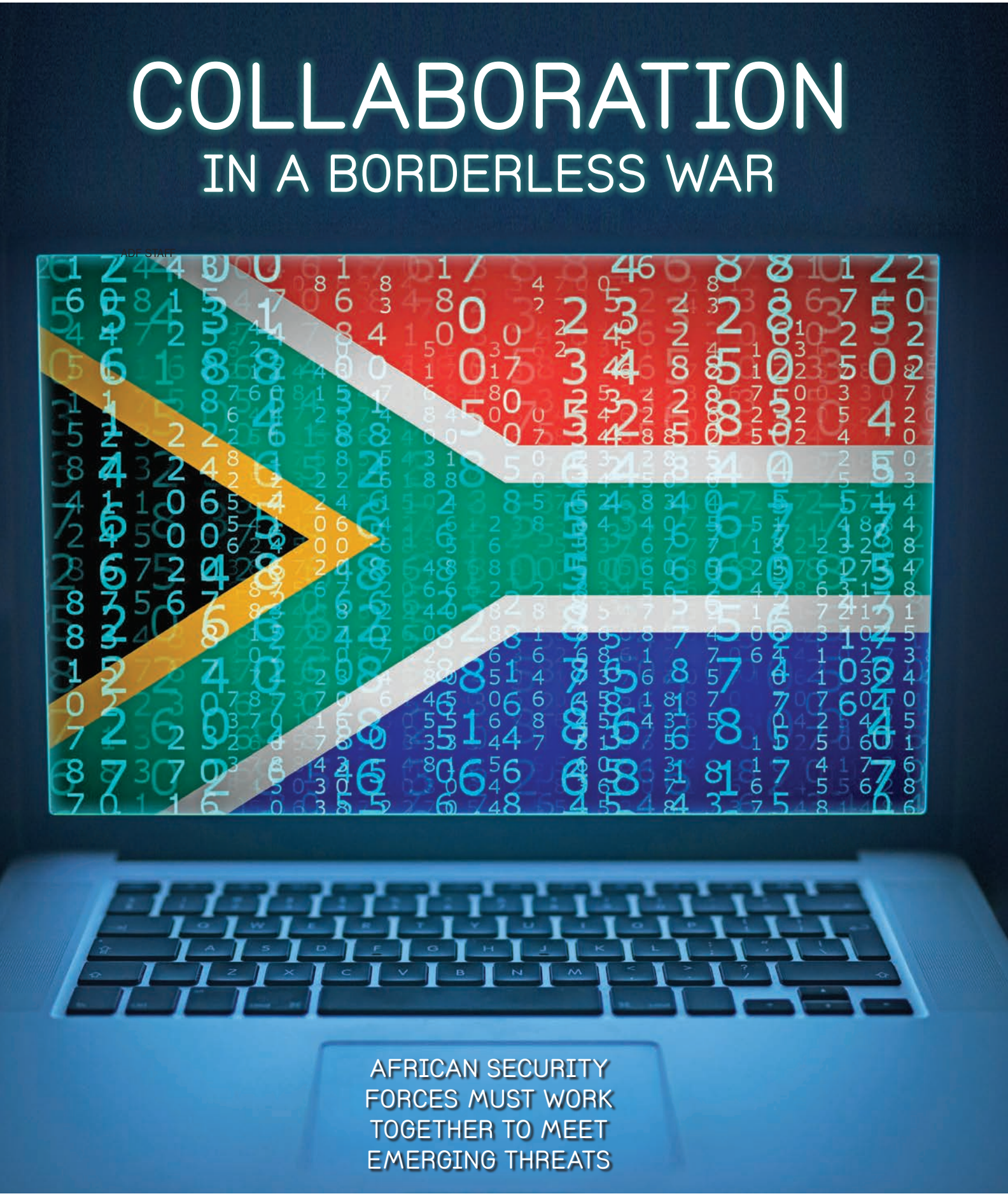
~ Noëlle van der Waag-Cowling, Stellenbosch University, South Africa

The stakes are high. If African countries are perceived as soft targets, hackers will attack them, Waag-Cowling warned.

"Cyber defence is, to an extent, reliant on attackers believing that there is sufficient indication of a State's ability to respond to attacks," she wrote. "Essentially, the power of a State lies within the perception of its power. A demonstrated and deepened commitment to advancing continental cyber security efforts is therefore required. The future prosperity of Africa and the safety of her people depend on this." ❑

COLLABORATION
IN A BORDERLESS WAR

ADF STAFF



AFRICAN SECURITY FORCES MUST WORK TOGETHER TO MEET EMERGING THREATS

***Dr. Jabu Mtsweni** is manager of the Information and Cyber Security Research Centre at the Council for Scientific and Industrial Research (CSIR) in Pretoria, South Africa. Mtsweni spoke to ADF about the types of cyber threats African countries face and how they might better prepare to address them. His remarks have been edited to fit this format.*

ADF: Please share a little about your background in cybersecurity issues, such as your education and training.

Mtsweni: My background is in computer science, my undergraduate qualification as well as postgraduate, and my Ph.D. includes computer science, but not focusing on cybersecurity initially. I started getting involved or specializing in cybersecurity around 2014. But I have worked in various cybersecurity aspects in small ways since 2003 or so. I have been involved in a number of initiatives like leading a group of researchers — about 15 of them — with a strong focus on supporting the military on the issues of cyberwarfare and building capabilities. Now I support a much bigger team — about 70 people — where we focus on supporting the Department of Defence in South Africa and in other countries, but dealing with the issues of cybersecurity in general in the public sector as well as in the private sector.

ADF: Briefly explain what CSIR does and your function as manager of the CSIR Information and Cyber Security Research Centre.

Mtsweni: The CSIR is a national government enterprise, which solely focuses on research and development in various socioeconomic domains — it could be water, it could be energy, it could be environment, it could be health, the issues of safety and security, the issues of logistics, the issues of smart places, ICTs [information and communications technologies]. My specific area of focus is obviously in defense and security, where I am leading the Information and Cyber Security Research Centre, where our core focus is about researching and innovating on new ways of protecting ourselves and our organizations and military, as well as building some technologies in a prototype form and then commercializing some of our local IP [intellectual property].

ADF: What is the single biggest and most prevalent cybersecurity threat on the African continent, and how should nations be addressing it?

Mtsweni: I think the biggest threat is obviously the risk to the sovereignty of countries from the digital space point of view. In other words, where the sovereignty of countries' digital space is compromised, whether through data breaches, through the issues of ransomware, and through the theft of IP, the intellectual property, or sensitive information from the nations in Africa. That threat is big because in geopolitics it's also about influence, where different countries may want to influence politics or any other thing in Africa. So the issues of data and information being stolen or being compromised becomes the biggest threat in Africa.

The key activity or action that African militaries need to take is about building capabilities from cyberspace. And when we talk about building these capabilities, we are not just talking about technology only; we are not only talking about data. But we are talking about the whole spectrum, where people are capacitated to understand the cyber domain; it's just like training people to maybe guard airspace or to guard land or sea. We need to drive that capability of empowering or capacitating our forces to be able to understand the cyber realm.

We also need to put processes in place from the policy point of view and have cyber strategies that are going to proactively deal with some of these threats. We need to understand our data. Countries need to understand what it is that they are protecting, because it is very difficult to protect what you don't understand. If you compare it to land, air and maybe sea, it is very easy to pinpoint the assets that you are protecting, but in cyberspace the realm is a bit wider, so the scope is a bit wider. So we need more awareness, but also more and more training. And of course we need the resources and tools that could aid us to be able to protect ourselves and to be able to detect threats when they are emanating from cyberspace.

ADF: In what ways, if any, does the CSIR or any of its divisions advise and assist the South African National Defence Force on these types of cybersecurity issues you've been talking about?

Mtsweni: The CSIR is what we call an independent smart buyer, smart user advisor for a number of government entities, and within the military space and particularly information and cyberwarfare, we play a very critical role. For example, this includes building prototypes for the military so that we can better understand how some of these capabilities can be available for use in a real-life environment. We do a lot of research and development for them so that they can understand the threat landscape. We also do a lot of work in terms of advising them on some of the technologies that they should use or not use, how they can protect themselves from the various threats that are in

the cyberspace, and then, obviously, supporting them in building some of these capabilities in order to protect the country and its citizens.

There are a number of examples, but much of the work is classified, so I can't really speak about specific work or projects per se, but I can speak generally. In terms of training we have supported the military, and there are a number of forces that have been trained, capacitated through the CSIR to deal with issues in cyberspace. We have assisted the military to also understand the importance of setting up its own infrastructure. And now and again, we are called upon and they would ask us to advise them on various matters that concern their domain.

ADF: More broadly, what should African countries be doing to ensure that their critical national infrastructure, such as the electric grid and water supply, are protected from cyberattacks?

Mtsweni: I think one of the key things we did on the African continent, but clearly in the African defense space, is the issue of collaboration. I think when it comes to cyberspace, the military from one country to another generally would not work together unless they are fighting against the same enemy. But within cyberspace I think that collaboration becomes very, very key. Why is it important? Because the threats are almost the same in cyberspace and when we collaborate, we can then be able to share threats.

The other thing that is key is the issue of situational awareness. It is difficult to protect what you don't know or to react to incidents that you do not see. So it's important for them to have that situational awareness through buildings, structures such as your national cyber incident response centers or computer security response teams. Over and above that, having real policies that mandate or clarify what the military needs to do or not because in the cyber domain, you have the civilian side, you have the nation-state side and then also the private sector side.

The CSIR developed a Cybersecurity Early Warning System that allows businesses to detect network invasion at an early stage and avoid losing sensitive information. CSIR

So just to summarize, in an African context: It's about collaboration, it's about situational awareness, and it's about building this capability that I've been talking about, and then over and above that it is about the African countries' structures such as the African Union having these threat-intelligence sharing units just like what Interpol does. I think the militaries in Africa could be having something like that, but over and above just collaborating on their own, we need to also collaborate with other nations in Europe, in the U.S., because I think it's important that we have allies and partners.

ADF: A few countries have created cyber commands or emphasized cyber training within the military. Do you think cybersecurity needs to be a greater point of emphasis within African militaries? What more specifically should militaries be doing to that end?

Mtsweni: I think that the emphasis on cybersecurity is very important, and I think it is emphasized or made important by the fact that we have already seen a lot of nation-state attacks. And we have already seen a lot of breaches in Africa that are purported to have been instituted by foreign countries. Even in South Africa we have lost some intellectual property — for example, the design of a military plane through cyberattack. So it is very important to have these capabilities, and not just in documents, but in the operational, including the training of the people. There are a few countries that have strong cyber defense — and by defense, I mean offensive and defensive. So we need to get to that because it's also about building our own tools, because if you look at the U.S. they have their Cyber Command, but they are constantly doing R&D [research and development], building their own tools for defense and for attack when it is necessary.

ADF: We've spoken quite a bit about training in broad terms, but there's also training on a micro level, that is to say with individual troops. To that point, what specific training or principles should be incorporated into training for all military and security forces to ensure that they have the basic understanding of meaningful and effective cybersecurity practices?

Mtsweni: I think the generic training is obviously understanding networks, because if you don't understand the technology it's going to be very difficult for you to either protect or attack it. And the second thing is about training them in just basic cybersecurity awareness. Because if somebody is not aware what threatens the tools that they are using, it could be a problem. So just the basic principles, the use of social media by the military forces, the use of these various technologies, and mobile devices and so on because once they have their awareness, they can then understand what the threats are and how scalable those threats are.

ADF: State-backed cyberattacks are now a reality in Africa. We've seen government agencies hit by ransomware and private businesses hit by foreign-backed hacking in recent years. How concerned are you about states using cyberattacks

Transnet, South Africa's stateowned transport and logistics company, was hit by a cyberattack in July 2021. The attack lasted several days. AFP/GETTY IMAGES

as a tool of war, and do you think we will see more of it in Africa in coming years?

Mtsweni: Cyberattacks used as a tool of warfare between nations are on the rise, they are increasing. And sometimes it is also used by just a nation alone, just political parties attacking each other using some of these tools. And definitely we are seeing more of it in Africa. We are seeing it particularly now with social media and a lot of access to technology.

One thing about this question that I wanted to bring forth is that cybersecurity is about power. Those who have tools, those who have people, those who have capability, they are able to then institute some of these attacks. Then you have the ones who do not have [capabilities] in the cybersecurity space, and those are the powerless; they may not be able to respond. So it's important that African countries prepare themselves for holistic, comprehensive cyber defense capabilities.

ADF: Extremist groups have been using the web for recruitment and spreading propaganda for years, but is there any evidence that extremist groups are trying to use cyber capabilities to launch attacks like ransomware or other types of attacks on the African continent? Is this something countries should be concerned about?

Mtsweni: I think in Africa there is limited use of cyberwarfare tools by extremist groups, but there are incidences even though they are scarce and sparse. In terms of the ransomware, I don't have much evidence of it, but we have seen extremist groups … targeting governments, and in South Africa we have seen that happening a lot. For example, the Department of Justice was attacked and Transnet was hacked as well, and this was through ransomware, and some of them we may not know because they might not necessarily say, but we are closely looking at this and we see them happening.

ADF: With regard to extremist groups like Boko Haram or al-Shabaab, are you seeing any evidence that those types of groups are going beyond just recruiting on the web and actually weaponizing cyber capabilities to further their jihadist or extremist or political ends?

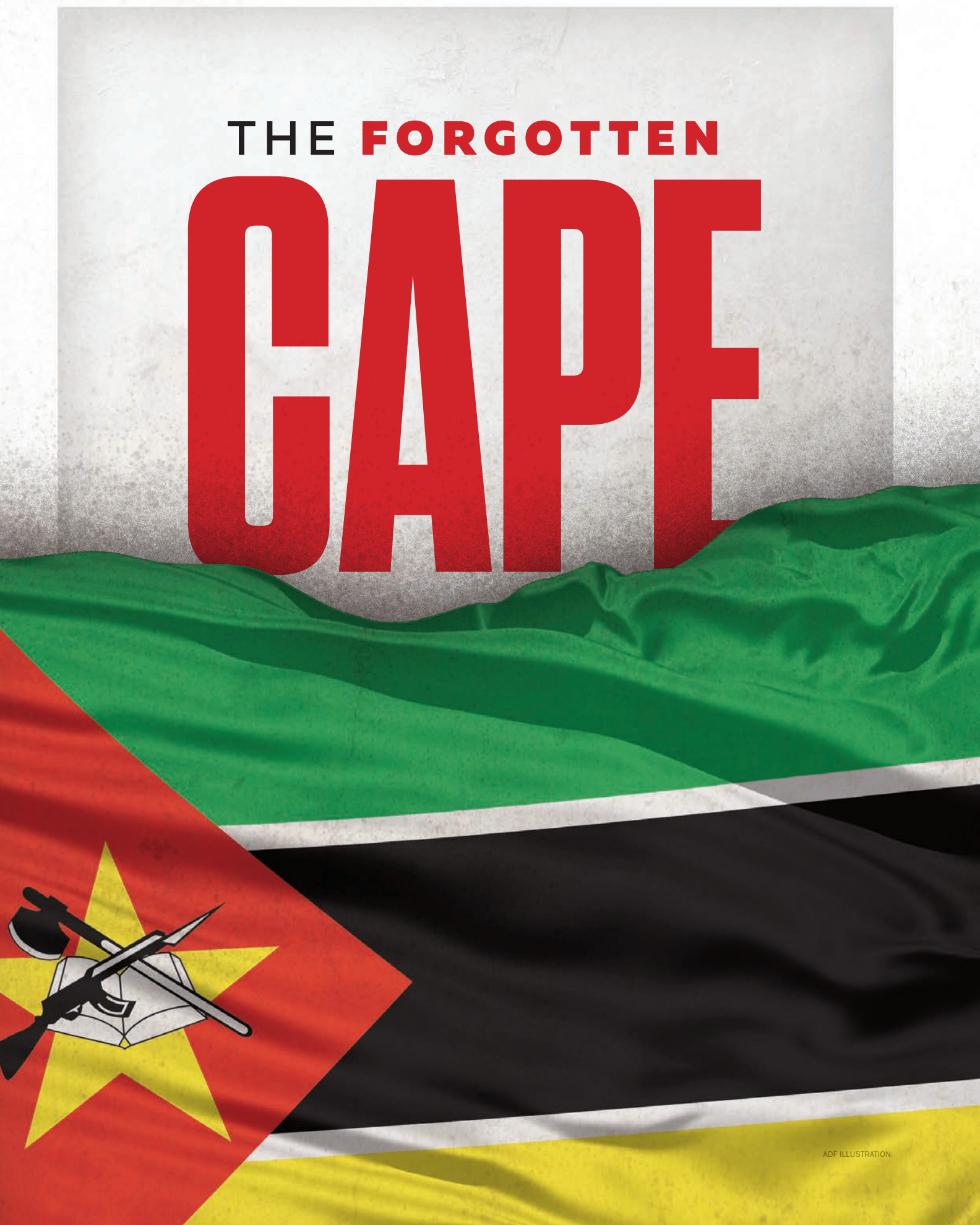
Mtsweni: I think there is definitely evidence, although it's limited. But let's just take a typical example of social media, right? If you look at social media as a cyber tool … it could be used by these extremist groups, so we see them using your deepfakes, using your social media to spread fake news. Because in our context the issue of spreading fake news is also another way of psychological operations if you look at the mental point of view because it's about influencing people, it's about pushing propaganda, it's about changing the narrative. And we see that the use of social media as a form of digital attack is growing in Africa.

In terms of them using the hardcore cyber tools, there's not that much evidence, but for communication and for the psychological operations attack we see that they're very strong, particularly in promoting these various conspiracy theories.

ADF: Is there anything else you'd like to mention that I have not asked you about?

Mtsweni: Definitely, cyber terrorism has an impact on human security, and I think the military, including the law enforcement agencies, have a high role to play as we become more digital. It's important that we build capabilities and we are prepared. Because it's not a matter of if, but it is a matter of when. ❑

THE FORGOTTEN CAPE



ADF ILLUSTRATION

GEOGRAPHY. HISTORY. POLITICS. MISTAKES.
THEY ALL PLAY A PART IN THE RISE OF VIOLENT EXTREMISM IN MOZAMBIQUE'S CABO DELGADO PROVINCE

ADF STAFF
PHOTOS BY: AFP/GETTY IMAGES

As young men prowled the streets of Mocímboa da Praia with machetes and AK-47s on October 5, 2017, some townspeople peered through windows in fear, recording the defiant march on their cellphones.

As a gun-toting militant walks by, one resident whispers an infamous and fearsome name: "al-Shabaab."

The scene is part of a BBC Africa Eye documentary titled "Sons of Mocímboa: Mozambique's terrorism crisis" that profiles the challenges posed by the terrorist group that has plagued Cabo Delgado province since that first attack back in October 2017. In that assault, about 30 insurgents laid siege to the town's three police stations, killing 17 people, including two police officers, and raided armories. Cabo Delgado is known by the nickname Cabo Esquecido, which means "Forgotten Cape."

Locals use the name al-Shabaab, which translates as "the youth," informally to refer to the group. But it is not affiliated with the al-Qaida-linked terrorist group in Somalia of the same name. It is also called Ansar al-Sunna, which means "supporters of the tradition."

The 2017 attack was the first of many in the region and led to the deaths of more than 3,700 people and the displacement of more than 850,000 as of February 2022. Rwandan troops and police entered the country in July 2021 and soon recaptured Mocímboa da Praia with a force of 1,000.

The multinational Southern African Development Community Mission in Mozambique (SAMIM) deployed days after Rwandan forces, adding several hundred Soldiers to Mozambique's troops from among eight participating nations: Angola, Botswana, the Democratic Republic of the Congo, Lesotho, Malawi, South Africa, Tanzania and Zambia. Ground troops mostly came from Botswana, Lesotho, South Africa and Tanzania with other participants contributing logistics, South Africa's Daily Maverick reported in January 2022.

Even as Mozambican, Rwandan and SAMIM forces logged notable successes during the second half of 2021 and into 2022, brutal violence persisted, and with it questions about whether the insurgency could have been headed off years earlier.

Rwandan police officers, left, and Mozambican Soldiers stand during an event on September 24, 2021, in Pemba, Cabo Delgado.

A HISTORY OF ISOLATION

The port town of Mocímboa da Praia is more than 2,600 kilometers by road from Mozambique's capital, Maputo. Distance from government centers is a common feature of radicalized areas in African nations. The distances tend to result in reduced government presence and services in remote areas, creating perceptions of marginalization among locals. Examples include northern Mali, the birthplace of that country's metastasizing jihadist extremism, and northern Nigeria, home to the Boko Haram insurgency.

Distance is further exacerbated by the fact that Mozambique still is recovering from a brutal civil war that lasted from 1977 to 1992. The war is estimated to have killed a million people and displaced millions more. Furthermore, the Cabo Delgado coast generally is associated with the rebel Mozambican National Resistance movement, known as RENAMO. In the war, its forces battled the Liberation Front of Mozambique, known as FRELIMO, which Mozambican President Filipe Nyusi now leads.

A Rwandan Soldier patrols near a burned-out truck in Palma, Cabo Delgado, in September 2021.

This camp for internally displaced people in Cabo Delgado's Metuge district housed about 30,000 people in May 2021, a fraction of those displaced by insurgents.

Some say this political division serves to further separate Cabo Delgado and its people from government attention and concern. Another chief regional issue is the discovery and capitalization of vast natural gas resources and smaller ruby mining interests. Experts point to locals being excluded — and at times removed — from ruby mining sites in the region after benefiting for years in the artisanal trade, thus losing access to economic opportunities, including illicit ones.

Geography, history and politics. All can be blamed to varying degrees for conditions in Cabo Delgado now. But experts say Mozambique's government also made mistakes along the way, failing to heed warnings and concerns emerging from the grassroots. Had security forces paid attention as far back as 2015, perhaps the insurgency could have been effectively confronted in its early stages.

MOZAMBIQUE'S RESPONSE

Once the October 2017 assault was over, Mozambican police arrived, blamed the violence on bandits and declared they would deal with the matter in a week's time, Dr. Salvador Forquilha, senior researcher with the Institute of Social and Economic Studies in Mozambique, told ADF.

Forquilha said the government made several sweeping mistakes in 2017. First, security officials responded with violence and closed mosques and made some quick arrests. This sowed confusion and also agitated some Mozambican Muslims, according to reports.

"I think that the government was not prepared to deal with such a phenomenon," Forquilha told ADF. "Remember that we had the civil war during 16 years, and we are still in the process of ending the process of civil war with the reintegration of the former guerrillas from the rebel group RENAMO. … So it came as a surprise."

Finally, he said, there were organization and coordination problems among the police and the Army. Sometimes this lack of coordination led to conflict between the two groups. As this problem persisted, insurgents spread into more and more areas until Rwandan and SAMIM forces deployed in 2021.

A woman holds a child amid the remnants of a village burned by insurgents outside Macomia in Mozambique's Cabo Delgado province.

"I DON'T THINK THAT ONE COUNTRY ALONE CAN FIGHT TERRORISM, JIHADISM, WHATEVER, WITHOUT COOPERATION WITH OTHER COUNTRIES, WITH OTHER STATES, WITH OTHER NATIONS."

— **Dr. Salvador Forquilha**
Senior researcher with the Institute of Social and Economic Studies

"I think that the approach from the government side to deal with the phenomenon was wrong from the very beginning, and it indeed was late when the government realized that the country was facing a serious problem linked to jihadism and terrorism," Forquilha told ADF.

SEEDS OF EXTREMISM

The October 2017 assault is widely regarded as Ansar al-Sunna's first organized and coordinated attack. But it was not the first instance of violence in Cabo Delgado or the first indication that radical Islamic teaching was festering in the region.

Ansar-al-Sunna emerged in 2015, attacking local Muslims. The BBC Eye documentary indicates that local leaders were sounding the alarm about a new form of Islamic teaching creeping into the region in 2015.

The mayor of Mocímboa da Praia announced that a group called al-Shabaab was recruiting young people in the area, which was posing a threat to peace, BBC Eye reported. A year later in 2016, a headmaster told Nacedje Community Radio in Macomia that attendance at his school had diminished, which he blamed on an Islamic sect that said going to school was useless.

One local chief in 2016 sent a list of concerns to the local Muslim council in which he listed elements of peculiar preaching from the insurgents. Instructions directed worshippers to pray with their shoes on, not carry identification, avoid state-sponsored schools, and eschew the national flag and national events. "They have been recruiting Muslims that are unaware, that didn't study and are poor," he said in the BBC report.

"Muslim leaders, they were actually warning, and some of them went to see local officials to say look, we are facing many challenges in our local mosques," Forquilha told the BBC. "We have people coming from abroad, especially young people, trying to preach a very radical Islam. There were no very clear actions coming from the government … in order to fight the group at the very beginning."

OUTSIDE INFLUENCES

Problems due to ineffectual government have long been present in Cabo Delgado province and surrounding areas. But the roots of radical Islam may extend out of the area and across the border into Tanzania and elsewhere, according to some experts. The Africa Center for Strategic Studies (ACSS) conducted a webinar in October 2021 to discuss the origins of violence in Cabo Delgado.

In it, Dino Mahtani, at the time deputy director of International Crisis Group's Africa Program, pointed to crackdowns on Islamic radicals in Tanzania in 2017 that may have pushed extremists into Mozambique, where they have merged with extremists there.

The crackdowns, Mahtani said, targeted those affiliated "with the al-Qaida franchises of the Swahili coast" from Somalia, through Kenya, Tanzania and into

Mozambique. The Islamic State group, he said, is trying to "drill into" the network and bring it into its fold, which already includes the Allied Democratic Forces in the Democratic Republic of the Congo. Research shows Tanzanians recruited since 2017 showing up in camps in eastern DRC and then Cabo Delgado, "so there is a to-ing and fro-ing of Swahili coast boys participating in violent conflict in Cabo Delgado, but also in eastern Congo," Mahtani said.

Dr. Adriano Alfredo Nuvunga, director of the Centre for Democracy and Development, a nonprofit civil society organization in Mozambique, agrees that outside influences have shaped the Cabo Delgado insurgency.

The region, Nuvunga said in the ACSS webinar, has long been marginalized and neglected by the central government. "The entire social fabric that's conducive to the conflict is linked to local problems," he said through an interpreter. But the barbarous violence perpetrated by insurgents, which includes decapitations and the severing of limbs, points to terrorist methods being exported to Cabo Delgado from outside.

A Rwandan Soldier, part of 1,000 military and police forces, patrols near Palma, Cabo Delgado, in September 2021.

WHAT COULD HAVE BEEN DONE?

Forquilha agreed that many extremists have crossed over from Tanzania. "What's surprising is to see that the government took so long, for example, to cooperate with Tanzania," he told ADF. Mozambique could have learned more about what to expect and how to deal with the insurgency by engaging with Kenya, Tanzania and Uganda, all of which have confronted extremist violence for years.

Other African nations faced with similar challenges would do well to take potential threats seriously from the beginning, he said. That includes making effective use of state intelligence services and trying to ensure that government institutions are strong enough to provide resilience and economic opportunities for residents.

If the Mozambican government had taken this more collaborative approach from the beginning, it might have kept insurgents from intractably embedding themselves throughout the region and leading to significant numbers of internally displaced people and other problems, Forquilha said.

Forquilha, who has conducted surveys and research in the affected areas of Cabo Delgado, was in the region in January 2022, talking with residents in Pemba, a port town and the capital of the province. He said residents told him that they "still have attacks in some locations," despite the presence of multinational military forces. Small groups of insurgents now target small villages for attacks, which will be more difficult and more time-consuming for Soldiers to combat. Military forces can improve the security issue "but it will not eliminate the insurgency itself," he said.

Before Rwandan and SAMIM forces intervened, Mozambique turned to private military companies, first from Russia's infamous Wagner Group, then from South Africa-based Dyck Advisory Group. Wagner forces left after sustaining heavy losses, and Dyck left after its contract expired in early 2021. ACSS webinar participants agreed with Forquilha that military intervention alone is unlikely to end Mozambique's insurgency.

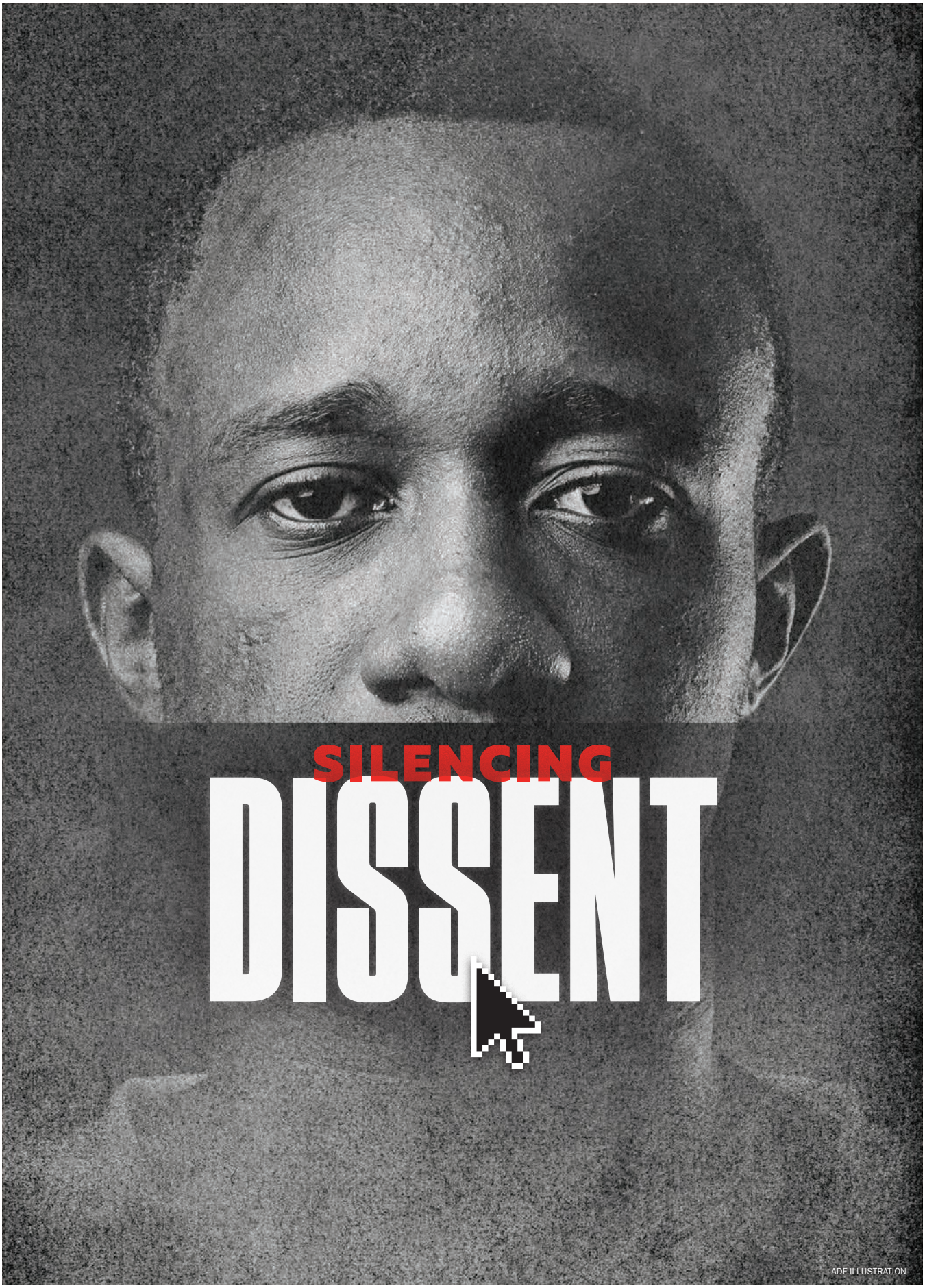
Idriss M. Lallali, head of the Alert and Prevention Unit at the African Centre for the Study and Research on Terrorism, drew parallels between Mozambique and what has happened in Mali since 2012. Mozambique must "reestablish state presence" and build trust between the state, the security sector and the people they serve.

"If you don't develop certain parts of your country, then it will come down and haunt you at some point or another," Lallali told the webinar. "And I think what happened in Mali is now happening in Mozambique."

At this point, Forquilha said, Mozambique will have to deal with internal dynamics with socioeconomic efforts that address poverty and lack of employment. That would go far in giving young people opportunities beyond recruitment by extremists. Such efforts also need to reach into neighboring provinces such as Nampula, Niassa and Zambezia, where conditions are similar.

The external dimension of Ansar al-Sunna's links to international terror organizations such as the Islamic State group and East African networks underscores the need for cooperation with other nations. The Islamic State group started claiming insurgents' attacks in 2019, "so the link is there, and we cannot deny the link," Forquilha said.

"I don't think that one country alone can fight terrorism, jihadism, whatever, without cooperation with other countries, with other states, with other nations," Forquilha said. "Because it became a kind of global phenomenon, a global threat, and it has to be dealt with as such. So the cooperation component is very, very important to take into account." ❑



ADF ILLUSTRATION

SHUTDOWNS, LEGISLATION AND FOREIGN INFLUENCE PART OF EFFORT TO CENSOR EXPRESSION

ADF STAFF
PHOTOS BY: AFP/GETTY IMAGES

After Twitter deleted a post by Nigerian President Muhammadu Buhari in 2021, Nigeria shut down access to the country's most popular social media site for seven months.

"The loss was humongous," Nigerian blogger and social media expert J.J. Omojuwa told ADF. "You got an awakening that this can happen anywhere."

Internet analyst NetBlocks estimated that the blackout cost Nigerians up to $1.6 billion in lost business. It also disrupted vital COVID-19 information that the Nigeria Centre for Disease Control published on the platform. Human rights groups condemned the blackout as a violation of Nigerians' right to free expression. In the end, the government restored access, but only after Twitter agreed to pay taxes and set up a local office subject to Nigeria's laws.

Nigeria's Twitter blackout belongs to a spectrum of direct and indirect actions intended to control how information is shared. And these information blackouts are becoming more common in Africa. In many cases, the controls are imposed in the name of national security. But the resulting disruptions create less security as they hamstring local economies, interrupt education and drive misinformation.

Along with internet blackouts, censorship efforts in Africa include new laws aimed at cybercrime and campaigns by Chinese and Russian forces to shape Africa's media environment. Together, they amount to a broad attempt to control the flow of information on the continent.

"When it comes to freedom of expression," Omojuwa said, "you're always defending it."

INTERNET SHUTDOWNS

The bluntest instrument that leaders use to censor citizens is the internet shutdown. Africa leads the world in them, according to internet monitor Surfshark. Since 2015, 32 African countries have taken that step to restrict the flow of information within their borders. Between September 2020 and January 2022, African countries accounted for half of the 24 internet disruptions worldwide.

Burkina Faso alone shut down the internet three times between November 2021 and January 2022, including during the coup that toppled President Roch Marc Christian Kaboré.

Coups, anti-government protests and elections are the events most likely to trigger a full or partial blackout. In Algeria and Ethiopia, leaders blocked the internet in 2021 to prevent cheating on national school exams. Ethiopia also has imposed a media blackout to control news relating to the ongoing civil war in the Tigray region.

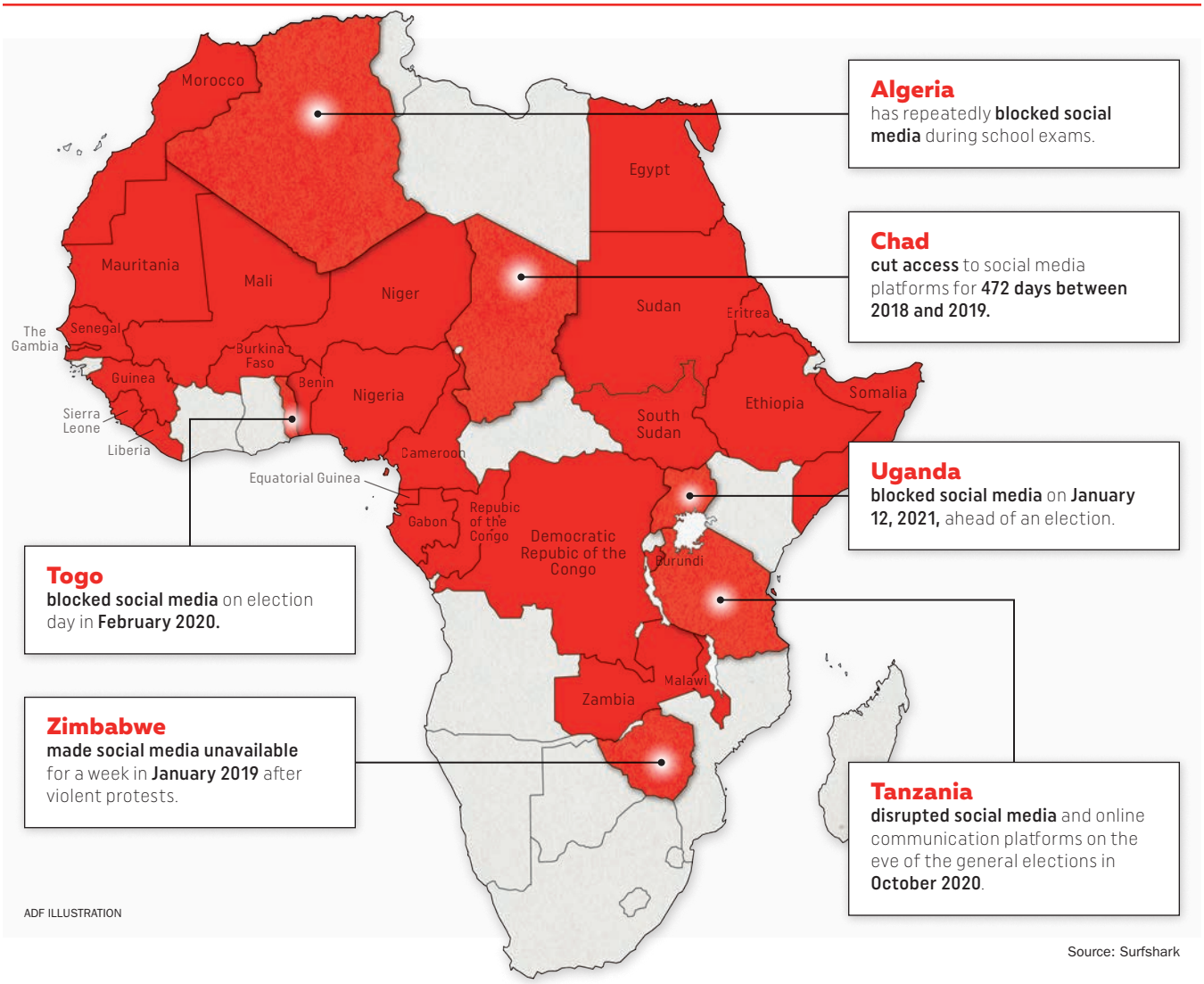
In some cases, leaders are most intent on throttling social media use. There's a clear reason for that, according to Lawrence Muthoga, former community engagement manager for Kenya-based Microsoft 4Afrika.

Nigerians protest the government's shutdown of Twitter in June 2021 after the social media site deleted a tweet by President Muhammadu Buhari, saying it violated its terms of service.

"It's because it's very easy to mobilize people on social media," Muthoga said during a discussion on African censorship hosted by Kenya's Moringa Group via Twitter Spaces.

"Most of the censorship that's happening across the continent as we speak is tied to controlling mobilization of people or the spread of ideas," Muthoga said.

32 AFRICAN COUNTRIES HAVE BLOCKED SOCIAL MEDIA IN RECENT YEARS



Source: Surfshark

Omojuwa sees another force at work: the generation gap between Africa's leaders and their young, tech-savvy citizens. Africa's median age is just under 20 years old. "They [leaders] don't understand these spaces," Omojuwa said.

Shutting down the internet is not as simple as closing a newspaper or silencing a radio broadcaster, Omojuwa said. During Nigeria's Twitter blackout, for example, Nigerians still could access the platform using virtual private networks operating through other countries.

"It's such a democratized space," Omojuwa said. "You can't stop people from talking."

LEGAL LIMITATIONS

The 39 African nations that have passed cybercrime legislation say they're targeting misinformation and national security risks. Critics say the laws threaten privacy and put people at risk of arrest for expressing themselves online.

"Governments haven't really caught up to what freedom of expression in the information age really means," said Setriakor Nyomi, Ghanaian director of technology for the Kenya-based Moringa School, which provides training for technology jobs.

"The question in the information age is how for governments to cope," Nyomi said during a conversation with Muthoga via Twitter Spaces.

Human rights should guide the process of creating internet regulations, according to Admire Mare, a professor of communication, journalism and media technology at Namibia University of Science. Mare studied cybercrime legislation in the 16 countries of Southern Africa. His report, "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights," cites South Africa as the only country in the region to craft legislation with citizens' rights in mind.

"In countries such as Zambia, Zimbabwe, Namibia and Malawi, there is deep-seated fear that existing and new legislation are already being used for surveillance

A man carries a banner protesting Nigeria's seven-month Twitter blackout, which caused an estimated $1.6 billion in damage to the country's economy.


DIGITAL
RIGHT IS
HUMAN RIGHT.
#LiftTwitterBan

Algerians protest government censorship of complaints about former President Abdelaziz Bouteflika's attempt to seek a fifth term in 2019. He resigned that year and died in 2021.

purposes," Mare wrote in the report published in conjunction with Zimbabwe's Media Institute of Southern Africa (MISA).

Zimbabwe's Data Protection Act bill bans messages inciting violence against people or property, bans transmitting false information meant to cause harm, and bans unsolicited emails, commonly referred to as spam.

MISA says the law lacks safeguards to guarantee that it won't be used to block civil society work, punish whistleblowers and violate the constitutional right to free expression. Before the bill passed, Transparency International Zimbabwe said it would hinder the public's ability to reveal government corruption.

"The authorities' loose interpretation and implementation of legislation is already used to repress the citizens they are supposed to protect," Muchaneta Mundopa, executive director of Transparency International Zimbabwe, wrote in the group's analysis of the then-bill. "This bill will make matters worse."

Mundopa cited the case of journalist Hopewell Chin'ono, who was charged under previously existing laws with inciting violence after exposing corruption in the government's procurement process for COVID-19 medical supplies. Whistleblowers such as Chin'ono need social media to alert the public to suspicious cases, Mundopa said.

"We therefore view the proposed legislation as the government's latest attempt to silence civil society and media and prevent us from playing our oversight role," Mundopa wrote.

Nigeria targeted social media with two proposals that met with stiff resistance from free speech activists. In 2015, the so-called Frivolous Petitions bill targeted misinformation online and criticism of public officials with fines of up to $10,000.

Free speech activists argued that the bill helped public officials silence critics and launched the #NoToSocialMediaBill campaign on Twitter. Facing public opposition, legislators eventually killed the bill.

Another social media bill drafted in 2019 was designed to criminalize the publication of false or malicious information online. That bill, too, eventually was withdrawn.

Omojuwa said Nigeria's two attempts at restricting communication online have put citizens on alert. "Anything the government does in the future, there will always be pushback," he said.

MEDIA AND SELF-CENSORSHIP

Alongside internet shutdowns and legislative efforts to regulate online speech, Africa's free expression advocates also confront growing Chinese and Russian influence in the continent's media environment.

China has spent many years building a continental network of print and broadcast media to promote

CHINA'S MEDIA STRATEGY BELONGS TO ITS "BORROWED BOAT" PHILOSOPHY, WHICH USES AFRICAN NEWS OUTLETS AND REPORTERS TO PUBLISH STORIES FAVORABLE TO CHINA

its own pro-government brand of journalism. China also spends heavily on advertising among some for-profit news outlets and provides others with expensive equipment such as satellite dishes as a way of gaining sway.

China sponsors hundreds of African journalists each year to receive training in Chinese newsrooms. There, they learn China's brand of journalism that emphasizes support for government policies rather than traditional reporting designed to hold government accountable to its citizens.

"In the spirit of the Beijing regime, journalists are not intended to be a counter-power but rather to serve the propaganda of states," Christophe Deloire, secretary-general of Reporters Without Borders, wrote in its report, "China's Pursuit of a New World Media Order."

Russia takes an even more heavy-handed approach. Through its Wagner Group private military contractor, it has launched a Russian-backed radio station in the Central African Republic (CAR) that broadcasts music along with news and talk shows.

CAR President Faustin-Archange Touadéra's Russian national security advisor, Valery Zakharov, installed two Russian public relations experts in his office to boost the president's image.

Meanwhile, much of the CAR's news media has taken a pro-Russian stance, giving extensive coverage to Russian actions such as donating sports equipment to a school. With no advertising to support their work, reporters in the CAR sometimes take money to write pieces favorable to the Russians, according to analyst Thierry Vircoulon, coordinator for the Observator for Central and Southern Africa at the French Institute of International Relations.

China's media strategy belongs to its "borrowed boat" philosophy, which uses African news outlets and reporters to publish stories favorable to China.

The smaller the media market, the greater China's influence, according to Dani Madrid-Morales, a professor at the University of Houston and expert in China's media machinations in Africa.

"What China has been able to do is establish these relationships at the personal level," Madrid-Morales told ADF. "By creating these links at the personal level, China helps gate-keep what information goes out."

That, he said, creates a form of censorship more subtle than internet shutdowns or legislative control: self-censorship by media outlets that soften coverage to avoid losing financial support and favorable reporting by journalists trained to avoid challenging those in power.

South Africa's IOL media network recently was sold to a group with Chinese investors. Soon after, the network's Western-trained editors were replaced with editors more favorable to the Chinese model. When columnist Azad Essa criticized China's treatment of its Uyghur minority, he lost his position the next day.

"I had, it would appear, veered into a nonnegotiable arena that struck at the very heart of China's propaganda efforts in Africa," Essa later wrote in Foreign Policy.

China's growing influence over Africa's media landscape includes training African journalists in China-based newsrooms, where the emphasis is on supporting government policies.

LOOKING AHEAD

What does the future hold for freedom of expression within Africa's media and online communities? Overall, the trend is toward more restrictions, according to Kian Vesteinsson, an analyst at Freedom House.

"Unfortunately, internet freedom has declined across Africa in recent years," Vesteinsson wrote. "At a high level, challenges to democratic transitions in countries like Ethiopia and Sudan have sharpened the decline of internet freedom in those countries."

Omojuwa said Nigeria's Twitter blackout proved an embarrassing failure but could inspire imitators elsewhere as more Africans find their voices on the internet.

"I think a lot of governments on the continent are looking at how Nigeria pushed Twitter around," he said. "Nigeria got away with it."

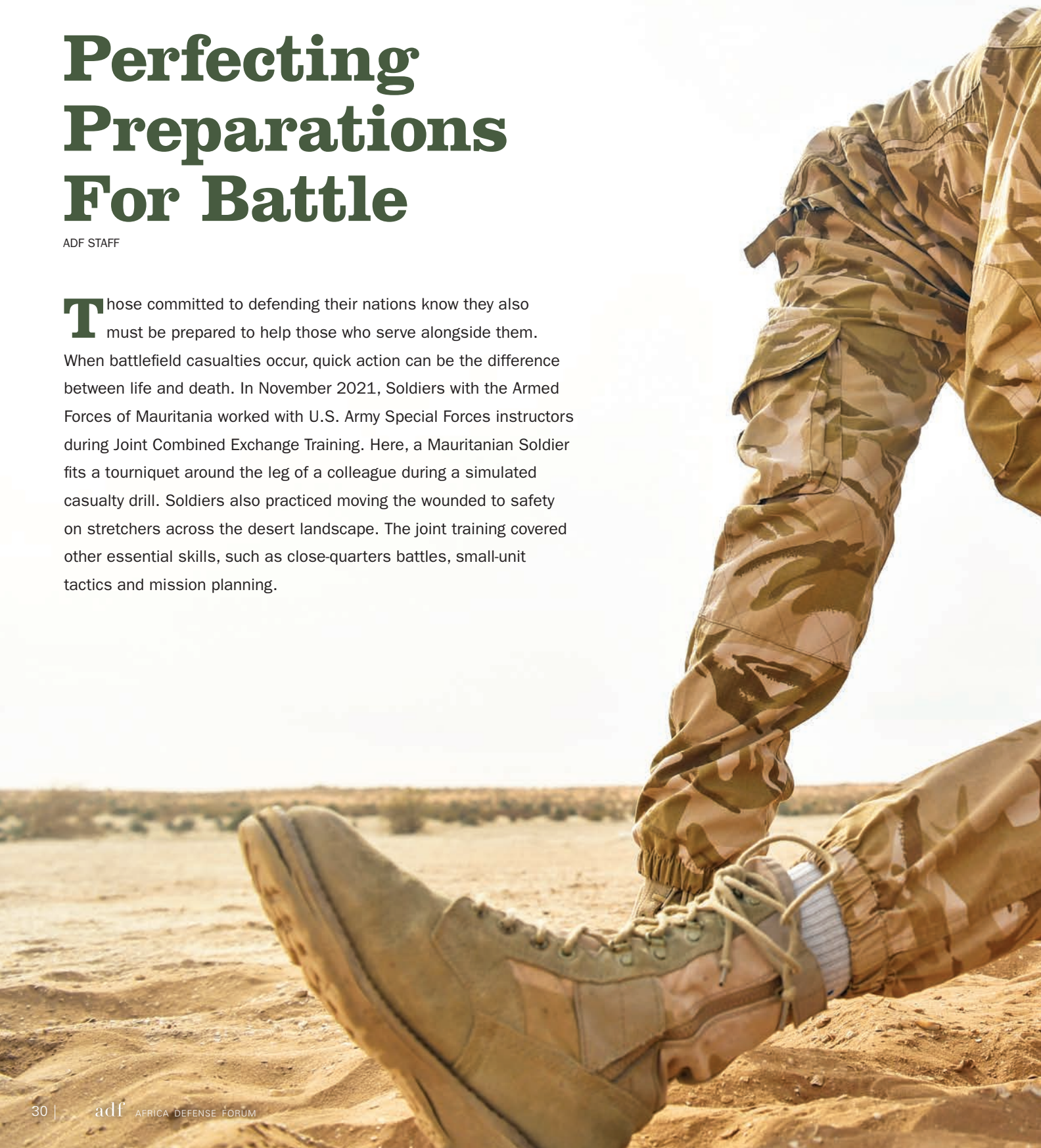
The impact of restrictions on free expression will be detrimental to democracy, he said.

"If the people don't have the ability to speak, what's the point of democracy?" Omojuwa said. ❑

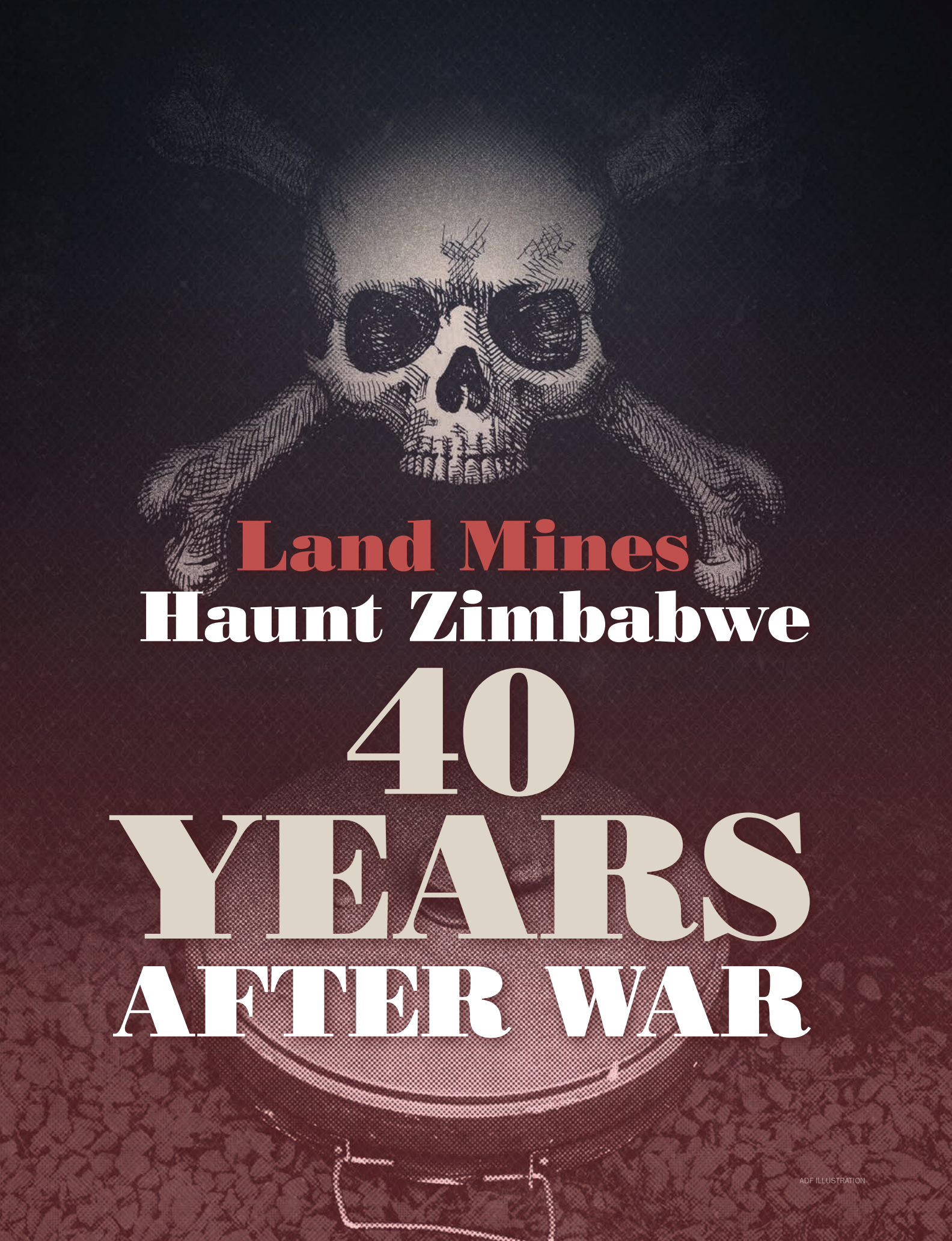
Perfecting Preparations For Battle

ADF STAFF

Those committed to defending their nations know they also must be prepared to help those who serve alongside them. When battlefield casualties occur, quick action can be the difference between life and death. In November 2021, Soldiers with the Armed Forces of Mauritania worked with U.S. Army Special Forces instructors during Joint Combined Exchange Training. Here, a Mauritanian Soldier fits a tourniquet around the leg of a colleague during a simulated casualty drill. Soldiers also practiced moving the wounded to safety on stretchers across the desert landscape. The joint training covered other essential skills, such as close-quarters battles, small-unit tactics and mission planning.



STAFF SGT. NICHOLAS BYERS/U.S. ARMY



Land Mines Haunt Zimbabwe 40 YEARS AFTER WAR

ADF ILLUSTRATION

The Southern African Nation Hopes To Be Free of Mines by 2025

BY CYRIL ZENDA

Talakufa Mudzikiti thought that the 1979 cease-fire ending Zimbabwe's 15-year war would make it safe to search for his family's lost cattle. It would end up being a costly adventure that he now regrets.

As he wandered the forests near Dumisa village in southeastern Zimbabwe, he stepped on an anti-personnel mine that blew off his left leg. "My life was destroyed that day … all my dreams were shattered," he said. Mudzikiti, now 70, is not alone in suffering from the legacy of land mines used in armed conflict.

Mudzikiti and his fellow villagers are among more than 2,000 Zimbabweans who are maimed but alive. Nearly 1,700 others have been killed by land mines over the past four decades.

Dense Belts of Land Mine Contamination

Zimbabwe, previously known as Rhodesia, gained independence in 1980, ending 90 years of colonialism and white minority rule. The 1970s were marked by a brutal bush war that killed more than 50,000.

To deter liberation fighters entering the country from neighboring Mozambique and Zambia, the Rhodesian army planted an estimated 3 million anti-personnel mines between 1974 and 1979 in five major minefields across 850 kilometers of the country's eastern and northern borders.

Mine Casualties Worldwide in 2020	
Civilian	4,437
Deminer	27
Military	1,105
Unknown	1,504

Source: Landmine Monitor 2021

Dense belts of land mines — some with about 5,500 per square kilometer — on Zimbabwe's border with Mozambique have hindered development in marginalized communities.

As of September 2018, mines were thought to dot more than 66 square kilometers of land. A survey of Zimbabwe's northeastern region identified 87 communities containing more than 75,000 people directly affected by mines.

The survey also found that 78 minefields were within 500 meters of residential areas.

Continued on page 35

Land mines and debris are disposed of outside Juba, South Sudan. AFP/GETTY IMAGES

A Libyan demining expert shows a buried mine believed to be planted by the army of former leader Moammar Gadhafi near Mitiga International Airport, outside Tripoli. AFP/GETTY IMAGES

Land mine victims wait to start physiotherapy in a ward at the Agostino Neto orthopedic center in Huambo, Angola. AFP/GETTY IMAGES

Continued from page 33

The land mines block access to residential land, inhibit cross-border trade, deny small-scale farmers access to agricultural land, separate communities from primary water sources, and adversely affect sanitation and livestock production. As a result, most affected areas have disproportionate levels of poverty and high rates of food insecurity.

National Mine Action Strategy

As a party to the Anti-Personnel Mine Ban Convention, the government of Zimbabwe is committed to working toward meeting the 2025 target of making the country free of land mines by putting into operation the National Mine Action Authority of Zimbabwe, a policy and regulatory body for mine action in the country. Reporting to the authority is the Zimbabwe Mine Action Centre (ZIMAC), which coordinates the country's demining activity. In 2018, Zimbabwe launched its National Mine Action Strategy 2018-2025.

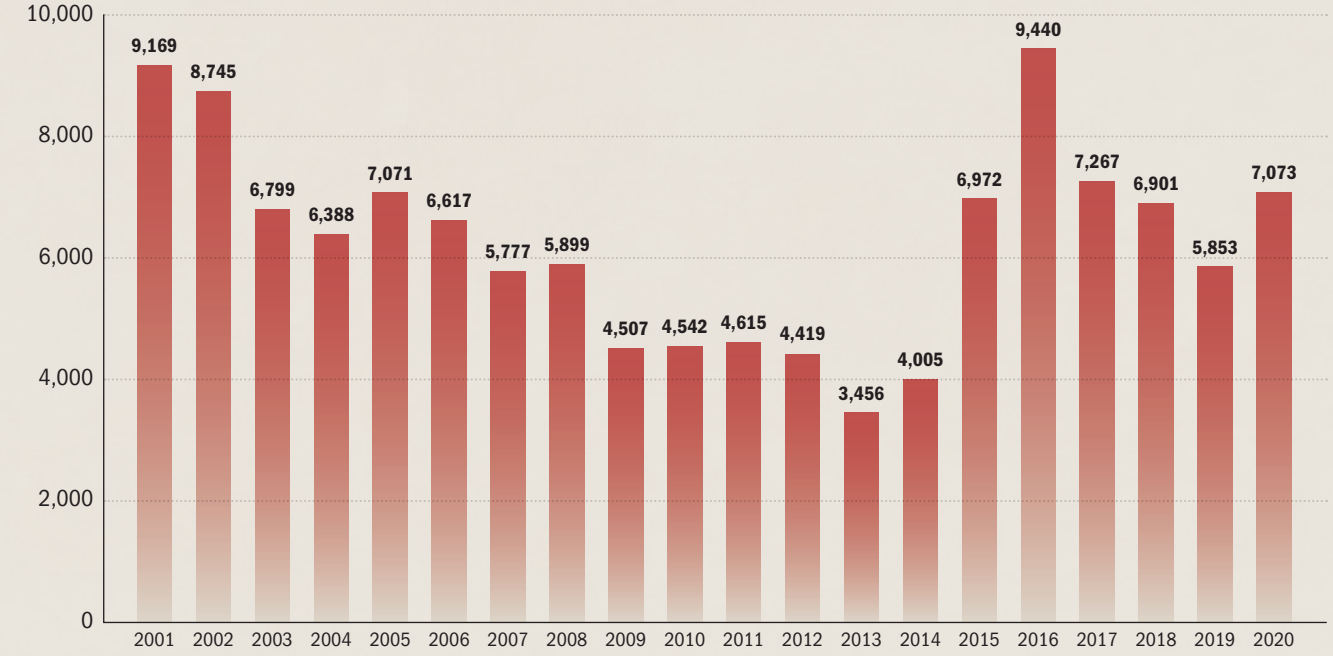
Zimbabwe has five demining missions: the Zimbabwe National Army's National Mine Clearance Unit, HALO Trust, Mines Advisory Group, the Norwegian People's Aid (NPA) and Belgian-registered APOPO, or Anti-Personnel Landmines Removal Product Development.

Sten-Trygve Brand, advisor for Mine Action and Disarmament at NPA, said the organization's mine clearance work has directly benefited more than 70,000 people in Zimbabwe.

"We have been part of the humanitarian demining efforts in Zimbabwe since 2012 …

Global Mine and Explosive Remnant Casualties: 2001-2020

Source: Landmine Monitor 2021



Talakufa Mudzikiti lost his left leg after stepping on a land mine in Zimbabwe.

CYRIL ZENDA

and currently operating with five demining teams and one MDD [mine dog detection] team," Brand said by email.

NPA has been working in three minefields with a total size of 16.7 square kilometers on the eastern border with Mozambique, namely Leacon Hill to Sheba Forest, Burma Valley and Rusitu to Muzite. Of these, the Burma Valley minefield was cleared and handed over in 2015, protecting 253 households. At the end of 2020, NPA had destroyed 26,982 anti-personnel mines and was left with an estimated contamination area of 7.2 square kilometers, which it intends to have cleared by 2024.

"Clearance and land release along the border have enabled communities and authorities to engage in activities such as border control, farming, access to clean water, attending schools in closer proximity to their villages, grazing livestock, as well as cross-border interaction without the threat of accidents, which may result in loss of a limb or life," NPA said.

HALO's work clearing land mines is focused in the nation's northeast, where it has been working since 2013 and has destroyed more than 100,000 land mines.

"Staggeringly, that's nearly four land mines for every person in that part of the country," the organization said. "Last year alone, HALO's team in Zimbabwe cleared nearly 10% of all land mines destroyed around the world."

Endangered Wildlife Also Killed

In addition to the human death and injury toll, anti-personnel mines have killed more than 120,000 cattle. The mines also have killed countless numbers of wild animals such as elephants, rhinos, lions and giraffes. Some of the minefields extend into the Gonarezhou National Park, which is part of

Lucia Zuka lost her right leg to a land mine in 1998 while searching for firewood. CYRIL ZENDA

the three-nation Great Limpopo Transfrontier Park. The larger park includes parts of Mozambique, South Africa and Zimbabwe, and allows for the free roaming of wildlife.

APOPO started demining work in December 2020 along the Cordon Sanitaire minefield that affects the Sengwe Wildlife Corridor in the southeastern part of the country. It intends to find and destroy about 15,300 land mines and clear 7.23 square kilometers.

"APOPO believes that it should be able to complete the task by 2025 or before with consistent donor support," the organization said.

"By clearing the land mines, APOPO can lay a strong foundation for communities to rebuild their lives and for agriculture and ecotourism to return and thrive, bringing many benefits to the nation as a whole."

Financial Constraints Delayed Clearance

The Zimbabwe National Army declined a request for comment. It is known, however, that financial constraints have hindered demining efforts. According to ZIMAC's revised mine action work plan for 2020-2025 submitted to Mine Action Review, $65.6 million is required by the mine action program to meet its extended deadline of 2025.

ZIMAC informed Mine Action Review that the economic downturn in 2018 likely would limit the government's potential to increase any funding for mine action, although it expected annual funding levels of $500,000 to be maintained.

The financial challenges facing the Zimbabwean Army have in the past been confirmed by Defense Minister Oppah Muchinguri-Kashiri, who said the Army has been lacking funding even for basic operations.

Villagers Grateful, Hopeful

"We are happy with the demining process which is taking place, but government should find a way of compensating us," Mudzikiti said in an interview. His sentiments are shared by other victims and family members of those killed.

Lisimati Makoti, who is Chief Sengwe in the Chikombedzi area, commended the land mine clearing exercise and said it is a noble initiative because his people had continued to suffer long after the war ended.

"We are grateful of this demining exercise," he said. "It was long overdue because my people were living at risk of losing their lives to land mines. … Many have also lost their livestock to the land mines." ❑

ABOUT THE AUTHOR
Cyril Zenda is a journalist based in Harare, Zimbabwe. His work has appeared in Fair Planet, TRT World Magazine, The New Internationalist, Toward Freedom and SciDev.Net.

ADF ILLUSTRATION

HOW TO CAPTURE A STATE

RUSSIA'S HYBRID TACTICS TO EXERT CONTROL IN THE CENTRAL AFRICAN REPUBLIC OFFER A WARNING TO THE CONTINENT

ADF STAFF

Small clouds of red dust rose from the Russian mercenaries' truck as they rode into the heart of Bambari, promising food to the hungry.

In the sweltering heat, dozens lined up along an earthen road in the Central African Republic's (CAR) fourth-largest city.

Instead of food, they were given handmade signs and ordered at gunpoint to protest MINUSCA, the United Nations peacekeeping mission in the CAR, demanding that the U.N. leave the city it liberated from rebels in late 2020.

It didn't add up for Nigerian journalist Philip Obaji Jr., who has reported extensively on the infamous Russian private military company (PMC) called the Wagner Group as it has expanded its operations in Africa.

"Multiple sources in CAR told me the anti-U.N. protest in the town of Bambari was a false-flag operation staged by Wagner mercenaries," Obaji told ADF. "Before significant numbers of Wagner left for Ukraine, I reported on new taxes on agricultural products that they've imposed and pocketed."

Obaji also received reports that Russian mercenaries massacred civilians in the villages of Mouka, Yangoudroudja, Aïgbado and Yanga.

Accusations of atrocities follow the Wagner Group like a shadow.

In the CAR, mercenaries are but one spoke in the wheel of Russia's hybrid approach that has combined hard and soft power for more than four years.

"CAR is currently in a state of state capture," Mattia Caniglia, a fellow at the European Council on Foreign Relations, told ADF. "The level of penetration we are witnessing now is enormous.

"At the moment you have a situation that is perfect for what Russia does."

A COUNTRY RIPE FOR EXPLOITATION

Russian operatives have been in the CAR since 2017 after crossing its porous northeastern border with Sudan. They have entrenched themselves by taking advantage of widespread instability, anti-French sentiment and a president in Faustin-Archange Touadéra who was on the verge of being overthrown by rebels.

A Russian military instructor works with a member of the Central African Armed Forces.

OFFICERS UNION FOR INTERNATIONAL SECURITY

RIGHT: A Russian military instructor speaks to a unit of the Central African Armed Forces.

OFFICERS UNION FOR INTERNATIONAL SECURITY

In more than four years, Russia has gained unprecedented access to the levers of governmental power and used it to spread propaganda, leaving many citizens uncertain of whom to trust in the country.

Caniglia describes Russia's approach in Africa as opportunistic and strategic, stressing the importance of distinguishing between its two pillars — official and unofficial activities.

"In the unofficial, we find a lot of asymmetric, hybrid stuff," he said. "In the official, we find that, too, but mostly it's about bilateral agreements, military training, weapons deals and more."

Russia's approach has been on full display in the CAR.

In 2018, Touadéra installed Kremlin-linked Valery Zakharov, a former Russian intelligence officer, as his national security advisor.

The European Union (EU) has called Zakharov "a key figure in … Wagner Group's command structure" who keeps "close links with the Russian authorities."

The level of power Wagner achieved in the CAR may have surpassed even its expectations.

"This is something rather unprecedented," Caniglia said. "But again, all of the conditions were right there in CAR. They achieved leverage that in any other place they were not allowed to have."

Another Touadéra ally, Alexander Ivanov, also reportedly has close ties to Wagner.

As the official representative of Russian military trainers in the CAR, Ivanov leads an independent "peace advocacy" group called the Officers Union for International Security (COSI).

Russia's Defense Ministry admitted that it used Ivanov to recruit all of its trainers deployed to instruct CAR's Armed Forces (FACA), according to Russia's statement to a U.N. expert panel.

Using private business proxies such as Wagner and COSI provides necessary cover for Russia. Its ability to deny official involvement is a critical piece of the deliberately opaque puzzle that is Russia's hybrid approach in the CAR.

"Their motivation is primarily financial," Kevin Limonier, a lecturer in geopolitics and specialist in Russian-speaking cyberspace, told The Africa Report magazine. "They see Africa as a place to make money and explore new horizons."

Russia's hybrid model lets it exert influence with a small investment of money and manpower.

"The Russian state does not necessarily have the means to fulfill its political ambitions in Africa," Limonier said. "It therefore relies on these networks that use unconventional methods and deny their involvement, should a problem arise."

With the Wagner Group, problems always arise.

HARD POWER: TRAINERS AND MERCENARIES

With an estimated 2,200 to 3,000 personnel, Wagner is the most notorious of the multiple Russian PMCs purportedly operating as trainers and security providers.

Whenever Touadéra and other high-level officials are in public, heavily armed guards in fatigues hover nearby. They travel in armored Russian vehicles and occasionally coordinate with Russian helicopters and drones.

What began as a training mission in 2018 ultimately evolved into counterinsurgency operations with Russian mercenaries in the field — in some cases commanding FACA units.

Reports of massacres at the hands of Russian mercenaries and FACA troops following their orders have destabilized the military.

The U.N. Office for the Coordination of Humanitarian Affairs estimates that 3.1 million people — more than 60% of the CAR's population — need urgent relief. The number of internally displaced people has risen to a record 722,000, and another 733,000 have sought refuge in other countries.

A Russian armored personnel carrier is delivered to the Central African Armed Forces in Bangui on October 15, 2020.

AFP/GETTY IMAGES

Alexander Ivanov speaks at the Bangui screening of the Wagner Group propaganda film "Tourist," which was shot in the Central African Republic.

OFFICERS UNION FOR INTERNATIONAL SECURITY

RIGHT: Ivanov speaks with a group of local journalists.

OFFICERS UNION FOR INTERNATIONAL SECURITY

In June 2020, a U.N. expert panel said it had "received numerous reports about Russian instructors who have been indiscriminately killing unarmed civilians," using excessive force and looting in the CAR, particularly in mining regions.

The panel also said Libyan and Syrian mercenaries had engaged in combat alongside Russian trainers.

The Office of the U.N. High Commissioner for Human Rights in March 2021 received reports of mass executions, torture, arbitrary detentions, forced displacement of civilians and attacks on humanitarian workers attributed to PMCs working with FACA, including the Wagner Group.

SOFT POWER: INFORMATION WARFARE

Russia has employed several soft-power means to promote its agenda in the CAR.

Through mercenaries, shell companies and other proxies, Russia has financed local media, sponsored "anti-imperialist" influencers, produced multimedia propaganda, and run disinformation and misinformation campaigns.

Wagner Group members and associates reportedly have built playgrounds and statues to themselves. They've created at least two Wagner Group propaganda films in the CAR to mythologize their actions. They've held football tournaments and beauty contests.

Kremlin-linked oligarch Yevgeny Prigozhin, accused by the EU of financing the Wagner Group, funded the creation of radio station Lengo Songo (which means "Building Solidarity" in the Sango language) for $10,000, according to the BBC. The station has a strong pro-Russia stance, blaming the U.N. and France for the CAR's crisis.

With Russia's mercenaries comes a suite of media services.

"They are cheap and come as part of a package of regime-support services, including political technologies," Mark Galeotti, an expert on Russian security affairs, said of Wagner to independent newspaper The Moscow Times.

Russian financing and media manipulation campaigns helped Touadéra win reelection in 2020 by a comfortable margin.

Zakharov reportedly oversaw the placement of Touadéra allies in key election positions, including vote tallying.

The CAR was one of eight African countries where social media giant Facebook suspended hundreds of fake accounts and dismantled what it concluded were Russian election interference campaigns. In the CAR, Russian trolls smeared the country's African neighbors and foreign partners while propping up Russia as a liberator.

Coordinated street protests followed, targeting France, MINUSCA and the Economic Community of Central African States.

MINUSCA in August 2021 also dealt with false rumors that it was supplying rebels with land mines, even as it was deploying personnel to remove such devices.

"MINUSCA has never used mines," U.N. forces spokesman Maj. Ibrahim Atikou Amadou told the BBC, noting that demining operations were at an impasse because of the allegations.

DIPLOMATIC POWER

Using its position on the U.N. Security Council, Russia created its first foothold in the CAR when the U.N. lifted an arms embargo, which allowed Russia to sell weapons to the country.

Russia's more recent U.N. efforts — blocking appointments to U.N. expert panels and thereby subverting the international sanctions

Central African Republic President Faustin-Archange Touadéra is believed to have first asked Russian President Vladimir Putin for military assistance during the 2019 Russia-Africa Summit in Sochi.

AFP/GETTY IMAGES

process — have thwarted investigations into Russia's and its PMCs' activities.

"It looks like Moscow wants to paralyze sanctions and panels of experts to divert attention from what Wagner is up to in Africa," International Crisis Group's U.N. Director Richard Gowan told Foreign Policy magazine. "So in some cases, it is simply a way of covering up some nefarious business."

THE COST FOR THE CAR

Securing lucrative gold, diamond and uranium concessions has been a high priority of Russian operatives in the CAR. With no government accounting of payments to Russian trainers or PMCs, experts believe mining rights are given in exchange for mercenary service.

The business of extracting the CAR's vast mineral wealth lies with Russian shell companies such as Lobaye Invest, which is linked directly to Prigozhin and was created in October 2017, along with a subsidiary PMC called Sewa Security Services.

Léopold Mboli Fatran, the CAR's minister of mines, gave Lobaye mining exploration permits in two regions in June and July 2018. He eventually granted permits in six regions: Alindao, Birao, Bria, N'Délé, Pama and Yawa.

Obaji and other journalists have connected massacres by mercenaries to many mining sites as the Russians attempt to secure their concessions.

Where once they were celebrated, Russians now find villagers fleeing their arrival.

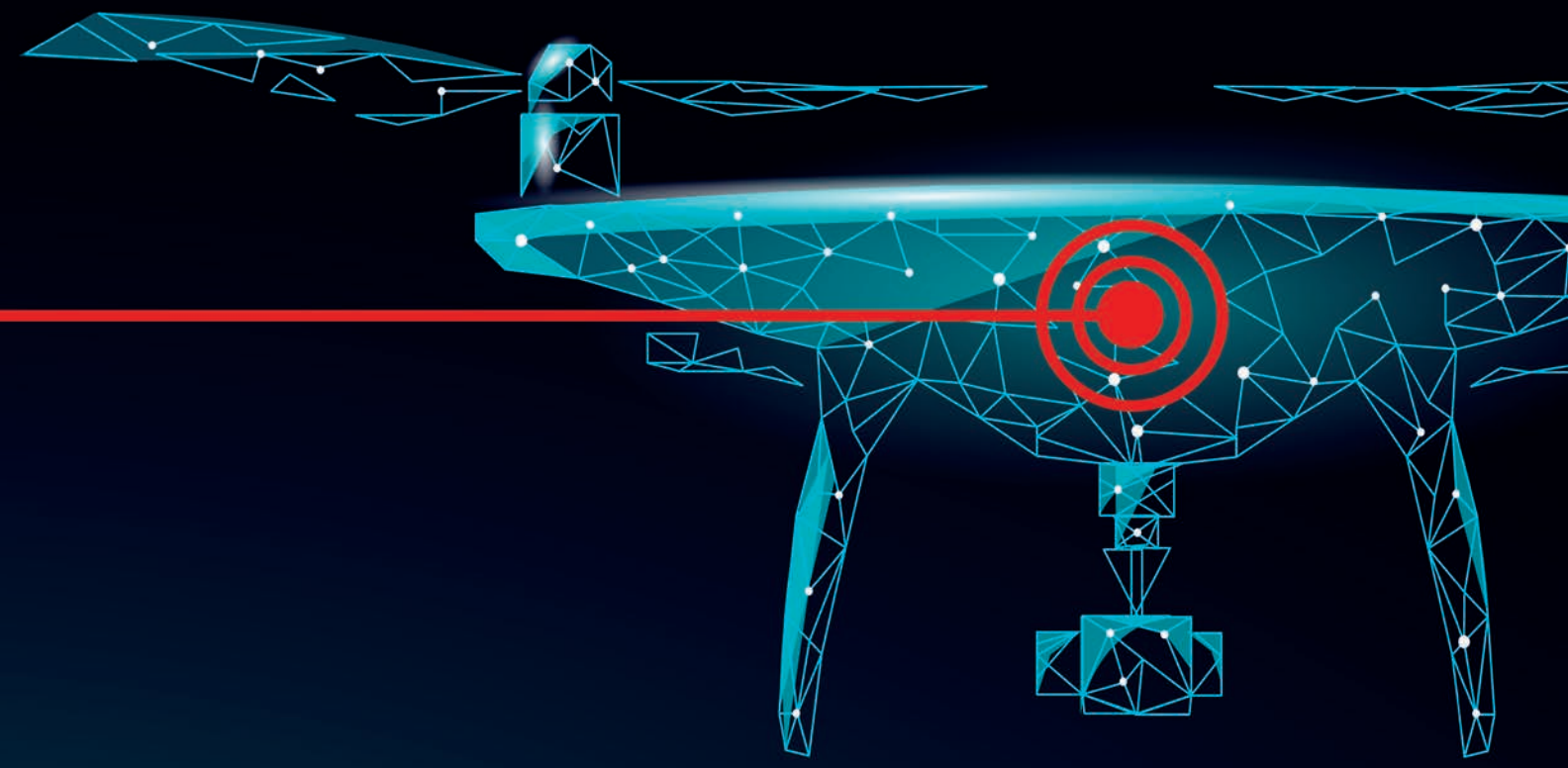
"The people were relatively happy with the Russians being there about two or three years ago," Caniglia said. "But now they know what kind of things are going down."

The U.N. Office for the Coordination of Humanitarian Affairs estimates that 3.1 million people — more than 60% of the CAR's population — need urgent relief. The number of internally displaced people has risen to a record 722,000, and another 733,000 have sought refuge in other countries.

Such results after more than four years of Russian involvement in the CAR could serve as a warning to other African countries considering their mercenaries, Caniglia said.

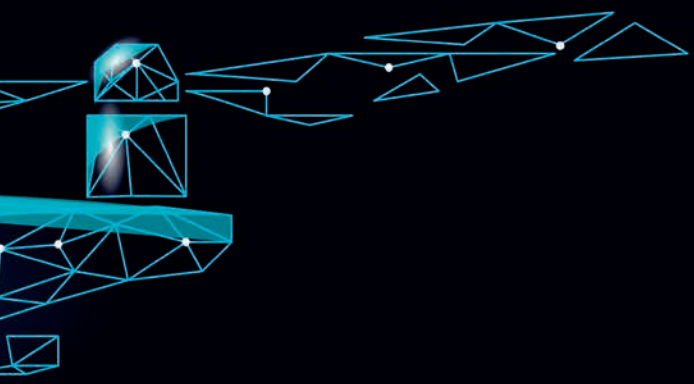
"But this is not what is happening," he said. Some countries in the Sahel region are signaling their openness to hosting Russian forces despite the clear track record they have of causing instability. Observers are surprised these countries are not learning the lessons from the CAR of the dangers of partnering with Wagner and Russia.

"What is happening in CAR is very bad, not only in terms of the level of influence that Russian nonstate actors have on the CAR government, but also in terms of human-rights abuses and further destabilization of the security situation. But it's not getting through. It's just not sticking," Caniglia said. ❑



DRONES CAN BE DEADLY WEAPONS FOR EXTREMISTS

Terrorists are using drones to identify targets and conduct surveillance in Africa. The next step will be weaponizing them.



ADF STAFF

Cheap, widely available drone technology has the potential to revolutionize medicine delivery, crop treatment and surveillance across Africa. But where innovators see an opportunity to improve lives, extremist groups see a chance to destroy them.

In the Middle East, terror groups have begun weaponizing off-the-shelf drones to attack civilian and military targets. Now, experts are warning, that deadly tactic could be coming to Africa.

"For $2,000 you can breach any fence in the world," Dedrone CEO Aaditya Devarakonda said, describing drones to Forbes magazine. "It's the most asymmetric threat out there." Dedrone secures airspace to protect organizations from malicious drones.

Signal-controlled drones, also known as unmanned aerial systems, date to the mid-1930s. Today, drones range from tiny radio-controlled $30 toys to craft the size of an airplane. In between are a staggering array of devices capable of transmitting video, scouting troop movements and carrying cargo.

The sophistication of over-the-counter "hobbyist" drones is astonishing. A simple drone that costs less than $1,000 includes four rechargeable motors with 30 minutes of flight time, a three-axis camera shooting high-resolution video, a sensor capable of shooting nighttime video and a video transmission range of more than 11 kilometers.

Most inexpensive drones can't carry much — less than 2 kilograms — but numerous companies have developed drones capable of transporting up to 200 kilograms. Such drones typically sell for about $250,000. That demonstrates the pace of drone development in the 21st century: A drone with such capacity would have been inconceivable at that price 20 years ago.

Science writer Kashyap Vyas said the past 10 years have seen a "huge explosion" in drone development.

"Drones are expected to become smaller and lighter with much longer battery life and flight times," Vyas wrote for the website Interesting Engineering. "In the civilian market, developments in improving flight times are allowing them to serve as delivery platforms, for use in emergency services, and for data collection in a number of areas too dangerous for humans, such as in power plants or fires."

Some now describe drone technology as a modern-day Pandora's box in that what started out for things such as aerial photography has grown and evolved in positive and terrible ways.

DRONES IN AFRICA

To date, there have been no reports of weaponized drones used by terror groups in Africa, but experts warn that this could change quickly.

Murtala Abdullahi, a Nigerian reporter who covers security issues for the site HumAngle, said drone access is tightly regulated in Nigeria so extremist groups have resorted to capturing government drones. So far, they mostly have been used for surveillance or propaganda efforts, but he said the groups are intent on expanding their use and want to learn from extremist groups in the Middle East.

"It has not been as sophisticated as in the Middle East where drones have been equipped with explosives to target troops, but it doesn't mean it won't happen in the future," Abdullahi said during an Africa Center for Strategic Studies (ACSS) webinar. "Information technology has allowed these groups to have knowledge from other regions, which means there is a huge risk of them improving what they already have by learning from others."

In Mozambique, extremists in Cabo Delgado province use drones for surveillance. Then-Mozambican Interior Minister Amade Miquidade reported in 2020 that extremists

Somali police and a Ugandan Soldier watch a drone during a training session.
REUTERS

REUTERS

A HISTORY OF WEAPONIZED DRONES

ADF STAFF

Terrorists' use of drones as weapons dates back almost a decade. Here are some known drone attacks:

- Al-Qaida used multiple drones in 2013 in an unsuccessful attack in Pakistan.
- The Islamic State group used small drones in attacks on Iraq and Syria in 2014.
- The Islamic State group used drones to drop light explosives on Iraqi Soldiers during the battle for Mosul in 2016 and 2017.
- A swarm of drones armed with bombs attacked Russian bases in western Syria in January 2018. Ten drones rigged with explosives attacked a Russian air base while another three targeted a Russian naval facility.
- Armed drones struck two oil-pumping stations in Saudi Arabia in May 2019. Officials blamed the attack on Yemen's Houthi rebels. Months later, Houthi forces launched drone attacks on three Saudi air bases. Houthi sources said the drones hit their targets, but Saudi officials said the drones were intercepted and downed.
- Houthi drones attacked two major oil facilities in Saudi Arabia in September 2019, causing fires.
- On September 14, 2019, the Houthis launched drone attacks at two major oil facilities run by Saudi Aramco and caused a blaze.
- Pakistan-based terrorists used two armed drones to attack an Indian Air Force base in June 2021.

had deployed drones in a region where a Southern African Development Community stabilization force had been authorized.

During extremist attacks in late March and early April 2021 that targeted, among other areas, the strategically important town of Palma, Miquidade said militants used drones to improve attack precision.

"If we look at the ease with which [the insurgents] are getting weapons and mounting attacks on the military, I will never underplay the possibility that they start making use of more technologically advanced capabilities, and with that I include drones," said Jasmine Opperman, a South African security consultant, in an ACSS paper. Opperman added that, "If you can bring in cellphones by the hundreds through illegal smuggling routes, what is preventing them from bringing in drones?"

Experts also are warning that drones have the potential to replace suicide bombers.

"Terrorist groups need individuals to carry out their attacks," wrote Maj. Thomas Pledger, an infantry officer in the U.S. Army National Guard. "Many groups typically conduct attacks with the expectation that their members will sacrifice themselves during the attack, either by being caught or killed. The use of drones, however, can allow an individual or a small group to conduct multiple attacks without self-sacrifice."

A major concern, say drone experts, is that developments in drone technology coincide with advancements in artificial intelligence (AI). Using AI could mean drones that don't need an operator. Experts envision extremists using "swarms" of small, inexpensive AI drones in targeted attacks.

Retired Col. David Peddle, a former member of the South African National Defence Force, confirmed that armed nonstate actors have been using drones for surveillance and believes it will be only "a matter of time" before the deployment of swarms or clusters of offensive drones in Africa, given their accessibility and relatively low cost.

Other experts agree, saying that modern technology and manufacturing has made drones increasingly affordable for terrorists. In his book "Life 3.0," physicist Max Tegmark wrote that "small AI-powered killer drones are likely to cost little more than a smartphone."

Additionally, drones will minimize the human investment required for terrorist attacks, with researchers noting that increased autonomy will enable one person to inflict more damage. AI could make terrorism cheaper and lower the human costs required to commit attacks, creating a new generation of "lone wolf" terrorists.

A technician checks a surveillance drone operated by the United Nations in the Democratic Republic of the Congo. REUTERS

The technology to attack individuals — facial recognition software, drones and machine-to-machine communication — already exists. Tegmark envisioned inexpensive AI-equipped assassination drones that are straight out of a James Bond movie: "All they need to do is upload their target's photo and address into the killer drone; it can then fly to the destination, identify and eliminate the person, and self-destruct to ensure that nobody knows who was responsible."

Researcher Jacob Ware, writing for the security website War on the Rocks, said the combination of simple AI and drones poses a genuine threat throughout the world.

"Terrorist groups are increasingly using 21st-century technologies, including drones and elementary artificial intelligence, in attacks," Ware reported. "As it continues to be weaponized, AI could prove a formidable threat, allowing adversaries — including nonstate actors — to automate killing on a massive scale. The combination of drone expertise and more sophisticated AI could allow terrorist groups to acquire or develop lethal autonomous weapons, or 'killer robots,' which would dramatically increase their capacity to create incidents of mass destruction in Western cities."

Pledger's study noted that drones open a new range of terrorist tactics and targets.

"A particularly frightening application of drones is the distribution of chemical and biological agents, especially infectious diseases," Pledger wrote. "Conversations around infectious disease are so prevalent, and the fear is known."

Pledger predicted that because of their "relatively low cost" and the "significant" distance from which they can be deployed, drones will be used as a "primary tactic of future terrorist attacks."

"Critical infrastructure is also vulnerable, and hardening thousands of locations against attack would be financially restrictive, at best," he wrote. "Probable infrastructure targets include fuel or water storage facilities, gas pipelines, power distribution plants and food supply locations, many of which are minimally or completely unmanned."

Karen Allen, a security expert for the Institute for Security Studies in South Africa, said drones represent "a new iteration of digital technology, and Africa will be involved."

"Although drone technology is largely used for positive purposes, the possibility for individuals to build drones with smartphones and open-source software will accelerate, and the results may be destabilizing," she wrote. "In short, drones are likely to be an integral part of future warfare in Africa." ❑

A technician launches a drone in Rwanda as part of a program that uses them to deliver medical supplies to rural areas.

AFP/GETTY IMAGES

ADF ILLUSTRATION

FACING HIGH-TECH ENEMIES

Extremists Are Weaponizing Technology, Social Media and Even Video Games In Their Attacks

ADF STAFF

More than 30 websites in Mozambique, including the Defense Ministry's, went down February 21, 2022, after being targeted by hackers.

An image of a man wearing a headscarf and holding a machine gun appeared on the site along with the words "hacked by Yemeni hackers." The targets included the portals of the national disaster management, roads administration and water agencies, as well as the Defense Ministry and the National Institute of Land Transport.

Officials said there was no loss of information or leak of citizens' personal data but noted that it was the country's first cyberattack of that magnitude. Analysts called on the government to strengthen cybersecurity amid fears that the hackers might be associated with terrorists.

As experts and researchers warn of a future in which extremists in Africa will use readily available technologies to advance their causes, other experts say it already has happened.

Extremists are using drones for surveillance. They're using social media for propaganda and to livestream events. They're making videos for recruitment and instructions. They're using communication tools to plan raids. In the future, experts say, commercial drones will be weaponized, and 3D printers will be used to make assault rifles.

It starts with the most common and versatile tool of all: a cellphone. As author Audrey Kurth Cronin noted during a May 2021 presentation by the Africa Center for Strategic Studies (ACSS), "Everyone has a powerful computer in their pockets."

A smartphone might not seem like a formidable weapon, or even a particularly sophisticated one, but it combines a computer, a precision timepiece, a camera, internet access, GPS, money transfer applications and more. It also eliminates insurgents' need to maintain radio communications equipment.

Extremists, experts say, use mobile phones for a wide range of purposes. One of them is to accept payments and transfer cash when they extort citizens for "tax payments" in remote areas they control.

Researcher Seth Harrison, writing for the Center for Strategic and International Studies, reports that groups such as the Islamic State group capitalize on readily available technology for propaganda and instructional purposes.

Chinese hackers stole information from African Union servers, forwarding the data to Shanghai. REUTERS

"These operations require little training or tactical planning, involve crude tools — like knives or cars — and can be conducted by anyone, anywhere. The combination of simple operations and increased communicative capacity has made terrorism accessible to the masses."

Two brothers used an al-Qaida online video, "How to Build a Bomb in Your Mom's Kitchen," to build a bomb they triggered at the Boston Marathon in 2013.

Smoke rises from Westgate Shopping Mall in Nairobi, Kenya, in 2013 after a terrorist attack. Terrorists publicized their attack on Twitter.

THE ASSOCIATED PRESS

Technology experts warn of extremists using easily available commercial drones to conduct surveillance and plan attacks. In the future, they say, drones could be used in Africa to transport small amounts of explosives and in assassinations.

ALREADY IN USE

It helps to divide technology into two groups: open and closed. Closed technology is unavailable to almost everyone but governments and includes nuclear weapons, major weapons systems, fighter jets and radar. Open technology is available to anyone and includes GPS systems, the internet, smartphones and microchips. Although closed technology occasionally has fallen into the hands of extremists, for the most part, open technology poses the biggest problems.

Although nonstate actors are a primary concern, they are not the only problem. As Nathaniel Allen of the ACSS noted in a January 2021 report, "The greatest concerns surrounding cyber espionage in Africa have been linked to China."

In 2018, it was reported that all content on the servers in the African Union's headquarters was being routinely transmitted to Shanghai, China, after network engineers noticed a spike in use during off-hours. Although engineers replaced the servers, Chinese hackers continued to spy on the AU in 2020 by stealing footage from surveillance cameras. They hid their tracks by transmitting the information back to China during normal business hours. A Chinese hacking group called Bronze President was to blame, according to Reuters, which said the surveillance covered "AU offices, parking areas, corridors, and meeting rooms."

A security guard patrols the reopened Westgate Shopping Mall in Nairobi, Kenya, nearly two years after terrorists attacked it.

THE ASSOCIATED PRESS

In June 2020, the Ethiopian Information Network Security Agency stopped a cyberattack from the Egypt-based Cyber Horus Group. Allen wrote that the attack, Ethiopian authorities said, was part of an attempt to put "economic, psychological, and political pressure

on Ethiopia" over the filling of the Nile River's Grand Ethiopian Renaissance Dam.

Ethiopian authorities said they prevented a broader attack, yet the Cyber Horus Group managed to hack into a dozen or so government webpages, posting messages threatening war if Ethiopia began filling the dam.

> *"Recruiters can target people on open platforms, and they start building relationships before inviting these people to more closed-off environments."*
>
> *~ The Radicalisation Awareness Network*

A LACK OF TECH

Anouar Boukhars, a professor of counterterrorism and countering violent extremism at the ACSS, noted that extremists in Africa are using cyber technology for training, propaganda, recruitment, financing and planning. He said extremists use information technology to control the pace and narrative of violence and that Boko Haram used cyber sabotage as early as 2012.

Boukhars said most extremists' cyberattacks in Africa have been fairly unsophisticated. He said although it can be assumed that extremists would like to have military-grade drones, such devices are costly to build, operate and monitor. Extremists are more likely to use commercial-grade drones. Even advanced government military operations are beginning to use civilian-grade drones.

Dr. Christopher Anzalone, a research assistant professor at Marine Corps University in Quantico, Virginia, said that al-Shabaab is among the most aggressive extremist groups in adopting technology for recruitment. Their propaganda films' polished appearance resembles "pseudo-documentaries," he said.

Anzalone said al-Shabaab also continues to rely on low-tech means — radio broadcasts and simple photography — to get its message out. But the group was an early adapter of Twitter, he noted, and live-tweeted its 2013 attack at Westgate Shopping Mall in Nairobi, Kenya, where 67 people died before four masked gunmen were killed.

VIDEO GAMES

A study at the University of North Carolina at Chapel Hill found that terrorist groups are lifting elements from popular video games, especially the popular Call of Duty series, to use for recruitment and practice. First-person

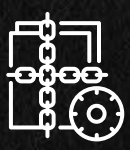
INTERPOL IDENTIFIES TOP AFRICAN THREATS

Interpol's African Cyberthreat Assessment Report 2021 identifies the most prominent threats in Africa, based on input from Interpol member countries and data drawn from private sector partners.

Online scams: Fake emails or text messages claiming to be from a legitimate source are used to trick individuals into revealing personal or financial information.

Digital extortion: Victims are tricked into sharing sexually compromising images that are used for blackmail.

Business email compromise: Criminals hack into email systems to gain information about corporate payment systems, then deceive company employees into transferring money into their bank account.



Ransomware: Cybercriminals block the computer systems of hospitals and public institutions, then demand money to restore functionality.

Botnets: Networks of compromised machines are used to automate large-scale cyberattacks.

AFRICA SLOW TO RATIFY CYBERSECURITY RULES

The African Union adopted the African Union Convention on Cybersecurity and Personal Data Protection, also known as the Malabo Convention, in Malabo, Equatorial Guinea, on June 27, 2014.

Its objective is to set out the critical rules for establishing a safe digital environment and address the gaps in the regulation and legal recognition of electronic communications and electronic signatures. It is also concerned with the absence of specific rules that protect consumers, intellectual property rights, personal data and information systems, and privacy online.

Currently, only eight African countries have ratified the agreement.

The Africa Data Security Conclave says that the key provisions of the Malabo Convention include:

- Setting forth security rules essential to establish a credible digital space for electronic transactions, personal data protection and combating cybercrime.
- Establishing a legal framework aimed at strengthening fundamental rights and public freedoms, protection of physical data, and punishing any violation of privacy "without prejudice to the free flow of personal data."
- Adopting legislative and/or regulatory measures as they deem necessary to put specific responsibility on institutions and their officials in relation to their responses to cybersecurity incidents.
- Promoting accountability in matters of cybersecurity at all levels of government by defining their roles and responsibilities in precise terms.
- Establishing a national protection authority as an independent administrative entity tasked with ensuring that processing of personal data is duly regulated.
- Developing public-private partnerships as a model to engage industry, civil society, and academia in the promotion and enhancement of a culture of cybersecurity.
- Forming international partnerships that aim to regulate issues of double criminal liability, exchange of information between countries and response to cyber threats.

On a more basic level, the realism of modern video games is such that players intent on real-world violence can actually practice their tactics while playing.

shooter video games are played by millions of people, generally under the age of 30 and overwhelmingly male — a critical demographic for extremist groups.

The Radicalisation Awareness Network (RAN) said games such as Call of Duty and Grand Theft Auto let users create their own modifications, which can be abused by extremists. "This tactic places powerful (gaming) engines at the disposal of extremists," the network reported.

"Extremist mods garner press attention and give the illusion of credibility and technical competence to those unfamiliar with the ease with which mods can be created," RAN reported in 2020. "It is unclear if modded games have ever had an impact on recruitment beyond propaganda."

Many such networked games include a chat feature, allowing players to communicate with each other. "Recruiters can target people on open platforms, and they start building relationships before inviting these people to more closed-off environments," RAN said.

On a more basic level, the realism of modern video games is such that players intent on real-world violence can practice their tactics while playing. Terrorist Anders Breivik, who murdered 77 people in Oslo, Norway, in 2011, trained for his rampage by playing Call of Duty. In a manifesto Breivik wrote, he called Call of Duty: Modern Warfare 2 "probably the best military simulator out there" and said he viewed the game as "part of my training-simulation."

PROTECTION NEEDED

Research shows that national governments need to be more proactive to protect themselves from cyberattacks. In the past 10 years, legal website JD Supra reports, 33 African countries have passed laws and adopted regulations on cybersecurity, cybercrime, electronic transactions and data protection.

Attendees play Call of Duty WWII at a videogame conference. Researchers say terrorist groups are lifting elements from such games to use for recruitment and practice. THE ASSOCIATED PRESS

African heads of state attend an African Union assembly in Addis Ababa, Ethiopia, in February, 2022. THE ASSOCIATED PRESS

Economists and technology professionals have urged African countries to ratify the Malabo Convention, which has been described as one of the world's most elaborate cybersecurity accords. Its purpose is to establish a "credible framework for cybersecurity in Africa through organization of electronic transactions, protection of personal data, promotion of cyber security, e-governance and combating cybercrime."

So far, only eight African countries have ratified the Malabo Agreement. For it to come into force, at least 16 African countries must adopt it.

Allen of the ACSS said there aren't enough highly trained cyber professionals available to combat threats. The continent is in a race to catch up.

"The lack of an effective response is due, in part, to deficits in capacity," Allen wrote. "The continent faces a growing 100,000-person gap in certified cybersecurity professionals. Many organizations, businesses, and agencies lack basic cyber awareness and fail to implement rudimentary cybersecurity measures. Governments frequently fail to monitor threats, collect digital forensic evidence, and prosecute computer-based crime. Ninety-six percent of cyber security incidents go unreported or unresolved, meaning that cyber threats in Africa are likely much worse than recognized."

A particular concern will be in striking a balance between stopping cybercrimes and cyberattacks while preserving human rights. Cyber terrorists, Boukhars said, need to be defined with "precision" so that ordinary citizens do not have their rights restricted. He noted that surveillance technologies frequently have been used to restrain legitimate political dissenters.

Cronin said governments can "overcorrect" on surveillance, spying on their own citizens. Such spying destroys the legitimacy of a government and its rule of law. She said that government legitimacy must be maintained by balancing going after bad actors and preserving human rights. ❑

DRC's Self-Taught Guitar-Maker

CATERS TO STARS

REUTERS

In a tin shed off the backstreets of Kinshasa, the Democratic Republic of the Congo's (DRC) capital, a barefoot 61-year-old Jean-Luther Misoko Nzalayala, known as Socklo, hacks with a machete at a lump of wood that is starting to resemble the neck of a guitar.

Later, he hammers bits of white plastic from a chair into it as inlay to help guide players around the fretboard, and he uses threads of motorcycle brake cable as strings.

For more than 40 years, the self-taught instrument-maker has used a variety of recycled materials and local hardwoods to create guitars. Socklo's passion began in his DRC village of Kikwit in 1975, when he dismantled and copied a guitar a friend had given him.

Three years later, he moved to Kinshasa, where he sold his first guitar to his cousin. "I couldn't imagine that people in a city like Kinshasa could like a guitar like this. It gave me courage."

He used negative feedback to improve his craft and finesse his designs. Soon, local and international musicians were flocking to his tin shed.

Congolese music star Jupiter Bokondji loved the sounds of Socklo's guitars and asked him to go electric. The result, Bokondji said, is far more authentic than top guitar brands, which cost up to 20 times more.

"I have played it all over the world; everyone is amazed," Bokondji said. "To see that guitar doing what it does, the way it plays, it's like a tornado."

Yarol Poupaud, a French guitarist who toured with rock 'n' roll singer Johnny Hallyday for years, has bought four of Socklo's creations.

"It has little imperfections; it's not perfect, but that really makes the magic," Poupaud said, strumming on a blue starburst guitar emblazoned with the DRC's flag.

Guitar-maker Misoko Nzalayala Jean-Luther, known as Socklo, plays a guitar in his workshop in Kinshasa, Democratic Republic of the Congo.

KEEPING TRADITION ALIVE,

ARTISTS CARVE CAMEL BONES

REUTERS

Somali artisan Muse Mohamud Olosow carefully sorts through a huge pile of camel bones discarded by a slaughterhouse in Mogadishu, selecting pieces that he will carve into jewelry and ornate beads used by fellow Muslims while reciting prayers.

To Olosow's knowledge, he is one of just four artisans in his country of 16 million people who work with camel bones. In 1978, in one of Somalia's many periods of war and turmoil, gunmen killed dozens of craftsmen in Mogadishu and another town, he said.

For years, he carved his bones secretly at home and then took them to markets to sell discreetly.

Olosow, whose strong hands and arms bear callouses and muscles from his work, learned his craft from his father in 1976.

He plans to ensure that this decades-old tradition does not fade away after he is gone.

"My kids will inherit these skills from me, that I inherited from my father," he said from his workshop in the Somali capital. "I do not want these skills to stop."

His clients mostly are government officials or wealthy Somalis living abroad. Just one set of his painstakingly carved prayer beads can cost about $50 in a country where seven in 10 people live on less than $2 per day.

A customer visiting his shop says the work justifies the price. "What matters is quality not price. I prefer this one to beads imported from other countries like China."

For Olosow and his family, carving bones has been their main source of income for decades. They invested nearly $5,000 to import machines from Italy to chisel and puncture the tough bones, he said, making it faster and safer to work "without bruises."

"Our plan is to export these items to other countries," he said. "We shall continue this art craft until we become rich! God willing."

Somali artisan Muse Mohamud Olosow works on ornate beads made from discarded camel bones at his workshop in Mogadishu. REUTERS

AFP/GETTY IMAGES

Tennis Star Plays for

'MY COUNTRY, MY CONTINENT, MY REGION'

ADF STAFF

Ons Jabeur of Tunisia hits a forehand return during a 2021 tournament in the United States.

Tunisian tennis player Ons Jabeur got the world's attention when she won the French Open junior title in 2011. Now, she says, tennis is more than just a sport for her.

Her home country has little in the way of tennis infrastructure and no established path for players to become professionals. Jabeur says she wants to change that.

"I don't play for myself anymore. I play for my country, my continent, my region," Jabeur told The National, a United Arab Emirates newspaper. "Tennis for me is not just a sport. I try to set an example for people who want to be here one day, to have that opportunity to compete."

As of early 2022, she was ranked 10th in the world, making her the top-ranked African tennis player, male or female, at that time.

She was 16 when she won the junior division at the French Open, making her the first North African junior to take the title. Since then, her career as a professional tennis player has had some challenges. She had to withdraw from the 2022 Australian Open because of a back injury. But she has firmly established herself as a top player on the Women's Tennis Association tour.

"I know there are a lot of women in other countries who are not able to do that, and by me representing Arab women, I can lead by example," she told The National. "It's very important for me and hopefully I can succeed in sharing this message."

Growing up in Tunisia, she at times had no access to school or club tennis courts, forcing her to practice at the courts of nearby hotels. Jabeur began playing on the International Tennis Federation's Junior Circuit in 2007 when she turned 13.

With her skills and the support of her parents, she trained in Belgium and France starting at age 16.

GLOBAL PIRACY DROPS TO 18-YEAR LOW

A helicopter from Nigeria's Maritime Security Unit prepares to rescue unit members as part of an anti-piracy drill in Lagos. REUTERS

DEFENCEWEB

Piracy and armed robbery at sea dropped to their lowest levels in 18 years in 2021. The International Maritime Bureau (IMB) is crediting "vigorous action" by authorities in protecting seafarers.

In 2021, the IMB Piracy Reporting Centre received reports of 132 incidents of piracy and armed robbery against ships. There were 115 vessels boarded, 11 attempted attacks, five vessels fired on and one vessel hijacked. The Gulf of Guinea remained the world's piracy hot spot.

IMB Director Michael Howlett welcomed the reduction in incidents while urging coastal states to stay attuned to the risk and "robustly" address crime in their exclusive economic zones.

"While the IMB applauds these actions, it further calls on the coastal states of the Gulf of Guinea to increase their collaboration and physical presence in their waters to ensure a long-term and sustainable solution to address the crime of piracy and armed robbery in the region," Howlett said.

The increased presence of international naval vessels and cooperation with regional authorities played a role in the reduction, Howlett said. This included the actions of the Royal Danish Navy, which returned fire on a speedboat carrying eight suspected pirates in November 2021, killing four and capturing the others.

The Gulf of Guinea region saw reported incidents decrease from 81 in 2020 to 34 in 2021. Kidnappings at sea dropped 55% in 2021 in the Gulf. The Gulf of Guinea continues to account for all kidnapping incidents globally, with 57 crew members taken in seven incidents.

The IMB Piracy Reporting Centre warned that the threat to seafarers persists, and it continues to urge crews and vessels plying these waters to be cautious. This is because perpetrators are violent and the risk to crews remains high. Evidence of this was the kidnapping of six crew members from a container vessel in mid-December 2021.

Kenya Builds DNA Database To Stop Illegal Fishing

ADF STAFF

Kenya is building a DNA database of its marine species to conserve its sea resources amid widespread illegal fishing. The exercise involves harvesting species and cataloging them to help the government prosecute illegal fishing cases. Since the program started in 2022, Kenya has produced bar codes for about 115 species, including sharks, rays, crustaceans and mollusks.

"Kenya has more than 6,000 commercial species and for years we could not claim any illegally harvested fish originated from the country," Thomas Mkare, a senior research scientist at Kenya Marine and Fisheries Research Institute, told The East African. "With this scientific exercise, we shall be able to claim our resources since even though fish look similar physically, each has special molecular identification which is associated with a certain region."

The project, which is expected to last several years, began after Francis O. Owino, newly appointed principal secretary of the State Department for Fisheries, Aquaculture and the Blue Economy, in March 2021 urged institute scientists to enhance research as the country looked to stimulate its blue economy.

"The country demands of you to provide answers as researchers to take the country to the next level," Owino said in a report by Science Africa. "We demand that you provide answers to the fishing challenges we face as a country."

Once established, the reference library is expected to strengthen food security by contributing to sustainable harvesting. Through the database, fish sold anywhere in the world can be traced back to Kenyan waters using their unique DNA identifiers.

Kenya's marine resources are declining due to an influx of foreign industrial trawlers, including those from China. Analysts say the COVID-19 pandemic also spurred unemployed people to turn to illegal fishing for income.

A report compiled by Global Fishing Watch revealed that 230 fishing trawlers operated off Kenya between May and August 2021. Many of them were owned by companies in China and Italy, Africanews reported.

AFP/GETTY IMAGES

NEW PAYMENT SYSTEM *Helps Intra-African Trade*

ADF STAFF

A new system is helping retailers make sales across borders. The Pan-African Payments and Settlement System (PAPSS) launched in Accra, Ghana, in January 2022. It lets a buyer make a payment in one national currency so a seller in another country can be paid in their own local currency. It is designed to open up trade between African countries and process payments in less than two minutes.

"There are 42 currencies in Africa. We want to make sure that a trader in Ghana can transfer Ghanaian cedi to a counterpart in Kenya, who will receive Kenyan shillings," Wamkele Mene, secretary-general of the African Continental Free Trade Area (AfCFTA), told Rwanda's New Times.

Mene said currency conversions cost Africa as much as $5 billion annually. In streamlining the process, PAPSS can keep that money on the continent and could eventually allow for a reduced dependence on foreign currencies.

"Why should we require hard currencies for trade between Kenya and Uganda or between Senegal and Guinea?" Benedict Oramah, president and chairman of the African Export-Import Bank (Afreximbank), told The Africa Report. "Why can't we operate as if every African currency is convertible within Africa?"

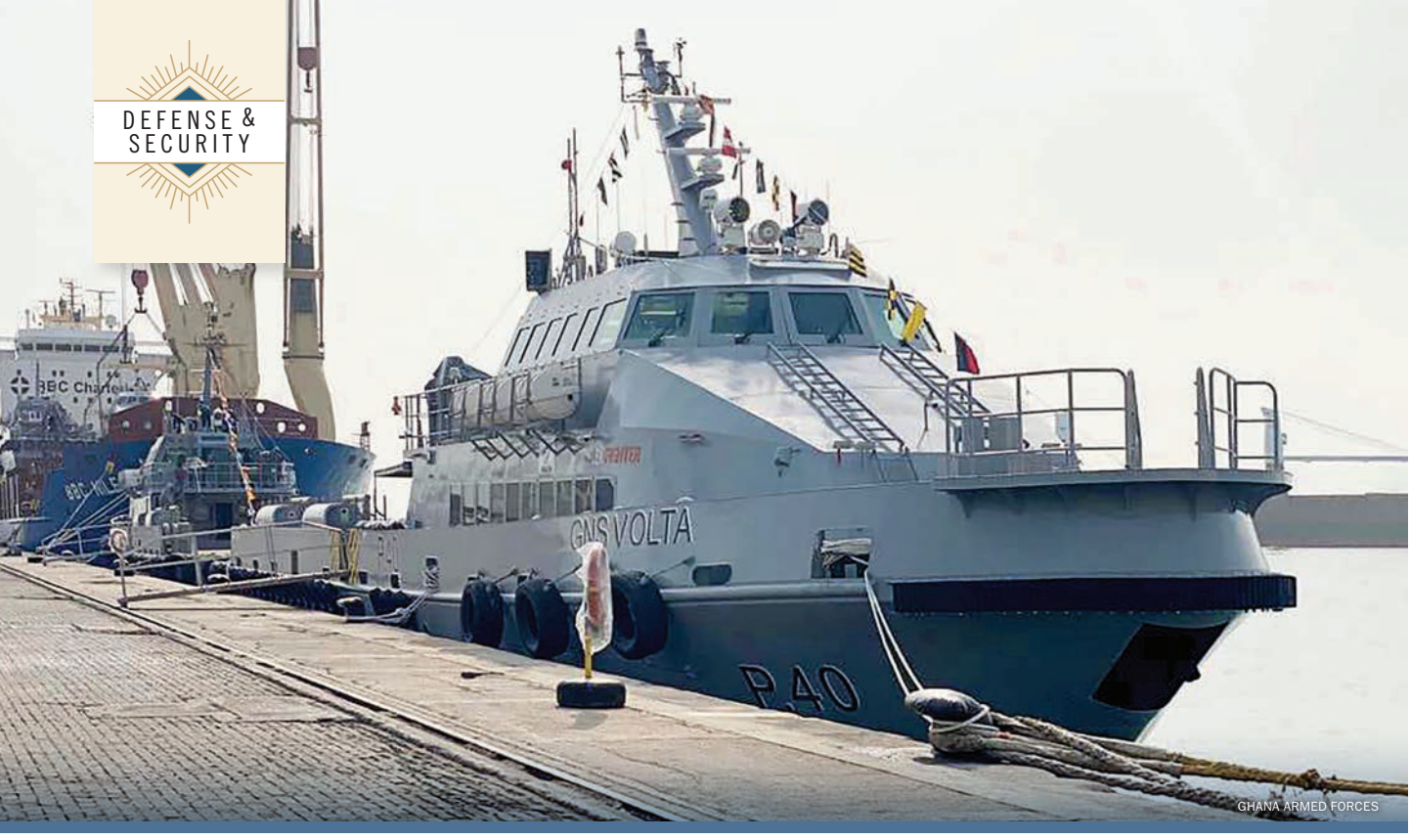
PAPSS was developed by Afreximbank and is a joint initiative that includes the African Union and AfCFTA. The idea for the project dates to 2016 when organizers studied payment systems and operators across Africa. The next year the West African Monetary Zone agreed to implement a pilot plan as a proof of concept.

Afreximbank is backing the system by providing settlement guarantees and overdraft facilities.

The program went live in August 2021 with transactions tested involving central banks of The Gambia, Ghana, Guinea, Liberia, Nigeria and Sierra Leone. It launched commercially in 2022. PAPSS has agreements with 12 commercial banks and four payment switches.

Aside from making payments across borders easier, the system also is making investments in security by formalizing previously informal payment systems and putting in place safeguards to make sure it is not used by criminals.

"The PAPSS will fill the real gap by adapting the necessary know-your-customer and anti-money laundering requirements to the African context," African Development Bank Vice President Solomon Quaynor told The Africa Report. "The infrastructure offered by the PAPSS will significantly boost intra-regional integration and intra-African trade."



GHANA ARMED FORCES

GHANA NAVY ADDS FOUR VESSELS TO SECURE OFFSHORE OIL INTERESTS

ADF STAFF


Commodore Samuel Walker, flag officer of Western Naval Command, speaks during a ceremony commemorating the addition of four new vessels to the Ghana Navy fleet. GHANA ARMED FORCES

The Ghana Navy added four new offshore security vessels to its fleet as it seeks to protect the people and industries operating in its exclusive economic zone.

Chief of Naval Staff Rear Adm. Issah Adam Yakubu received the Flex Fighter vessels during a ceremony at the Port of Takoradi on January 10, 2022. The 40-meter armored boats have space for more than 70 people and can carry 60 tons of cargo. The acquisition is part of a larger effort to protect offshore petroleum infrastructure from piracy.

"I can assure you that in the next few months, we are going to step up our surveillance and vigilance based on this capacity that we are building, and we are going to nip this canker [Gulf of Guinea crime] in the bud," Yakubu told My Joy Online.

In recent years, private security guards have proliferated in the region to protect offshore oil and gas work. The Ghanaian newspaper the Daily Graphic reported that, beginning in 2022, only Ghana Navy ships will be allowed to protect these installations. Tullow Oil and its partners operating at the Jubilee Oil field off the coast of Ghana have signed a five-year memorandum of understanding with the Ghana Navy to provide security for oil infrastructure and personnel.

During the event, Commodore Samuel Walker, flag officer of Western Naval Command, said the boats will go a long way to improve the Ghana Navy's ability to protect oil fields and provide revenue to the country, Ghana Peace Journal reported.

He congratulated the first Sailors chosen to staff the vessels and urged them to hold themselves to the highest levels of professionalism and to remain vigilant about vessel maintenance.

KENYA TO BUILD
COUNTER-IED CENTER

ADF STAFF

Kenya is building a counter-improvised explosive device (C-IED) center in Embakasi to fight extremist threats in the region.

The new facility at the Humanitarian Peace Support School is funded by Germany and the United Kingdom. Since 2016, the C-IED wing has trained more than 1,700 military and police personnel from Kenya and 21 other countries.

During a cornerstone-laying ceremony, experts from the Kenya Defence Forces (KDF) demonstrated how to safely detonate an IED using a remote-controlled robot. They also showed how a water bottle can be used as an explosive device.

A Kenya Defence Forces Soldier demonstrates techniques during an event to commemorate the construction of a new center to train security forces to detect and disarm improvised explosives.

KENYA DEFENCE FORCES

"IEDs are killers; they do not only kill Soldiers but also police officers and civilians," German Deputy Ambassador Thomas Wimmer said at the event. "That's the reason Germany is willing to fund the counter-IED wing. It really helps prevent people from being killed, crippled and injured."

IEDs are the most lethal weapons employed by the extremist group al-Shabaab. Between January 2017 and April 2020, IED blasts killed 153 African Union Mission in Somalia (AMISOM) troops and 489 Somali security forces. Kenya contributes troops to AMISOM.

"These devices pose the greatest threat to KDF and troops from other contributing countries who are fighting al-Shabaab as part of the African Union Mission in Somalia," Josephine Gauld, British deputy high commissioner to Kenya, said during the ceremony.

Gauld said the C-IED center is part of an expanding center of excellence in Embakasi, where the region's armed forces can learn skills needed to combat a multitude of threats.

"The Humanitarian Peace Support School is a unique initiative on the African continent, providing a solid foundation on which to build a competent, capable regional center of excellence where police and military personnel across East and Southern Africa receive IED disposal training that helps to promote security and stability in Somalia," she said.

The first phase of construction will cost about $2.6 million and will include 12 buildings.

CIVIL-MILITARY EVENT OFFERS FREE VETERINARY CARE

ADF STAFF

During three days in February 2022, herders from southwestern Niger brought cattle and other livestock to receive badly needed veterinary care at a free event.

During the event in Gaya, veterinarians treated more than 13,000 animals with vaccines and vitamins. Organizers also handed out solar-powered hand-held radios, which allow herders to track weather and security developments in the region.

The event was one of many organized by the Nigerien Armed Forces (FAN) Civil-Military Action (ACM) division, whose goal is to support vulnerable communities and build trust between the military and civilians.

The ACM unit at Air Base 101 in Niamey organized the veterinary event with support from U.S. Civil Affairs Soldiers stationed at the base. Similar events have been held around Air Base 201 in Agadez.

A Nigerien cattle herder displays a certificate of a "healthy herd" after a free veterinary event in Gaya organized by the Nigerien Armed Forces Civil-Military Action division. U.S. EMBASSY IN NIGER

"The different actions of defense and security forces and American partners are really appreciated by the local population," said Capt. Badagé Oumarou, commander of Air Base 201, after an event in 2021 in which Soldiers handed out rice, footballs and prayer mats. "The people of Teghazert showed their gratitude and urged us to expand and continue the effort."

During its first year, the Agadez ACM unit conducted 11 aid missions in the region, helping an estimated 4,200 residents with staple foods and sanitation supplies to protect them from COVID-19.

"Donations like this show the long-term value of the efforts led by the FAN/ACM, especially as the unit continues to expand its reach and serve more communities," said Sgt. Joseph Bovee, a U.S. Civil Affairs Soldier.

Malawi Rolls Out Mosquito Net Program

ADF STAFF

Malawi has begun a mass distribution of mosquito nets to reach as many of the country's 19 million people as possible.

Nets reduce the spread of malaria, which in Malawi accounts for 36% of all hospital outpatients and 15% of hospital admissions.

Khumbize Kandodo Chiponda, Malawi's minister of health, announced the Global Fund-supported campaign during the commemoration of Southern Africa Development Community Malaria Day. She told the Nyasa Times that the hope was that the 9 million nets in the program would each reach two people sharing a netted space or bed.

She also said that health workers will give antimalarial drugs to all expectant mothers to prevent them from suffering from the disease while pregnant.

Malaria is the most deadly disease in Malawi. In 2020, malaria killed 2,500 people there, more than any other disease, including COVID-19.

Chiponda said the campaign has major challenges.

"And one of the challenges is that when you distribute the nets, you will find that, especially along the lake, these nets are used for fishing and sorts of things," she told the Voice of America.

To reduce the chances of such misuse, the campaign also involves teaching recipients about the importance of sleeping under the nets.

"Africa spends about 12 billion dollars on Malaria annually," Chiponda told the Nyasa Times. "There are 400,000 Malaria induced deaths in the SADC [Southern African Development Community] region annually. So, as SADC member states, we are coming together to ensure that we fight Malaria head-on."

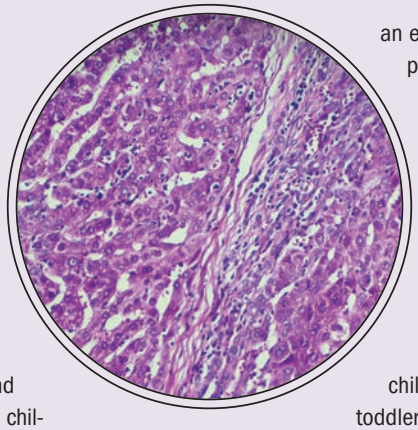
New Drug Test Offers Hope to Millions

REUTERS

An adjusted version of an established drug against schistosomiasis, a tropical parasitic worm disease, has been shown to work in preschool children, likely offering a cure for millions.

German chemical company Merck KGaA reported that in a late-stage trial in Côte d'Ivoire and Kenya, more than 90% of the participants, infected children ages 3 months to 6 years, had no more parasite eggs in their stool or urine after up to three weeks of treatment.

The company said it now will seek regulatory approval to produce and distribute the oral drug. Arpraziquantel is an experimental pediatric version of the standard drug praziquantel.



Schistosomiasis human pathology sample under a microscope

It also was shown to be safe and tolerated well, Merck said.

The Pediatric Praziquantel Consortium confirmed the positive results and said that schistosomiasis is one of the most damaging parasitic diseases in the world. The World Health Organization reported that 105.4 million people were treated for the disease in 2019.

Praziquantel is the standard treatment for schoolchildren and adults, leaving an estimated 50 million toddlers and preschoolers without a treatment option.

The disease, also known as bilharzia, is caused by parasitic flatworms. It spreads via freshwater snails in tropical and subtropical regions across the globe but mostly affects poor and rural communities in Sub-Saharan Africa.

Dawn of Humanity *Pushed Back 30,000 Years*

ADF STAFF

The age of the oldest fossils in eastern Africa widely recognized as representing the human species has long been uncertain. Now, the dating of a huge volcanic eruption in southwestern Ethiopia reveals that some of the fossils are much older than previously thought.

Scientists found the remains, known as Omo I, in Ethiopia in the late 1960s, SciTechDaily reported. They have been trying to date them precisely ever since by using the chemical fingerprints of volcanic ash layers found above and below the sediment in which the fossils were discovered.

Now, an international team of scientists, led by the University of Cambridge, has reassessed the age of the Omo I remains and humans — Homo sapiens — as a species. Earlier dating of the fossils put them at less than 200,000 years old, but the new research shows they have to be older than a colossal volcanic eruption 230,000 years ago. The results were reported in the journal Nature.

"The Omo Kibish Formation is an extensive sedimentary deposit which has been barely accessed and investigated in the past," said Professor Asfawossen Asrat of Addis Ababa University, as reported by the University of Cambridge. "Our closer look into the stratigraphy [the order and position of layers of archaeological remains] of the Omo Kibish Formation, particularly the ash layers, allowed us to push the age of the oldest Homo sapiens in the region to at least 230,000 years."

The region in Ethiopia has a long history of high volcanic activity and is a source of early human remains and artifacts such as stone tools.

"Omo I possesses unequivocal modern human characteristics, such as a tall and globular cranial vault and a chin," Dr. Aurélien Mounier of the Musée de l'Homme in Paris reported in the study. "The new date estimate, de facto, makes it the oldest unchallenged Homo sapiens in Africa."

Scientists have updated their research on human fossils found in the Omo Kibish formation in southwestern Ethiopia.

PHOTO BY JOHN FLEAGLE/NATIONAL SCIENCE FOUNDATION

Somalia Opens Center To Monitor Locusts

ADF STAFF

Since late 2019, the Greater Horn of Africa region has been dealing with the worst desert locust invasion in decades. Now, Somalia has opened a locust detection center to help deal with the crisis.

The locusts have destroyed tens of thousands of hectares of cropland and pasture. In Somalia, where the majority of people depend on agriculture and livestock for their livelihoods, recurrent drought and floods have significantly eroded household food security. The desert locust crisis has only made life harder.

Somalia, along with the Food and Agriculture Organization of the United Nations, opened the National Desert Locust Monitoring and Control Centre, based in Qardho in the northeast part of the nation.

AFP/GETTY IMAGES

Somali Minister for Agriculture and Irrigation Said Hussein Iid said the government has made control of the desert locust and other invasive species a priority and is enacting laws to protect the country from such invasions, Hiiraan News of Somalia reported. The monitoring center will be a major source of information on locust invasions throughout the region.

The U.N. says that Somalia has made major gains in suppressing one of the largest desert locust surges in recent history.

Desert locusts can cause major damage to crops because the insects are hardy, highly mobile and feed on large quantities of any kind of vegetation, including crops, pastureland and cattle fodder.

A typical swarm can be made up of hundreds of millions of locusts per square kilometer. They fly along with the winds, traveling up to 150 kilometers in a day. They are easily capable of eating vegetation equal to their body weight daily.

Benin Named Fastest Place to Start Business

ADF STAFF

In the past, Benin was perhaps best known for its cotton exports and its bright clothing designs. But it is now known for its streamlined paperwork, allowing new businesses to establish faster than in any other African country.

By providing a full online service, the government has helped entrepreneurs create businesses and jobs during the COVID-19 pandemic. One-third of Benin's new entrepreneurs are women, according to the United Nations.

A U.N. report described how Sandra Idossou, a Beninese entrepreneur, opened a handicrafts shop in the country's commercial capital, Cotonou. With COVID-19 restrictions in place and enforced by authorities, she used her smartphone to log into Benin's new business registration website. Within 10 minutes, she had entered her information, photographed and uploaded her identity documents, and paid by credit card.

Two hours later, an email arrived with her certificates of incorporation, and her business was officially created.

Her shop, Kouleurs d'Afrik, now sells handcrafted goods made from discarded items found around town. "Had it not been for this facility to create a business online, if one had to go stand in line, wait in line, go through the maze of administration to start a business, I wouldn't have done it," Idossou told Voice of America. "It's as simple as that. I would have stayed in the informal sector."

A U.N. digital government platform called eRegistrations now places Benin jointly with Estonia as the fastest country in the world in which to start a company. The average startup time in the European Union is three days, while in New York it is seven days.

The eRegistrations program operates in other developing countries, including Lesotho and Mali. The platform makes official procedures accessible and transparent, particularly for small businesses. Paper-based administrative procedures are characterized around the world by long lines outside government offices with hours of bureaucracy. Such procedures also can include trips to different government bureaus involving near-identical forms.

Africa's Taxis Going Green

REUTERS

In late 2021, Nopea Ride, Kenya's electric taxi fleet service, opened an electric vehicle (EV) charging hub at Village Market in the capital, Nairobi, demonstrating the growing demand for electric mobility in East Africa.

The Finnish electric cab company earlier had announced that it planned to triple its fleet in Nairobi, helping reduce emissions from the city's notorious traffic. EkoRent, the parent company of Nopea, now has about 1,500 EVs in its fleet.

Estonian on-demand transport company Bolt announced in October 2021 that it will roll out electric cabs in South Africa. It came four months after the company introduced e-bike food delivery services there.

"We are looking to roll out a green taxi category in South Africa in the next few months, and plan to roll out green categories in other African markets," said Paddy Partridge, Bolt's regional director for Africa and the Middle East.

EVs make business sense in Africa, and especially in Kenya where fuel prices fluctuate without warning. Taxi drivers and owners of electric or hybrid vehicles enjoy better profit margins and longer mileage between maintenance.

In May 2020, Vaya Africa, a ride-hail mobility venture founded by Zimbabwean mogul Strive Masiyiwa, unveiled an electric cab service and charging network in Zimbabwe, with plans to expand across the continent.

NOPEA RIDE

USED TIRES ARE BLACK GOLD

REUTERS

In Nigeria, a country heavily reliant on revenues from its oil exports, entrepreneur Ifedolapo Runsewe has identified another type of black gold: used car tires.

A man arranges rubber interlocking tiles manufactured from recycled car tires at the Freetown Waste Management Recycle factory in Ibadan, Nigeria.

REUTERS

She has set up Freetown Waste Management Recycle, an industrial plant dedicated to transforming old tires into paving bricks, floor tiles and other goods that are in high demand.

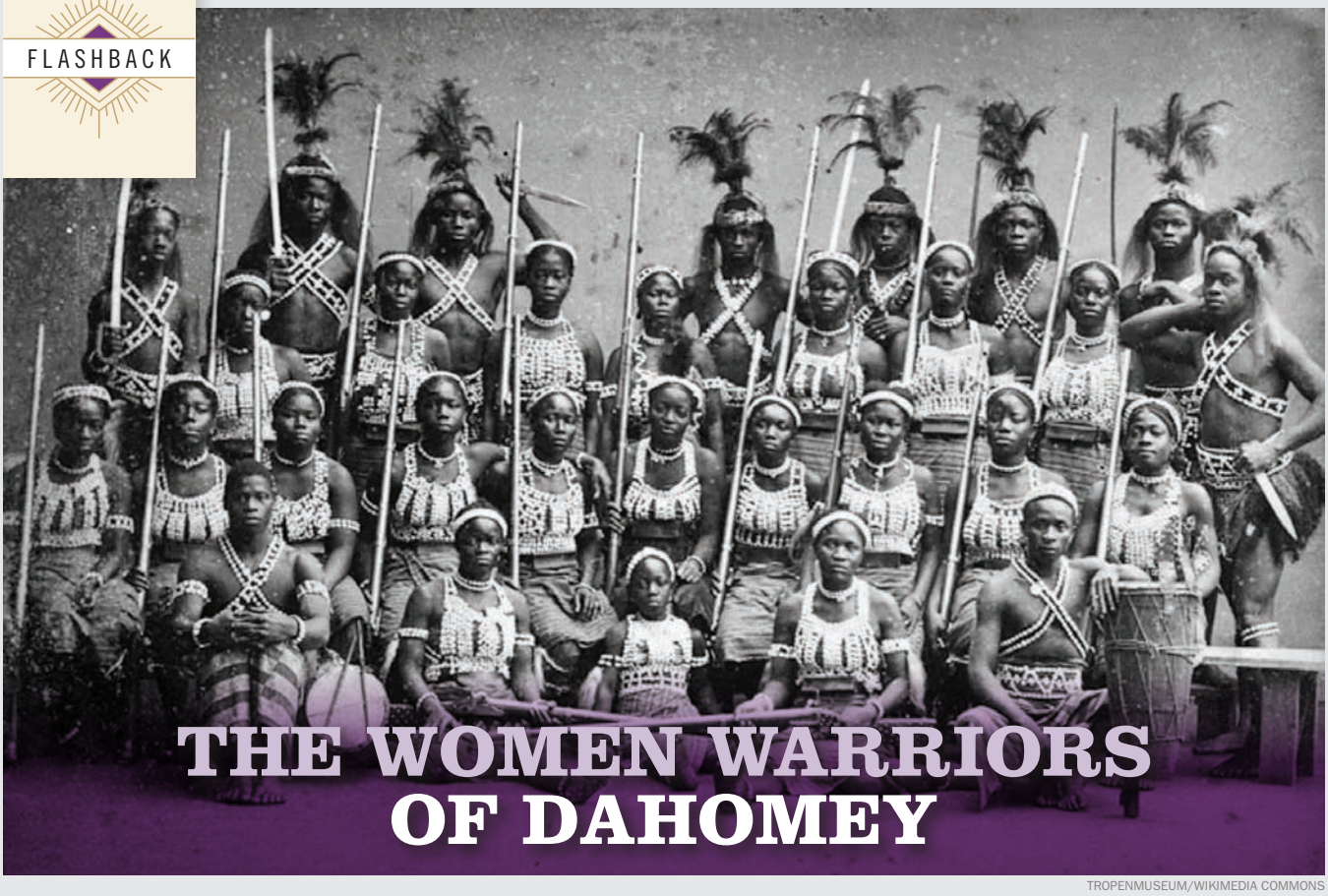
"Creating something new from something that will otherwise be lying somewhere as waste was part of the motivation," Runsewe said at her factory in Ibadan. "We are able to create an entire value chain around the tires," she said, holding a paving brick that is one of the company's best-selling products.

Waste management in Nigeria is patchy at best. In villages, towns and cities, piles of waste are a common sight, and residents often burn trash at night for lack of a safer disposal method. Tires routinely are dumped and abandoned.

Freetown relies on scavengers who collect old tires from dumping grounds. They are paid 70 to 100 naira (17 cents to 24 cents) per tire. Some tires also are supplied directly by mechanics, such as Akeem Rasaq, who is delighted to have found a place where he can make some money from old tires.

"Most of the tires end up in public drainage clogging up the drain, but things have changed," he said at his roadside workshop.

Freetown started operations in 2020 with just four employees. Growth has been so rapid that the workforce has jumped to 128. So far, more than 100,000 tires have been recycled into material such as speed bumps and soft paving for playgrounds.



THE WOMEN WARRIORS OF DAHOMEY

TROPENMUSEUM/WIKIMEDIA COMMONS

ADF STAFF

In 1861, 3,000 heavily armed female Soldiers charged a thorny wall during a skills demonstration.

King Glele, their ruler in Dahomey, a region that is now part of Benin, was eager to show off the ferocity and skill of his warriors. The 400-meter-long wall bristled with acacia branches with 5-centimeter-long, needle-sharp thorns.

The women were barefoot, armed with clubs and knives. Some of them — "Reapers" — had 1-meter-long razors that, the king said, could be used to cut a man in half.

The warriors charged the wall, ignoring the savage wounds caused by the thorns. They clawed their way to the top, simulating hand-to-hand combat with an invisible enemy. They fell back and climbed the wall a second time, this time rescuing a band of villagers acting as prisoners.

The demonstration proved to the visitors that the women were not merely ceremonial figures. They were, in fact, the only female Soldiers in the world at that time who served in combat.

The women warriors of Dahomey probably originated in the 17th century. One theory states that they began as hunters in the Fon tribe. However, Stanley Alpern, the leading expert on the warriors, wrote in his 1998 book, "Amazons of Black Sparta," that they likely began as palace guards in the 1720s. They came to be known as "Mino," which means "Our Mothers" in the Fon language.

The Dahomey women fought in major battles. Alpern said that in four major campaigns in the late 19th century, at least 6,000, and as many as 15,000, died in battle.

There are several theories as to how the Dahomey warriors came to be, but most believe it was a matter of necessity — the Fon men, as a result of wars and the slave trade, were outnumbered 10 to 1 by their rivals in the Yoruba tribe. As a result, Fon women were recruited to fight.

There were only about 600 Dahomean female warriors until the mid-19th century, when King Ghezo increased their numbers to about 6,000. He was likely able to recruit many women to live as warriors because Dahomey women of that time lived in poverty and often were treated poorly.

As warriors, the women lived in the king's compound. Explorer Sir Richard Burton reported that the women were supplied with food, tobacco, alcohol and slaves.

The warriors were exhaustively trained to fight, to endure great pain and to survive. Observers said that although they were not good with firearms, they were experts in hand-to-hand combat and the use of knives.

Until the beginning of the 20th century, the women were in a state of constant war at the behest of their ambitious kings. But when the French invaded with modern weapons, the women were defeated and their ranks disbanded.

Their bravery is summed up in a credo the women reportedly repeated to show their spirit: "Those coming back from war without having conquered must die. If we beat a retreat our life is at the king's mercy. Whatever town is to be attacked we must overcome it, or we bury ourselves in its ruins."

WHERE AM I?

CLUES

1. Humans have fished and hunted in the area for 2,000 years, creating shellfish mounds, some of which are several hundred meters long.
2. Some of the mounds contain burial sites.
3. This area was formed within the delta of three rivers.
4. It includes 200 islands and islets, mangrove forests, and a mix of salt water and fresh water.

ANSWER Saloum Delta, Senegal

SHARE YOUR KNOWLEDGE

Want to be published?

Africa Defense Forum (ADF) is a professional military magazine that serves as an international forum for military and security specialists in Africa.

The magazine is published quarterly by U.S. Africa Command and covers topics such as counterterrorism strategies, security and defense operations, transnational crime, and issues affecting peace, stability, good governance and prosperity.

The forum allows for an in-depth discussion and exchange of ideas. We want to hear from people in our African partner nations who understand the interests and challenges on the continent. Submit an article for publication in ADF, and let your voice be heard.

AUTHOR GUIDELINES FOR ADF SUBMISSION

EDITORIAL REQUIREMENTS

- Articles of approximately 1,500 words are preferred.
- Articles may be edited for style and space, but ADF will collaborate with the author on final changes.
- Include a short biography of yourself with contact information.
- If possible, include a high-resolution photograph of yourself and images related to your article with captions and photo credit information.

RIGHTS Authors retain all rights to their original material. However, we reserve the right to edit articles so they conform to AP standards and space. Article submission does not guarantee publication. By contributing to ADF, you agree to these terms.

SUBMISSIONS

Send all story ideas, content and queries to ADF Editorial Staff at **ADF.EDITOR@ADF-Magazine.com**. Or mail to one of the following addresses:

Headquarters, U.S. Africa Command
ATTN: J3/Africa Defense Forum Staff
Unit 29951
APO AE 09751 USA

Headquarters, U.S. Africa Command
ATTN: J3/Africa Defense Forum Staff
Kelley Kaserne
Geb 3315, Zimmer 53
Plieninger Strasse 289
70567 Stuttgart, Germany

adf
AFRICA DEFENSE FORUM

Can't wait until the next edition?

At ADF-Magazine.com we bring you in-depth coverage of current issues affecting peace and stability every week. Check out our website for the same credible and accurate security news, reported weekly, from around the continent.

STAY CONNECTED

If you would like to stay connected on social media, follow ADF on Facebook, Twitter and Instagram, or you can join our email list by signing up on our website, **ADF-Magazine.com**, or email **News@ADF-Magazine.com**.