

# adf

AFRICA DEFENSE FORUM



## A WEB OF THREATS, A WORLD OF POTENTIAL

As Africa Closes the Digital Divide,  
It Must Improve Cyber Security

VISIT US ONLINE: [ADF-MAGAZINE.COM](http://ADF-MAGAZINE.COM)



# features

**8 A Web of Threats, a World of Potential**  
As Africa closes the digital divide,  
it must improve cyber security.

**16 Who Defends the Web?**  
Militaries are launching cyber commands,  
but their role is still being debated.

**22 Development Through Digitalization**  
Ghana's cyber security advisor says the  
country is preparing for the opportunities  
and threats of a digital world.

**28 Threats Abound as Continent Connects**  
With Africa's internet growth comes  
more risks and more opportunity.

**34 Africa Takes on Cyber Crime**  
As the continent improves its  
communications infrastructure,  
it becomes a bigger target for  
cyber criminals.

**40 Competitors and Comrades**  
OSMA shows that athletic competition  
among Soldiers can have a broad impact.

**44 Training for the New Battlefield**  
Simple, low-cost measures can put  
militaries on the road to cyber security.

**50 Countering the Message**  
Stopping online propaganda by  
extremists takes more than just  
shutting down the messenger.

# departments

4 Viewpoint

5 African Perspective

6 Africa Today

26 African Heartbeat

56 Culture & Sports

58 World Outlook

60 Defense & Security

62 Paths of Hope

64 Growth & Progress

66 Flashback

67 Where Am I?



***Africa Defense Forum  
is available online.***

Please visit us at:  
[adf-magazine.com](http://adf-magazine.com)

50



**ON THE COVER:**

This illustration represents the digital connections across the globe and highlights the need for improved cyber security to defend Africa's economic growth.

ADF ILLUSTRATION





There was a time when a military commander could comfortably say, “I’m not a computer person” or “I don’t really use the internet.”

That attitude is no longer an option.

Being a security professional today means keeping up with threats that lurk in cyberspace. Foreign adversaries can attack weapon systems, put troops’ lives in danger and create chaos on networks that support railways, water distribution and electricity.

Being knowledgeable about cyber issues is not only about threats. It means being comfortable using computers to access information and communicate. Technology doesn’t just support the modern defense mission; it is central to it.

Security professionals everywhere are trying to do a better job. It starts with training in national universities, staff colleges and continues with midcareer training. Militaries need to make cyber security a dedicated specialty and ensure that all Soldiers have a minimum level of computer competency.

It also is time to examine the military’s role in guarding against cyber attacks. Countries such as South Africa and Nigeria are launching cyber commands, and other nations are nurturing cyber specialties within existing command structures. This should coincide with a national dialogue about the role the military can and should play in cyber security.

Finally, security professionals must practice cyber awareness. Threats are evolving, and cyber hygiene best practices must evolve as well. Anyone who doesn’t know how to spot phishing attacks and avoid malware or ransomware puts an entire network at risk. Multilevel security protocols and identifying insider threats are equally important.

Internet access is growing faster in Africa than anywhere else in the world. The continent and its economies now rely on high-speed internet. Security professionals must be ready to do their part to ensure that cyberspace stays safe.

U.S. Africa Command Staff



Soldiers test communications equipment during Africa Endeavor, an annual military communications exercise hosted by U.S. Africa Command. U.S. AFRICA COMMAND



## Cyber Security

Volume 12, 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.



# Safeguarding Africa's Cyberspace



**Cheikh Bedda, director of the African Union Commission's Department of Infrastructure and Energy,** addressed the workshop for AU member states on cyber strategies, cyber legislation and setting up CERTs (computer emergency response teams) on July 23, 2018, in Addis Ababa, Ethiopia. His remarks have been edited to fit this format.



Africa, like the rest of the world, is embracing its digital future. African leaders are committed to boosting the digital economy and the digitalization of strategic sectors such as education, health, entrepreneurship, employment, peace and security, and good governance by facilitating the delivery of public services and creating more interactions between governments and citizens.

On the continent there are many successful digital experiences that need to be replicated in other countries to promote economic growth and social development.

However, the more digitalized and connected our economy, the more important it becomes to secure our systems in cyberspace.

African countries today face a full spectrum of cyber threats, cyber crime, attacks, espionage and other malicious activities. Most of the time they don't have the means to monitor and control their networks, which exposes them to risks that may affect their national security and economy.

As African countries increase access to broadband connectivity, they are becoming more interconnected and vulnerable to cyber attacks. It becomes critical to reinforce our human and institutional capacity to secure our cyberspace by building trust and confidence in the use of cyber technologies by African states and citizens.

According to the report "Cybersecurity and Cybercrime Trends in Africa" that we published in collaboration with Symantec in 2016, many African countries have yet to adopt policy instruments and legislative frameworks to fight malicious use of information and communications technology (ICT). Only eight countries have national cyber security strategies, and only 13 African countries have established their national computer emergency response teams.

The security and stability of our common African cyberspace relies on the local and national ability of all countries to cooperate to prevent and react to cyber incidents and investigate and prosecute cyber crime and cyber terrorism.

From the African Union Commission's (AUC) perspective, a resilient and safe cyberspace depends on the successful implementation and execution of a holistic cyber security strategy, including the development of a vibrant ecosystem with strong legislative frameworks and technical know-how that gives oversight for securing networks and protecting critical infrastructure.



Participants from Gabon, left, and the Republic of the Congo take part in a cyber security exercise at Africa Endeavor 2018 in Cape Verde.

U.S. AFRICA COMMAND

To address the challenges posed by crime committed with the use of ICT, the AU 23rd Assembly of Heads of State and Government adopted in 2014 the Convention on Cyber Security and Personal Data Protection. Known also as the Malabo Convention, it focuses on essential security rules for establishing a credible digital environment and enabling the development of a modern information society in Africa.

However, four years after its adoption, only three countries — Guinea, Mauritius and Senegal — have provided the AUC with ratification instruments. Its entry into force requires 15 ratifications.

We must safeguard our common African cyberspace as a shared asset and also as a shared responsibility to ensure its security and accessibility to all of our citizens.

We believe strong cyber security is a key building block of Africa's digital transformation, so it is important to build up our capabilities by developing cyber policies and legislation and raising awareness at all levels of the benefits and threats related to the use of digital services.



# UGANDA'S GRASSHOPPER DELICACY ON THE DECLINE

AFP/GETTY IMAGES

BBC NEWS AT [BBC.CO.UK/NEWS](http://BBC.CO.UK/NEWS)

In Uganda's grasshopper season, the insects are seen as a nutritious delicacy — either boiled or deep-fried. They are so popular that some people are worried about declining harvests.

"When the season starts, we watch the cycle of the moon and prepare. [They tend to come out at full moon]. We also keep hoping for rain," said Quraish Katongole, one of Uganda's most experienced grasshopper trappers. "The larger numbers appear when it has rained."

His workers set up barrels at a trapping site near Masaka town. As it grows darker, the slim-bodied insects swarm around the lights. The trappers burn fresh grass, and the rising smoke makes the insects dizzy. The grasshoppers smash against iron sheets and fall into the drums.

During rush hour in the capital, Kampala, young people weave through traffic selling boiled or deep-fried ready-to-eat grasshoppers to commuters. A tablespoonful costs 1,000 Ugandan shillings (27 cents).

Ugandans are among more than 2 billion people worldwide who eat different species of insects.

A 2013 United Nations Food and Agriculture Organization report urged others to consider adding them to their diet, saying that this could boost nutrition and food supplies.

But in Uganda, the number of grasshoppers could be falling as feeding and breeding habitats around Lake Victoria shrink.

Evidence from the night's work supports that. The young men empty the drums and manage to fill just two sacks. "There was a time when I would catch 20 to 25 sacks a night," Katongole said.

Ugandan scientists are trying to understand more about the grasshopper life cycle to see if they can be harvested in a more sustainable way. Professor Phillip Nyeko said that, apart from loss of habitat, aggressive harvesting presents another threat.

"They do not swarm to be eaten; they swarm to feed and breed. But when you put up lights and collect them in the thousands, you're upsetting their life cycle," Nyeko said.

Street vendors sell small portions of fried grasshoppers in Kampala, Uganda.



## Africa Eyes MOBILE GAMING BOOM

AGENCE FRANCE-PRESSE

An army of humans laid waste to an alien colony as South African video game maker Simon Spreckley enthusiastically controlled the action using his phone's touch screen.

"The penetration of mobile devices in Africa is huge. People often have two or three phones, which is pretty crazy," said Spreckley, 40. "So that's one of the big pluses and why we are trying to do this," he said, promoting *Invasion Day*, which will likely launch on Apple's App Store and Google's Play platform in 2019.

Many other African developers also are opting to tailor games for mobile devices instead of traditional consoles or desktop computers.

"There's enormous potential in Africa because the continent is primarily mobile," said Sidick Bakayoko, 34, founder of Paradise Game, an umbrella group for developers in Côte d'Ivoire. He joined African game coders, developers and artists with top executives from Sony and other industry giants at the Africa Games Week convention in Cape Town.

Bakayoko said the increasing number of African gaming products for hand-held devices mirrored the explosion of mobile banking and financial tools such as Kenya's Mpesa.

Spreckley hopes *Invasion Day* will catch the eye of a major investor, but many African mobile game developers have struggled to turn creations into cash. Google's decision in June 2018 to let African game developers make money from creations sold on its Play Store could revolutionize the sector.

"Most people use [Google] Android here," said Sithe Ncube, 24, founder of Zambia's Ubongo Game Lab. "People haven't had a way to monetize their mobile games. People have actually been developing apps for a while, but there hasn't been a way to use it as a business model."

A delegate plays an unreleased brawler game called *Shattered Realms* at Africa Games Week in November 2018 in Cape Town, South Africa. AFP/GETTY IMAGES



## BANANAS

### HELP PEEL AWAY ANGOLA'S OIL DEPENDENCY

AGENCE FRANCE-PRESSE



A worker cleans, sorts, and packs bananas at a farm near Caxito, Angola. AFP/GETTY IMAGES

**B**oxes of green bananas are shifted one by one from a stack of crates into a refrigerated shipping container in Caxito, Angola.

Stamped "From Angola, with Love," the fruit is shipped to consumers 6,000 kilometers away and is part of Luanda's drive to diversify its economy and wean itself from oil dependence.

Novagrolider, a private company, produces several dozen metric tons of bananas weekly for shipment to Portugal.

"We have two grades: domestic and export," said supervisor Edwin Andres Luis Campos. "Domestic will be sold here in Angolan supermarkets in about four or five days. Export will be shipped to Europe in refrigerated containers that will arrive in Europe in between 20 and 25 days."

Novagrolider's output has grown exponentially in recent years, and its parent company, Grupolider, which also has interests in transport and property, employs 3,500 people.

It grows mangoes, pineapples, watermelons and bananas on its four Angolan fruit farms.

After a cautious start, company boss Joao Macedo's ambition grew rapidly. Macedo hopes to double production to 170,000 metric tons annually and establish a foothold in South Africa.

Back in Caxito, the province's top agriculture official shares Macedo's enthusiasm.

"We're financially encouraging small-scale farmers to increase the size of the areas they cultivate," said Eliseo Mateos. "Until now they've mostly used their production for subsistence, but now we want them to grow more so they can sell their crops at market. Bananas are our 'green fuel' — here we have one possible way of diversifying the economy."

In the decade after the bloody 27-year civil war that ended in 2002, Angola enjoyed strong double-digit growth fueled by oil, which accounts for 90 percent of Angola's exports and 70 percent of government revenues.

Slumping crude prices in 2014 shook the nation's economic model, locking it into contraction. By producing more at home, the country would need to use less foreign currency to import food.

"With government support and organization, the agricultural sector could be the driving force of this country's development," Macedo said.



# A Web of **THREATS,**

---

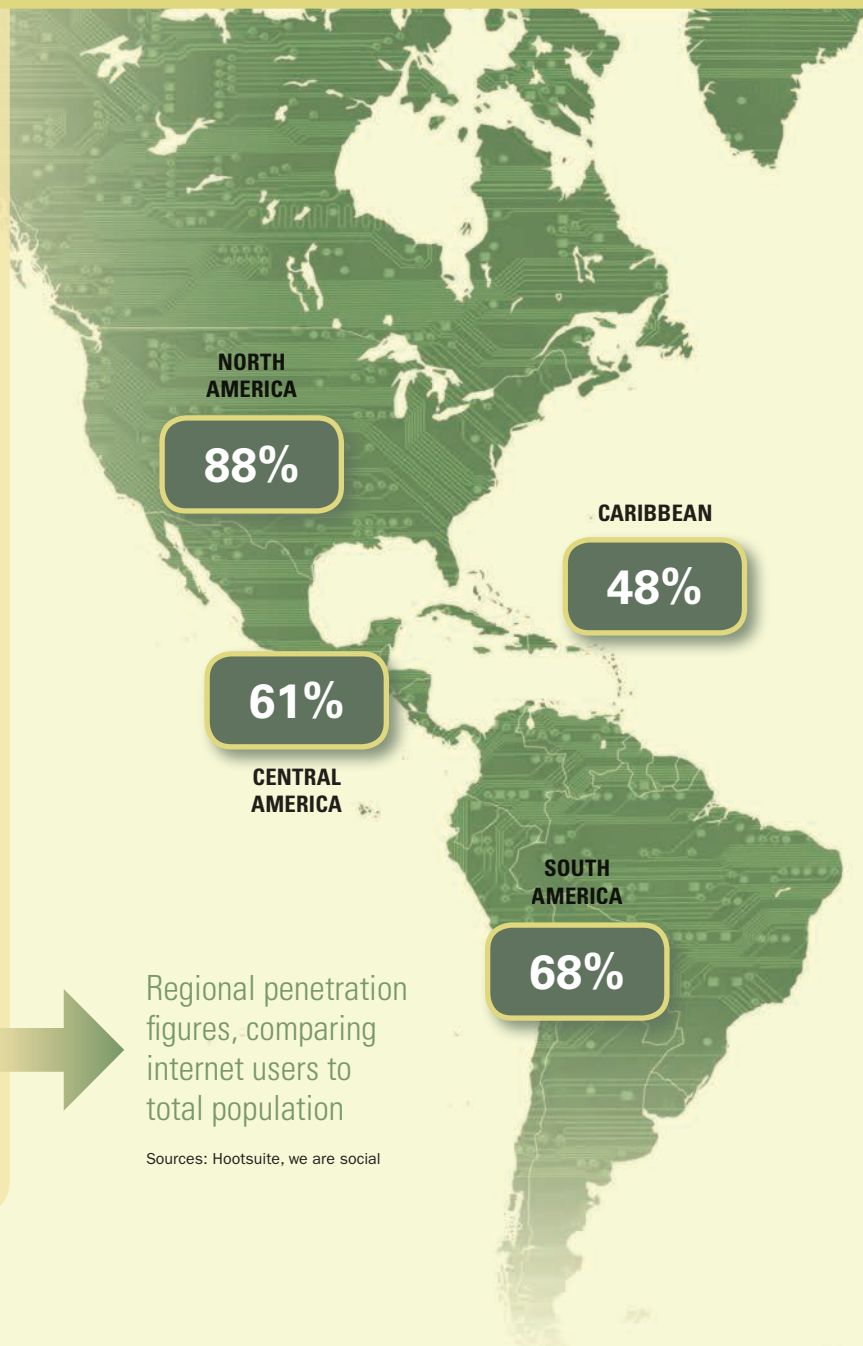
# A World of **POTENTIAL**

## As Africa Closes the Digital Divide, It Must Improve Cyber Security

ADF STAFF

### Internet Penetration

Internet penetration in Africa lags behind much of the world, but the continent is catching up fast. Nations are investing heavily in fiber optic cables and other means to bring the internet to people of all income levels. **Between 2017 and 2018, Africa achieved 20 percent growth in internet access**, the fastest growth rate in the world. In Benin, Mozambique, Niger and Sierra Leone, the number of internet users more than doubled during that time. **Today, 52 African countries are connected to submarine internet cables or a fiber optic network, and 44 percent of people live within 25 kilometers of a fiber node** that provides high-speed internet. Although this growth opens many avenues for economic development and improved governance, it comes with risks.



Regional penetration figures, comparing internet users to total population

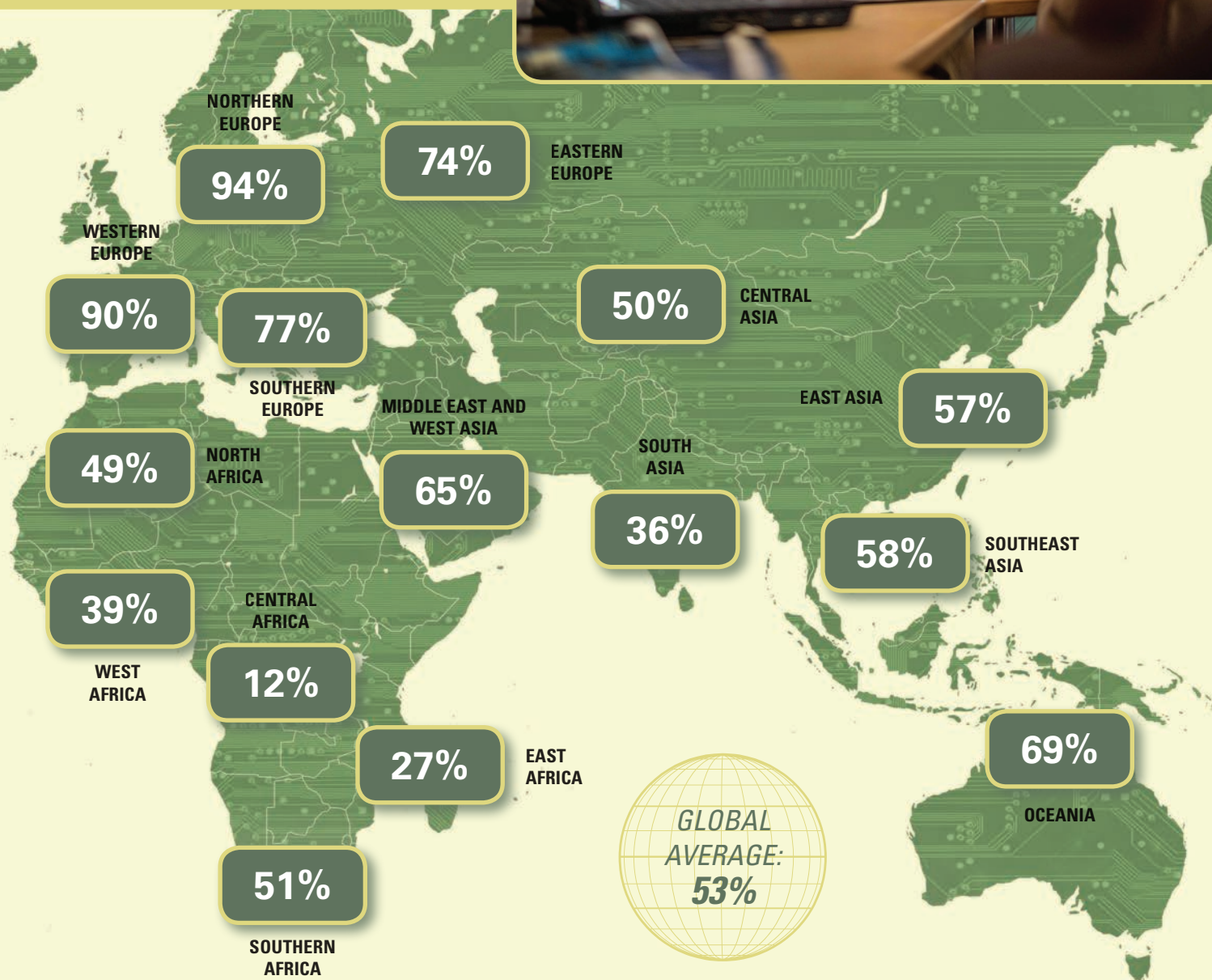
Sources: Hootsuite, we are social





Children in rural Benin receive computer training.

AFP/GETTY IMAGES



ADFILLUSTRATION

# CYBER ATTACKS

## By the Numbers

Cyber attacks have financial consequences. The WannaCry attack paralyzed banks, hospitals and government agencies in multiple countries, including **Kenya**, where financial institutions were affected. In **Morocco**, a Renault automobile plant closed for a day, halting the assembly line.

**Continentwide**, the cost of cyber attacks to economies is **\$3.5 billion** annually. These crimes range in severity from the theft of a credit card number that results in unauthorized charges, to the theft of national security secrets that imperils the safety of millions.

In **South Africa**, one of the continent's most connected countries, **67%** of adults reported experiencing cyber crime.

Average loss per year for each cyber crime victim: **\$274**

Source: Symantec



### Morocco

A cyber attack halted production at an automobile factory



### Nigeria

**\$649 million** lost per year



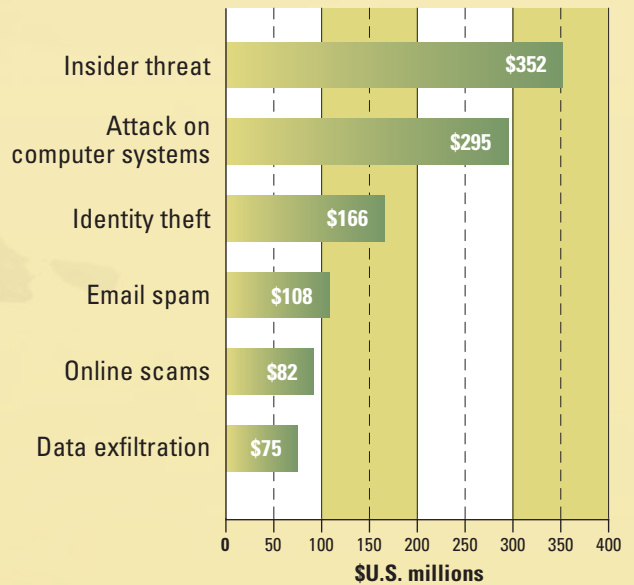
### Ghana

**\$54 million** lost per year



# The Most Common Types of Attacks in Africa and Their Cost

## Cost 2017



## Definitions



### INSIDER THREAT

An employee or someone with privileged access misuses data



### ATTACK ON COMPUTER SYSTEMS

An external attack designed to harm functionality



### IDENTITY THEFT

A hacker steals personally identifying data



### EMAIL SPAM

Messages designed to trick the user into handing over information or clicking on a malicious link



### ONLINE SCAMS

Fake stories designed to trick users into entering into a business or personal relationship



### DATA EXFILTRATION

The unauthorized removal of data

Source: Serianu



**Uganda**  
\$67 million  
lost per year



**South Africa**  
Two-thirds of adults reported  
experiencing cyber crime



**Tanzania**  
\$99 million  
lost per year



**Kenya**  
\$210 million  
lost per year

ADF ILLUSTRATION

## Methods of Attack

Criminals are constantly adapting, seeking to exploit new weaknesses and abandoning old methods once a defense is developed. Although cyber attacks take thousands of shapes, most fall into several general categories.



### Ransomware

These attacks take control of a computer or network. Typically, the computer hijackers demand a ransom payment to release and/or decrypt the data they have seized. These attacks sometimes gain access to a computer when the user clicks on a link, but in other cases they are able to infiltrate a network and travel between computers automatically. These attacks are becoming more common. According to Help Net Security, there were 181 million ransomware attacks in the first six months of 2018, nearly double the amount during the same period the previous year.

#### HOW TO AVOID

Use anti-virus software and a firewall when possible. Use a virtual private network (VPN) when accessing the internet on a public Wi-Fi connection. Back up all files regularly so they can be recovered in the event of an attack. Finally, if hit by ransomware, do not pay the ransom. It only encourages future attacks, and it offers no guarantee of data recovery.



### Phishing Scams

This typically involves an email asking the user to click on a link. The link might lead to a site that mimics a financial institution or email provider. The user may be led to a page that asks for a username and password with a claim that it needs to be reset. The actual intention is to capture the user's password so the attacker can access the target's information.

#### HOW TO AVOID

Do not click on links or open attachments from unknown or untrusted sources. Look for suspicious language in emails, such as misspellings, and look for unusual email addresses. Install an anti-phishing toolbar on your browser. Most internet browsers offer toolbars that scan sites before the user visits them to determine whether they are phishing sites. Use a firewall, anti-virus software and be suspicious of all pop-up advertisements. Never give personally sensitive or financial information to unknown and untrusted sources. Respectable institutions do not email clients asking for their password or personal information. Be suspicious.





## Malware

These are intrusive software programs that infiltrate a computer system, often without the user's knowledge. They can damage the system or steal information. Malware and related programs include viruses, worms, trojans, spyware and ransomware.

### HOW TO AVOID

Use firewalls, anti-virus software, and do not visit or download content from untrusted sites.



## Watering Hole Attack

In this type of attack, the hackers observe or guess a site that an individual, group or members of an organization are likely to visit. The attackers infect that site with malware or other harmful viruses. Once targets visit the site, they become infected, allowing the malware, in some cases, to spread to other members of the organization. Respected websites are not immune to these attacks. In 2013, sites associated with Twitter, Facebook and Apple were compromised.

### HOW TO AVOID:

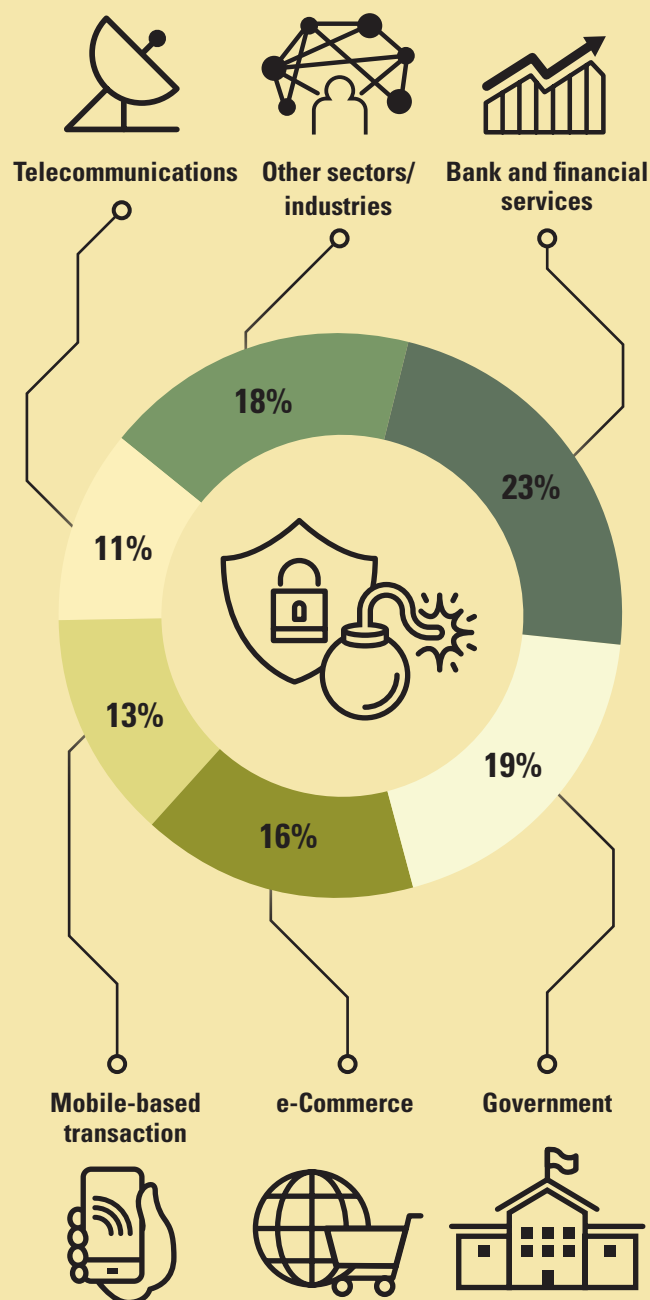
Hiding online movement using a VPN prevents outside actors from tracking certain browsing activities. Additionally, updating software to patch bugs and monitoring suspicious activity on a network help prevent intrusion.



## Popular Targets

Critical infrastructure, industry, banks and weapon systems are connected digitally in many countries. This increases the speed of business, but it leaves organizations vulnerable to cyber attacks. In 2017, an attack known as WannaCry moved across computer systems globally. The attack spread malicious code, crippling some systems and forcing others to shut down for fear of being hit.

Below are the sectors in Africa most targeted by cyber criminals:



ADFILLUSTRATION

Source: Serianu

# How Cyber Attacks Affect National Security

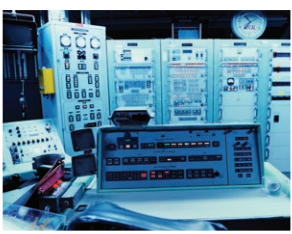
Cyber attacks are becoming the tactic of choice by those who like to strike from a distance and at a relatively low cost. Groups such as hostile foreign governments, activists, terrorists and criminals now use these tactics. “The threat of cyber attacks has gained a foothold in Africa, yet

governments and the private sector are yet to invest in adequate defenses to curb their spread,” said William Makatiani, CEO of the Kenyan cyber security company Serianu. “Securing data should therefore be a priority for public and private institutions in the light of rapidly evolving threats.”



## Critical Infrastructure:

Electrical grids, water and sewer systems, subways, dams and even nuclear power plants have been the target of cyber attacks. In many parts of the world, these are operated by outdated systems and are particularly vulnerable to hackers. One example is the December 2015 attack on the power network in Ukraine. Attackers reportedly used a phishing email to gain access to the power grid and cause a power failure affecting 230,000 people.



## Weapon Systems:

Modern weapon systems have essential embedded software and information technology. This could include targeting systems used to fire missiles, flight software and weapons-launching mechanisms. Although this connectivity allows for advances in fighting wars, it also leaves these systems open to intrusion and disruption by adversaries.



## Financial Institutions:

Banks are the most common targets of cyber attacks. In some attacks, criminals use malware or other methods to gain access to stored information such as credit card numbers, login credentials and government-issued ID numbers. Other attacks aim to deny service and cause system failures. Overwhelming a server with simultaneous requests can paralyze it. In 2017 in Kenya, customers of M-Shwari, a mobile banking service, were locked out of accounts for five days. Once access was restored, some reported missing money.



## Government Agencies:

Government offices are an attractive target for cyber criminals. Some attackers use ransomware to take over governmental websites; others seek to steal confidential or classified information held by the government. Sometimes the aim is to make a political statement. A notorious hacker in South Africa has taken over the websites of the presidency, the treasury, Cybersecurity Hub and the Department of Environmental Affairs to display political messages.

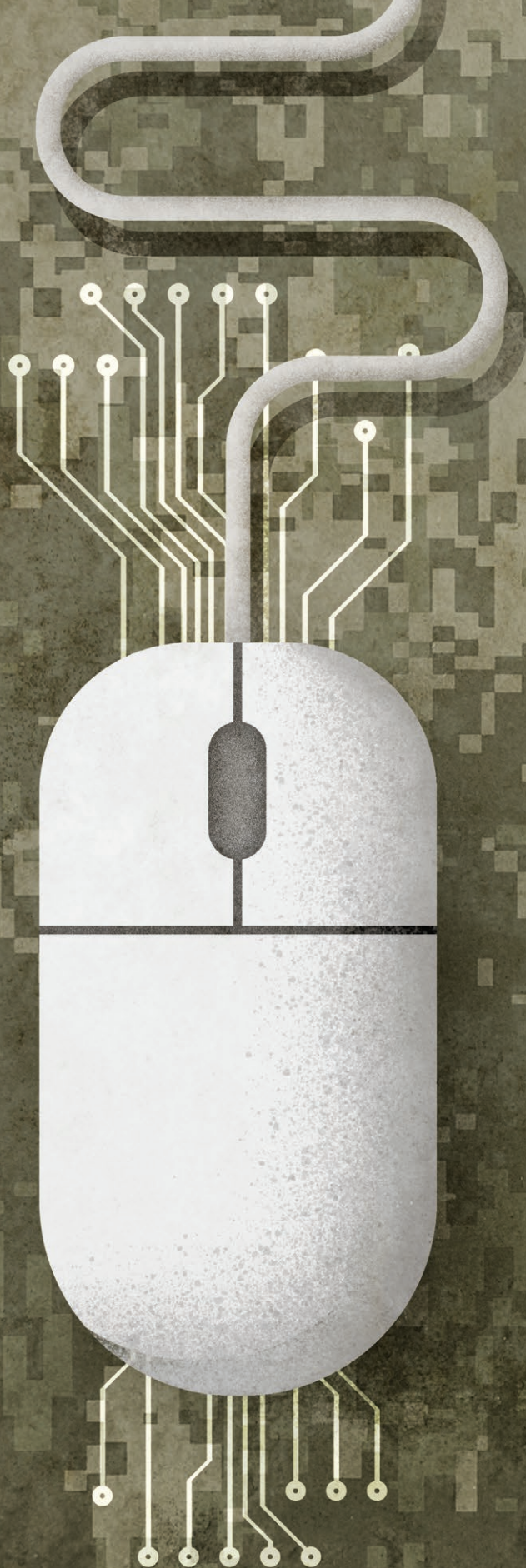


## The Loop of Safety

Guarding against cyber crime requires preparation, vigilance and rapid response. Security experts say it is helpful to think of cyber safety like a loop in which each aspect of preparedness is linked to the next. By building and maintaining this loop, organizations of all sizes can protect against attacks.









# WHO DEFENDS THE WEB?

---

MILITARIES ARE LAUNCHING CYBER COMMANDS,  
BUT THEIR ROLE IS STILL BEING DEBATED

ADF STAFF

**T**hroughout history, technological advances and new discoveries have led to military reorganization. Eight years after the first flight, planes flew in combat in World War I. Shortly thereafter, the first air forces were formed. Similarly, the advent of submarines led to underwater warfare, and space travel has spurred discussions on how to defend space.

Militaries have always adapted to changing threats. Their latest challenge is cyberspace.

Militaries typically are charged with defending the nation against foreign threats while police and other security agencies handle domestic issues.

But cyber threats are foreign and domestic. Attacks can originate from anywhere on the globe and infect information systems inside the country. Attackers can be states, terrorists, petty criminals or activists. Solutions to this

problem vary, but nearly all nations agree the military has a role to play.

"The potential consequences of a major cyber attack in terms of damage to the economy and to the ability of the country to function are such that this should be regarded as part of the defense domain," said South African defense analyst Helmoed Romer Heitman in a defence-Web article. "This is an intelligence-heavy area, so the requisite intelligence and protection/defense capabilities, and the development or pre-emptive and counterstrike capabilities, should ... lie with defense intelligence."

In many nations the military has advantages in terms of resources and know-how that make it the natural candidate to protect against cyber crime. South Africa and Nigeria are launching standalone cyber commands, and many other African nations are beefing up their training and capabilities within existing command structures.

# PROS AND CONS

---

*As militaries prepare to play a role in national cyber security, they are confronted with the benefits and drawbacks of stepping onto this new battlefield.*

## CAPACITY TO HELP

**Pro:** Militaries typically are well-resourced and mission-oriented. In less-developed countries, the military might be the only institution capable of marshaling resources against a large cyber threat.

**Con:** If the military takes the lead in cyber security, it might crowd out the private sector and stunt its cyber security development.

## WITHIN THE MISSION

**Pro:** Cyber security fits the mission of defending the homeland from foreign adversaries.

**Con:** Chasing all instances of cyber crime can overextend the military and lead to accusations of overstepping its legal mandate.

## CRITICAL INFRASTRUCTURE

**Pro:** Attacks against critical infrastructure, such as electric grids or air traffic control, can cripple a nation. The military has a duty to protect against such attacks.

**Con:** Defending the cyber networks that control critical infrastructure requires special expertise. Cyber experts employed by the private sector, local governments or as part of a computer emergency response team are better suited to study and defend these networks.

## ON THE OFFENSIVE

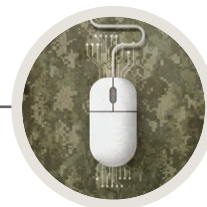
**Pro:** Offensive military cyber attacks can hit adversaries before they strike. In some cases these attacks can disrupt enemy weapons programs or damage infrastructure.

**Con:** The weaponization of the web could prompt an escalation in the conflict and invite retaliation.

**“ IF YOUR COUNTRY IS UNDER A SUSTAINED, ALL-OUT CYBER ATTACK AGAINST KEY INSTITUTIONS, YOU WOULD WANT TO CALL ON ALL THE ASPECTS OF NATIONAL POWER, INCLUDING THE MILITARY. ”**

**– Ian Wallace**

co-director of the Cybersecurity Initiative at the New America Foundation



Given this, it is important to examine the roles and limits on what the military can do to meet the cyber threat.

## 1. PROTECTING MILITARY COMMUNICATIONS AND HARDWARE

In most nations the military is responsible for signals intelligence and operates a variety of communications equipment such as satellite phones and radios. Defense equipment and weapons are becoming more sophisticated and reliant on information systems. Global positioning systems can track everything from bombs to jeeps to Kevlar suits. Disrupting this information flow could be catastrophic.

“The ability to protect those systems becomes absolutely essential,” said Ian Wallace, co-director of the Cybersecurity Initiative at the New America Foundation. “It’s not even necessarily that those systems might be prevented from being used effectively but also that they might be penetrated by adversaries for information or even spoofed.”

The cornerstone of any cyber defense operation must be to protect its own assets and information.

The military secures reams of information that could imperil lives if accessed. Some of this is obvious, such as a battle plan or theater strategy, but other information, such as military health records, can be equally important. In a hypothetical attack, Wallace said, cyber adversaries could breach military health records and alter the blood types listed in order to disrupt care at hospitals.

## 2. MAINTAINING AN OFFENSIVE CAPABILITY

Defeating cyber threats requires the ability to disrupt an attack before it reaches its target.





Skilled professionals can go to the source of a threat and degrade it rather than waiting for the enemy to launch an attack. In a war, this offensive capability also can be used to shut down parts of an adversary's infrastructure.

This is a controversial aspect since it leads to charges of "weaponizing cyberspace" and could prompt retaliatory attacks. But some have argued it is necessary. Lt. Col. Michael Aschmann of the South African National Defense Force co-authored a paper outlining why he believes that African nations need to invest in "cyber armies."

"A cyber army [cyber command] for an African nation state will be an extension of the nation's military power to close the gap of the fifth dimension, the info sphere," Aschmann wrote. "It will enhance the defending and protection of the technological realm and the cyberspace of the nation and be able to offensively fend off a cyber-onslaught from an adversary nation."

This capability is still in its infancy in many countries. Debate about where and when it should be used is robust.

### 3. PROTECTING CRITICAL INFRASTRUCTURE

A cyber attack on critical national infrastructure can cripple a country. Assets such as roads and bridges, energy production, commercial air travel, water, and health systems are key to national defense.

Because of this, the military must be prepared to respond to an overwhelming cyber attack against critical infrastructure. However, Wallace cautions against making the military the first line of defense in this realm.

"If your country is under a sustained, all-out cyber attack against key institutions, you would want to call on all the aspects of national power, including the military," he said.

But having the military take the lead against the numerous, smaller cyber incidents that regularly crop up can be a problem in two ways. First, the military could crowd out the private sector, stifling cyber security development there. Second, the military could become overextended and divert resources from other missions.

Military vehicles are displayed at the Egypt Defense Expo in Cairo. Modern vehicles and weapon systems often include digital components, leaving them vulnerable to cyber attacks.

REUTERS

# NIGERIA FORMS AFRICA'S FIRST CYBER COMMAND

ADF STAFF

**N**igeria has been one of Africa's most proactive countries in fighting cyber crime — and with good reason. The Nigerian Communications Commission says that Nigeria ranks third globally in cyber crimes, behind the United Kingdom and the United States.

Nigerian interests are plagued by ransomware, cryptocurrency scams, cyber Ponzi schemes and other crimes. For years, computer viruses have been common. The extent of the problem is unknown, because an estimated 80 percent of Nigeria's cyber crime is unreported.

The country's 2015 Cybercrime Act imposes punishments, up to the death penalty, for cyber crime convictions.

The country's military decided in 2016 to take on cyber crime, but it wasn't until August 2018 that the Cyber Warfare Command was established, beginning with 150 Soldiers pulled from the ranks and trained in information technology. Their mission is to monitor and defend cyberspace and attack cyber criminals.

In February 2019, Nigerian Lt. Gen. Tukur Buratai said, "I have directed the Nigerian Army Cyber Warfare Command to disrupt terrorists' propaganda activities by embarking on robust counternarratives to neutralize efforts aimed at misleading and misrepresenting the situation on the ground."



Nigerian Chief of Army Staff Lt. Gen. Tukur Buratai

REUTERS

Buratai has said that cyber warfare is the fifth domain of warfare after land, sea, air and space. He contends it is the most dangerous form.

"The intrinsic features of cyberspace can be easily exploited for information warfare by actors with malicious intent to plant and disseminate fake news and instruct paid users to spread online manipulated content," Buratai said, as reported by the Nigerian newspaper *Leadership*.

Buratai said he has assigned the command to routinely survey and analyze suspicious online activity to help the Army become proactive in dealing with cyber crime. Africa Independent Television reported that the command will address issues such as cyber terrorism, extremist propaganda, terror recruitment drives, fake news and data theft. "It will also enhance digital monitoring of all ongoing operations, especially the war against Boko Haram in northeast Nigeria," the network reported.

Temporary headquarters for the command will be in Abuja, with regional stations added as needed. A permanent office complex has been authorized for construction. Nigeria also has been in talks with South Africa to work together against cyber crime.





TO PROTECT CRITICAL INFRASTRUCTURE, MANY COUNTRIES ARE SETTING UP COMPUTER EMERGENCY RESPONSE TEAMS WITH EXPERTS FROM A RANGE OF BACKGROUNDS.

Wallace recommends a “lock your own door” approach in which the private sector, backed by police, takes the lead in responding to most cyber attacks. The military would only be called in as the last line of defense to thwart a major attack.

“Given the ubiquity of information systems through society, if the military were solely responsible for defending those systems, then you would be introducing the military into many parts of society where, for the good of the country and for the good of the military, it is probably better that they’re not engaged,” Wallace said.

To protect critical infrastructure, many countries are setting up computer emergency response teams (CERTs) with experts from a range of backgrounds. Often backed by government funding, these specialists have

intimate knowledge of key national systems and can serve as first responders after an attack or suspicious activity.

Dr. Benoit Morel, an information and communications technology expert, argued that African nations particularly need to develop CERTs. He pointed to Morocco and Egypt as success stories. “African countries should not wait. They should build expertise at home, now,” Morel wrote. “At the moment, the best experts in cyber security tend to be the cyber criminals. Building that kind of expertise at home, when it comes to Africa, means doing something different from the actions taken in advanced economies. A kernel of expertise has to be developed ... a group of people (it does not need to be very large) whose mission is to take responsibility for cyber security in the country.” □

**The port terminal in Algiers, Algeria. Cyber adversaries target critical national infrastructure, and some militaries are training to protect them.**

REUTERS

# Development Through Digitalization

Ghana's Cyber Security Advisor Says the Country is Preparing for the Opportunities and Threats of a Digital World



GHANA MINISTRY OF COMMUNICATIONS

Since 2017, Dr. Albert Antwi-Boasiako has served as the national cyber security advisor to the government of Ghana. He is also the founder of e-Crime Bureau, a pan-African cyber security and digital forensics company. E-Crime Bureau has worked with police, military, and private and public institutions across the continent. It formed the first cyber security and digital forensics lab in West Africa. This interview has been edited to fit this format.

**ADF:** In your current role as national cyber security advisor, you're helping to shape Ghana's cyber security policy. What are the biggest threats facing Ghana in this realm?

**Antwi-Boasiako:** My fear is a cyber attack targeting critical national information infrastructure. That is the most difficult issue. It's what keeps me thinking, what denies me sleep — an attack that would undermine our critical information systems. In Ghana, cyber fraud, impersonation, identity theft and business fraud are quite prevalent. However, those things, you live with them. They are reported, and some kind of response is deployed. But what really could undermine our developing country [is a different type of attack]. I'm making this point because the government has what is called a "Ghana Beyond Aid" agenda. This

is a framework and policy direction of the government, and there is a huge element of digitalization. The government wants to develop through digitalization. A lot of initiatives have been deployed. We have the paperless ports, so ports, customs services, imports, exports are done through an online platform. The government is also rolling out a national identification system across the country. We just launched an E-Justice system in which the administration of justice is being delivered electronically. We have launched a national property addressing system. All these are what I call "government digitalization initiatives," and together with the critical national information infrastructure, they constitute a significant sector of our economy. The fear of a cyber attack is that it would impact national security, and it would erode the trust that we are building in terms of cyber security.





The Bank of Ghana and the rest of the country's financial sector are working to shore up cyber security.

REUTERS

**ADF:** What sector is most targeted?

**Antwi-Boasiako:** We have experienced a number of attacks targeting critical national information infrastructure in the financial sector. Indeed, more than 70 percent of the attacks that we have experienced are financially motivated. Systems are being compromised; attempts are made to remove money from customers' accounts. The government has taken the initiative in establishing security systems in the Bank of Ghana to address the issue. A new finance cyber security directive has been introduced to ensure the financial institutions scale up their cyber security efforts. These measures are being rolled out across the critical national information infrastructure sectors, and that is a direct response to the fear that our critical information resources could be a target of a cyber attack.

**ADF:** Ghana has become a regional and continental leader in cyber security. The country is launching a National Cyber Security Centre. What role will this center play in improving cyber security?

**Antwi-Boasiako:** Cyber crime is a cross-cutting issue. It's a multidimensional problem. Consequently, you have different agencies, both public and private, whose role or mandate relate to cyber security. In addressing a problem of this nature, you need to establish a central point of contact. So the National Cyber Security Centre has been established to coordinate cyber security-related activity both in government and the private sector. Some of its key functions are incident response, awareness creation, engaging with Parliament, providing advice and developing best practices. In terms of operationalization, we are



# “A Safer Digital Ghana”



Ghanaian President Nana Akufo-Addo speaks at the beginning of National Cybersecurity Awareness Month in Accra.

GHANA MINISTRY OF COMMUNICATIONS

creation. We are deploying technology to facilitate threat and cyber incident information-sharing that will bring in all the stakeholders. This means they will be able to report incidents but also receive threat information that the center will distribute.

**ADF:** Ghana’s Ministry of Communications is partnering with the Kofi Annan International Peacekeeping Training Centre to create a training laboratory for security professionals. How important do you believe it is for members of the military and police to be trained in cyber security? What role should the military play in cyber security?

**Antwi-Boasiako:** In terms of the national architecture of cyber security, the military is an important player. Essentially, we’re talking about cyber defense that must be integrated into the military training. It’s also important to appreciate that there is a paradigm shift, and the necessary actions must be taken to incorporate cyber defense in the curriculum, in the thinking, in the strategy and policy in the military environment. So e-Crime Bureau established a relationship with the Kofi Annan International Peacekeeping Training Centre. A lab has already been established, a 32-computer lab with technology, hacking tools, forensic tools and training programs. The training is at two levels: creating awareness among men and women in uniform as well as law enforcement officers to appreciate the dangers of cyber issues so that they can lead the military action in terms of capacity building and research and development. There have also

at a formative level. We’re not a startup anymore, but still formative. This means we have been able to recruit staff, and we are actively working on awareness

been training programs to introduce military officers who are technical to be able to play around with cyber offensive and defensive tools, just to get insight into this new field. Any military, to be relevant, has to embrace this and develop. I think, in terms of the military cyber capability, they are developing phenomenally in our region, and my advice is for government to develop a defense strategy that effectively incorporates cyber security both in protecting the data, systems and the networks of the military, but also in preparing our Soldiers to protect and defend the country. Attacks are coming from outsiders who are aiming to really damage and bring our country down. The military has to have a role in terms of preventive measures and defensive measures.

**ADF:** Ghana is creating computer emergency response teams (CERTs) to respond to cyber incidents. What role will these CERTs play in protecting the country from cyber attacks and responding quickly in the event of an attack?

**Antwi-Boasiako:** The national CERT has been established within the National Cyber Security Centre. Ghana is operating a decentralized system of CERTs. Decentralized means you have identified certain critical sectors. The military is one sector, the financial sector is another, government, telecommunications, energy and academic environment. Each of those sectors is working on a CERT that operates in coordination with the national CERT. So, for example, we already have established the CERT for the telecommunications sector. The National Communications Authority, which is the regulator and has authority for the security of the critical systems in the telecommunications environment, oversees this. The financial sector has established a CERT to protect the devices and networks in the financial sector, and that also is





An illustrator speaks to a client in Accra, Ghana. As digital commerce grows, the country is working to reinforce cyber security. REUTERS

linked with the national CERT. The national CERT has a wider coordinating role while the sectorial CERTs have a role in taking care of the systems, networks and data within their territory, their particular sector. This has worked overall, and we have had countries in West Africa that are coming to learn from the Ghana example.

**ADF:** Many countries, including some in West Africa, have limited resources. How should they prioritize cyber security?

**Antwi-Boasiako:** By my estimation, in the next 50 years, I don't think the question of lack of resources or lack of finances will be a question of the past. It will still be part of the African story. Let's take this approach: If we should wait until we get money to get results, we will never get there. It is a question of pragmatic intelligence. The question we need to ask is: Do we see our development linked to digitalization? How can African economies develop without going digital? It is an impossibility. We would actually be cut

off from the global world. I think the argument that Ghana has made is that we don't have an alternative to digitalization. The United Nations and the World Bank have estimated that it has the potential to transform our economy. E-commerce is creating jobs on the continent. So, for any forward-thinking African country, digitalization is key, and therefore measures must be taken to ensure that the investment in information and communications technology development is protected. The government of Ghana has resolved to establish a cyber security fund, because the nation's cyber security development cannot be sustainable if it is underpinned by donor support. Our president wants to build "Ghana Beyond Aid," and we need to be innovative. By the end of the year the government will establish a cyber security fund to develop the cyber security ecosystem. And I have advised to look at innovative ways to have the necessary funds to staff the criminal justice sector, the defense sector, the government sector, private sector, civil society. That way they can have those resilient cyber ecosystems so that our investment in digitalization can be protected. □







# Ivoirian Painter Gives New Life to Electronic Waste

STORY AND PHOTOS BY REUTERS

**D**esire Koffi often walks through Koumassi, a working class district of Abidjan, Côte d'Ivoire, to buy old mobile phones from people for 500 CFA francs (\$0.87) a pair.

Back home, the 24-year-old artist smashes the phones with a hammer and pulls out the screens and keypads. He uses them for his paintings, which can take three to five days to complete.

Koffi grew up in Koumassi and says he was drawn to recycling and incorporating e-waste into his art after seeing how it affected his environment.

"My number one goal is to try, in my own small way, to reduce electronic waste that is found in the streets and in the bins," he said. "Here, we are in one of the city's most popular neighborhoods, where you usually find old phones which can no longer be repaired."

With a population of 5.5 million, Abidjan generates up to 1,500 tons of e-waste per year, according to the E-waste Implementation Toolkit. Koffi says much of this waste can be used to make money.

With several exhibitions abroad and at home under his belt, Koffi is quickly becoming one of Côte d'Ivoire's most important figures in contemporary art.

"I think his work is great. He has decided to go into recycling, and it really suits him because his work stands out from all others," said fellow Ivoirian artist Ezechiel Guibe.

"Despite incorporating recycling material into his work, he manages to capture all these forms, faces and emotions in his work, which really blew us away," added art gallery director Olivier Pepe.







# THREATS ABOUND AS CONTINENT CONNECTS



# With Africa's Internet Growth Comes More Risks and More Opportunity

ADF STAFF

The prospects for crippling cyber attacks are no longer the stuff of science fiction and blockbuster movies. The tools of cyber warfare have been tested on large and small scales all over the globe.

In short, cyber attacks are here to stay. Perhaps Ukraine offers the most effective and well-known example. It was there, in December 2016, that the lights went out. Hundreds of thousands of residents were plunged into darkness for hours until workers could manually re-engage the electricity grid. A similar attack had occurred a year earlier. The blackouts were not isolated incidents, but instead part of a stream of attacks, according to a June 2017 article in *Wired* magazine.

"They were part of a digital blitzkrieg that has pummeled Ukraine for the past three years — a sustained cyberassault unlike any the world has ever seen," *Wired* reported. "A hacker army has systematically undermined practically every sector of Ukraine: media, finance, transportation, military, politics, energy. Wave after wave of intrusions have deleted data, destroyed computers, and in some cases paralyzed organizations' most basic functions."

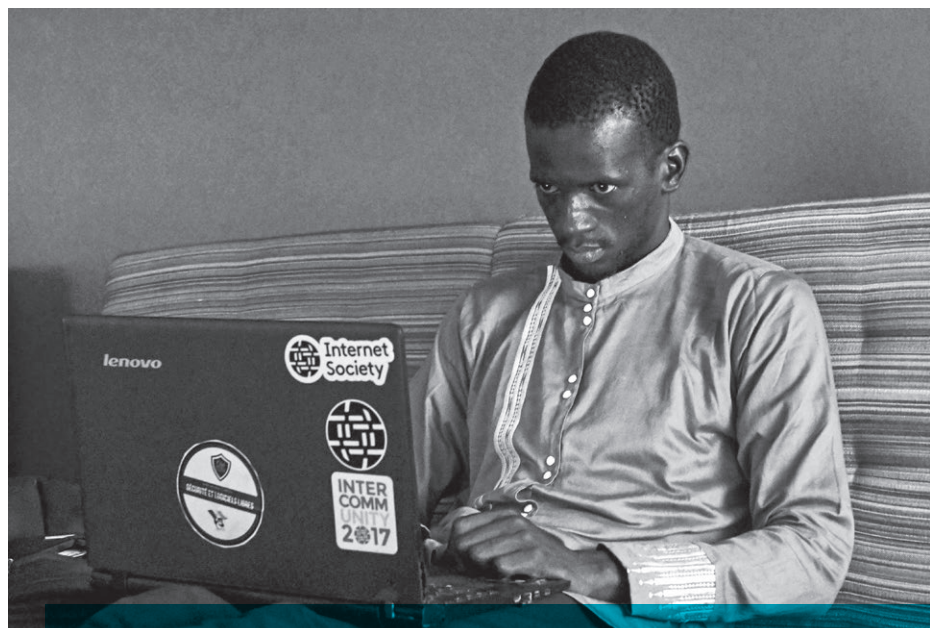
Russia, increasingly famous worldwide for cyber mischief, is presumed to be responsible for the Ukrainian attacks.

In December 2016, Ukraine's president, Petro Poroshenko, said there were 6,500 cyber attacks on 36 targets in the Ukraine in two months' time. He blamed the attacks on the "direct or indirect involvement of secret services of Russia, which

have unleashed a cyberwar against our country," *Wired* reported.

Many observers see Russia's apparent attacks on the Ukraine as a series of test runs. The nation could have gone further, caused more damage for longer, but it pulled back before it did irreparable harm.

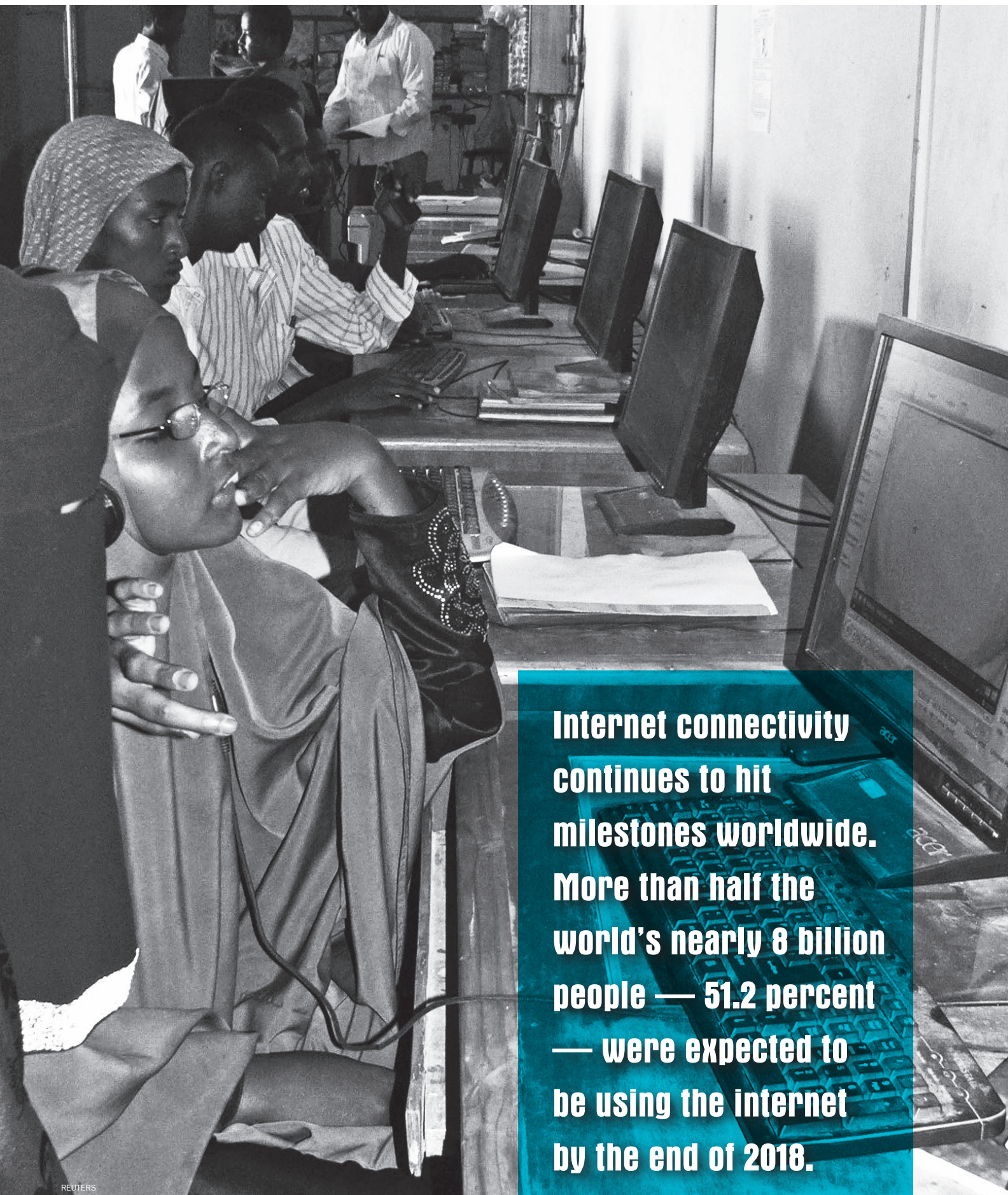
"The gloves are off. This is a place where you can do your worst without retaliation or prosecution," Kenneth Geers, a NATO ambassador who focuses on cyber security, told *Wired*. "Ukraine is not France or Germany. A lot of Americans can't find it on a map, so you can practice there."



A man uses a computer at Impact Hub Dakar, a web design startup in Senegal.

AFP/GETTY IMAGES





**Internet connectivity continues to hit milestones worldwide. More than half the world's nearly 8 billion people — 51.2 percent — were expected to be using the internet by the end of 2018.**

REUTERS





A Liberian voter checks his name against the government's official website on a mobile phone outside a polling station.

AFP/GETTY IMAGES

## THE THREAT IN AFRICA

At first glance, African nations might not seem to be likely cyber targets. But that is certain to change as connectivity across the continent increases.

Internet connectivity continues to hit milestones worldwide. More than half the world's nearly 8 billion people — 51.2 percent — were expected to be using the internet by the end of 2018, the United Nations telecommunications agency announced that December. The figures also show that Africa experienced the strongest growth in internet access, going from about 2 percent in 2005 to more than 24 percent in 2018, the website Modern Diplomacy reported.

By 2022, 60 percent of the global economy is expected to be digitized, according to CNBCAfrica. And although those improvements can be a boon to development, increased connectivity will intensify opportunities for cyber crime. Cyber attacks lead to \$400 billion in annual global economic losses.

Malicious actors compromised more than 4.5 billion records in the first half of 2018, which was nearly double the 2.7 billion records compromised in all of 2017.

Dr. Greg Conti, security strategist at IronNet Cybersecurity in the United States, said there are two major types of cyber attacks: targeted and untargeted. In a targeted attack, cyber warriors might decide to compromise a particular nation's energy sector or power grid, such as what happened in the Ukrainian attacks.

In an untargeted assault, cyber attackers might decide to indiscriminately go after dams all over the world. "If it's easy, why not sweep us as much as you can? Find the vulnerable systems," Conti said. Detecting vulnerabilities is not as difficult as it may sound. For example, a tool called Shodan, which a CNN report called "the scariest search engine on the internet," looks for internet-connected devices 24/7, collecting information on 500 million services and devices each month.



Nigerian journalists view election results. Elections have come under cyber attack in Nigeria and elsewhere. REUTERS

Shodan turns up information on everything from the mundane — security cameras, traffic lights and home appliances — to the more sensitive, such as command-and-control systems for nuclear power plants. Many of these detected devices have no security measures, CNN reported.

“A quick search for ‘default password’ reveals countless printers, servers and system control devices that use ‘admin’ as their user name and ‘1234’ as their password,” CNN reported. “Many more connected systems require no credentials at all — all you need is a Web browser to connect to them.”

A security specialist used Shodan to find a car wash that could be turned on and off, CNN reported. A city’s entire internet-connected traffic control system could be put into test mode with a single command. So if it’s so easy to scan the entire internet for connected and vulnerable devices, it’s possible that African nations could get caught up in a wide-ranging, opportunistic attack.

“I have to think state actors, they plan ahead,” Conti told *ADF*. “If something’s easy, if it’s not that hard to do, I could see them sweeping Africa and countries that aren’t obvious power players in the world.”

Bad actors will prioritize regions, and Africa will not be ignored in that calculus. An October 2018 *New York Times* report indicated that Chinese and Russian spies have listened in on the personal conversations of world leaders. The communications systems of the heads of various military institutions in Africa also are valuable. So although such targets might not warrant the same level of effort by state-backed hackers, they would not be immune from attacks, Conti said.

## AFRICA RESPONDS

Although cyber capabilities still need much growth and development, a number of African countries are showing increasing awareness and concern in the cyber security realm.

South Africa began an offensive strategy in 2016 and established a Cyber Security Incident Response Team “to prevent or recover from a cyber warfare incident through the establishment of the cyber command centre,” according to OIDA Strategic Intelligence, a French independent consulting firm. The team has been issuing periodic information security advisories and reports since at least October 2018.





A Nigerian bank and cyber cafe are indicative of the growing connectivity across Africa.

REUTERS

Nigeria also is proactive in addressing cyber threats. The Nigerian Army has formed its Cyber Warfare Command, which reportedly will employ 150 people drawn from the military who are to be trained in information technology, according to a *Forbes* report. The command's aim is to "monitor, defend and assault in cyberspace through distributed denial of service attacks on criminals, nation states and terrorists." Nigeria has suffered numerous cyber attacks, including one blamed on insurgent group Boko Haram during the election in 2015 that hacked the Independent National Electoral Commission website.

Ghana's Ministry of Communications has established the National Cyber Security Centre, which is charged with coordinating cyber security activities in government and the private sector. It also is responsible for cyber security incident coordination and awareness. The nation's 2019 budget provides for the establishment of a National

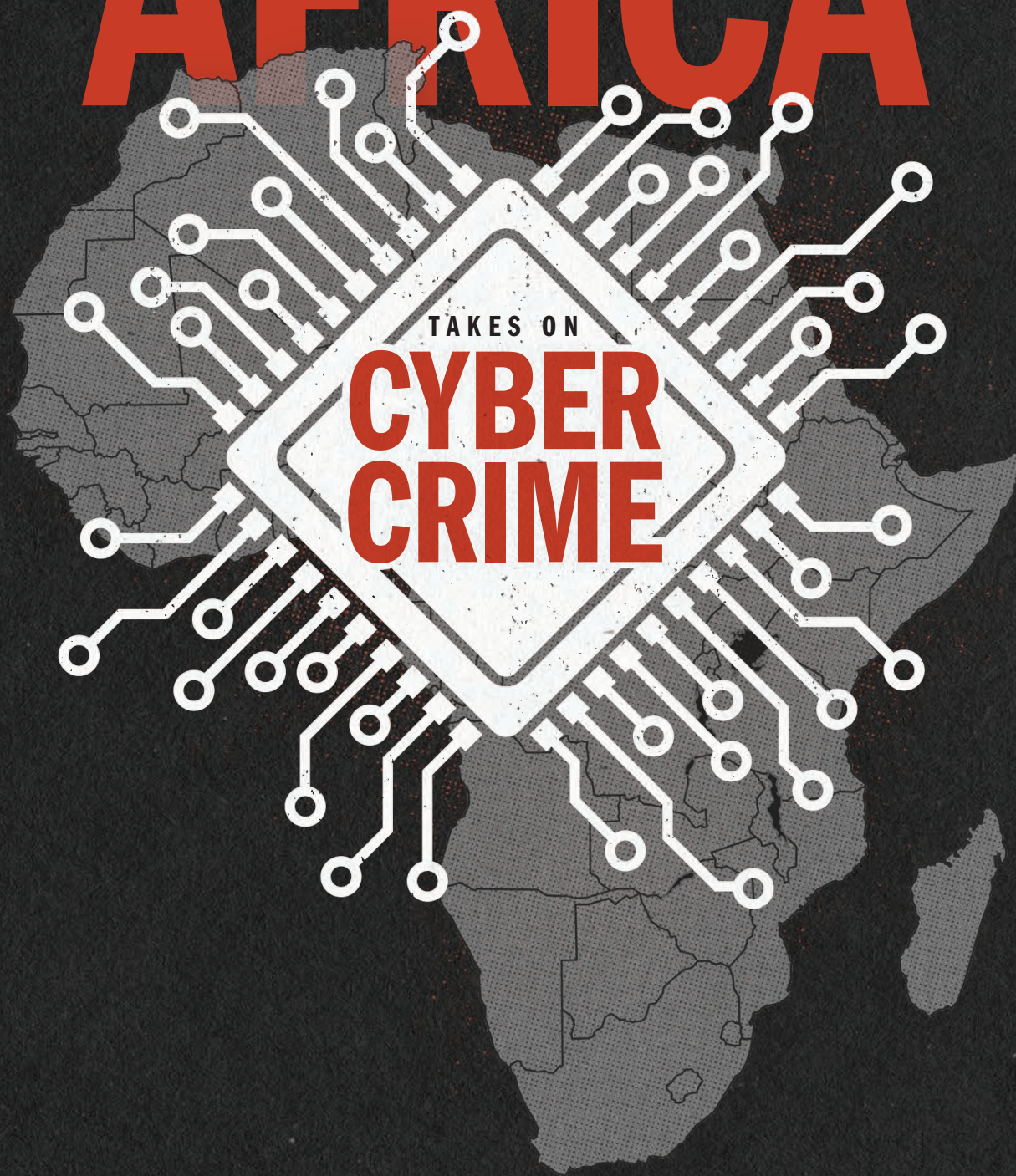
Cyber Security Authority to oversee protection of critical national information infrastructure, according to Myjoyonline.com.

Senegal has set up the National Cyber-Security School to train security service, judiciary and business personnel in how to combat cyber crime such as terrorism funding and propaganda, Agence France-Presse reported.

More than 1,300 delegates from 28 African countries and beyond met for two days in Nairobi, Kenya, in July 2018 at the inaugural Africa Cyber Defence Summit. Attendees included representatives from government, business and academia across a wide range of industries and disciplines. According to ITWeb Africa, Mauritius' minister of technology, communication and innovation, Yogida Sawmynaden, told assembled delegates that Africa needs a single cyber security law "to harmonize our laws and speak one digital language in order to counter attacks." □



# AFRICA



TAKES ON  
**CYBER  
CRIME**



## AS THE CONTINENT IMPROVES ITS COMMUNICATIONS INFRASTRUCTURE, IT BECOMES A BIGGER TARGET FOR CYBER CRIMINALS

ADF STAFF

---

**S**eparated by cultures, religions, languages and 8,458 kilometers, Morocco and India appear to have little in common. And yet, in late 2018, the two countries signed a memorandum of understanding (MoU) to work together on several fronts.

One of the problems the two countries share is cyber crime. According to India's Policy Commission, India ranks third in the world in terms of internet users, after the United States and China. India's internet use grew sixfold between 2012 and 2017, with an annual growth rate of 44 percent. With that growth has come cyber crime: The country ranks seventh in the world in sending out spam and ranks among the top five countries afflicted by online crimes.

Morocco's judicial police recorded 1,091 cyber crime cases in 2018, compared with 765 cases the previous year — a 33 percent increase. Moroccan police recorded 435 victims of online sexual blackmail, including 125 non-Moroccans, with 267 arrests.

The MoU means the two countries will work together on cyber security. "The MoU aims to promote closer cooperation for the exchange of knowledge and experience in detection, resolution and the prevention of security-related incidents for both sides," a news release said. "The implementation of the MoU will result in significant mutual benefits in India's cyber security sector, through institutional and capacity-building with Morocco."

Morocco has been among Africa's leaders in trying to address cyber crime. It requires companies to comply with laws on cyber crime, the protection of personal data and electronic exchanges.

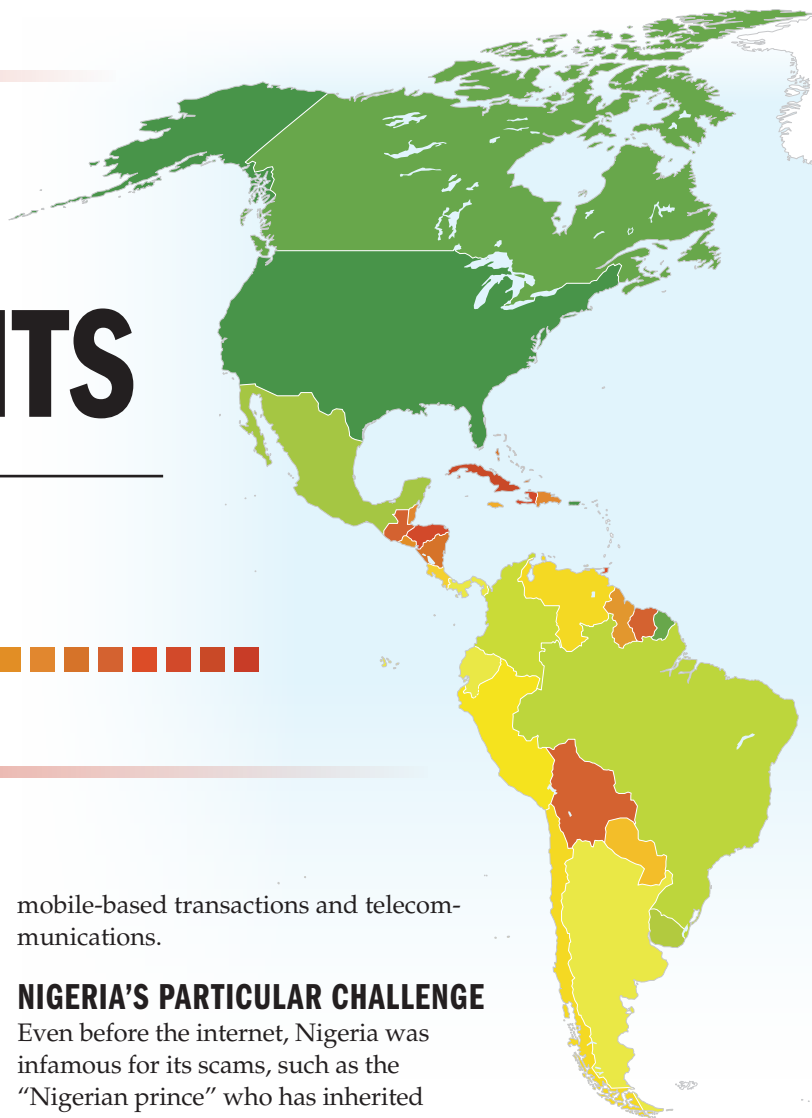
**"IT WOULDN'T BE UNREASONABLE TO SAY THAT 80 PERCENT OF ALL COMPUTERS YOU FIND IN AFRICA WILL HAVE SOME NASTINESS ON THEM."**

— Tariq Khokhar, computer scientist

The United States-based Brookings Institution says the average cost of cyber crime for businesses throughout the world has increased 22.7 percent since 2016. Data leaks have increased 27 percent. A single attack of the WannaCry ransomware in May 2017 hit more than 400,000 computers in 150 countries in a matter of days. As of early 2019, intelligence officials said, the WannaCry ransomware was

# NATIONAL CYBER SECURITY COMMITMENTS

**LEVEL OF COMMITMENT:**  
from **GREEN** (highest) to **RED** (lowest)



still on hundreds of thousands of computers, albeit in a dormant state.

In a 2018 report, Brookings wrote, “As cyber-crimes are threatening companies all over the world, the risk is even higher for African businesses.” Although Africa is comparatively limited in its communications infrastructure, its low level of cyber security has made it a prime target of cyber criminals.

Computer security is not a new problem for Africa. In a 2016 study, the Business Software Alliance said that 57 percent of software installed in Africa and the Middle East was pirated, promoting cyber attacks and causing a potential loss of \$3.7 billion. Computer scientist Tariq Khokhar said, “It wouldn’t be unreasonable to say that 80 percent of all computers you find in Africa will have some nastiness on them.”

The nations of Africa will not thrive without addressing cyber security. The European Union’s General Data Protection Regulation, which the EU describes as “the most important change in data privacy regulation in 20 years,” went into effect in May 2018, and African countries wanting to maintain commercial relations with Europe will have to comply with the union’s rules.

Cyber crime affects every facet of life in Africa. The “Africa Cyber Security Report 2017” said Africa’s banks and financial services account for nearly one-fourth of the continent’s cyber crime losses, followed by governments, e-commerce,

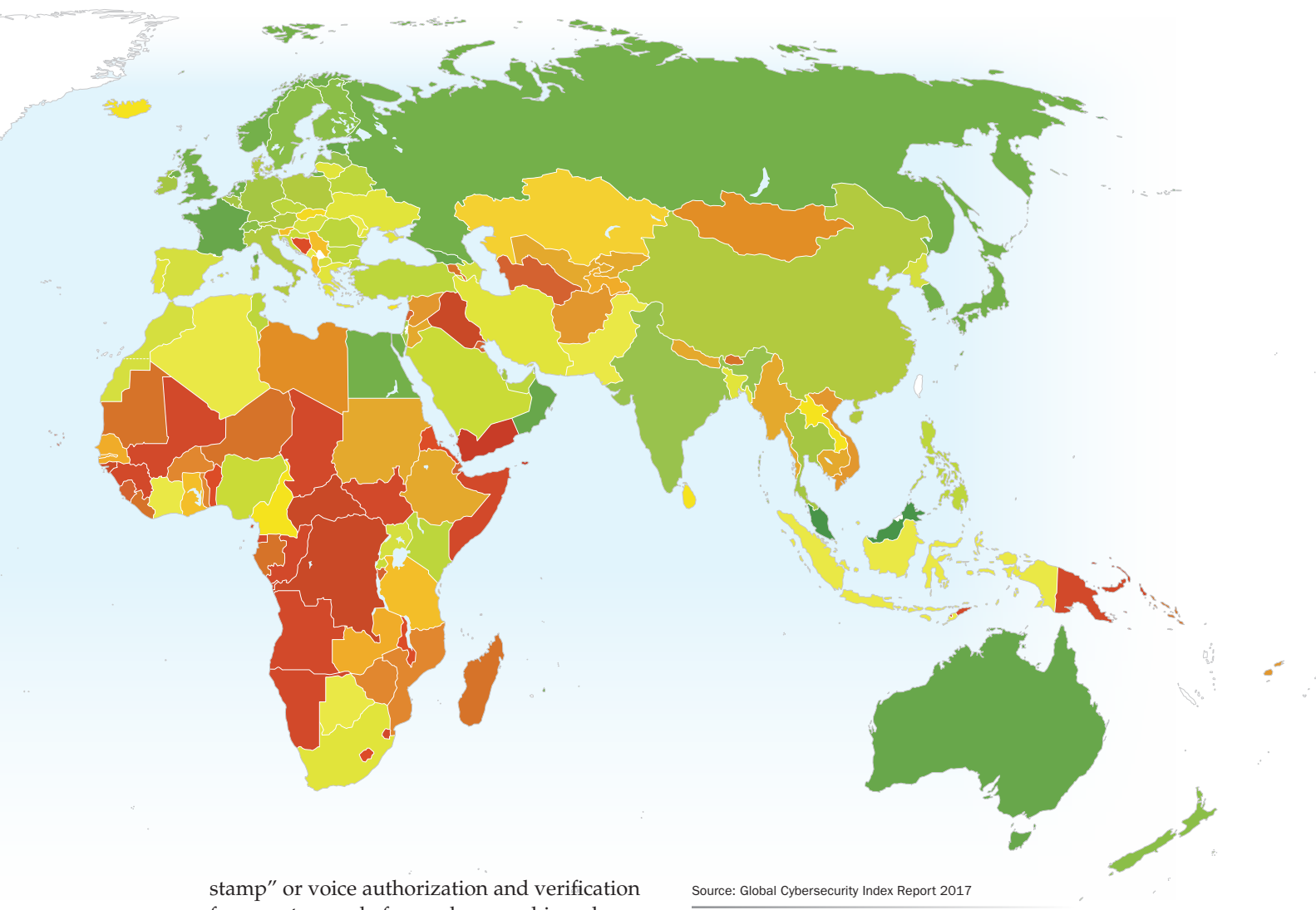
mobile-based transactions and telecommunications.

## **NIGERIA’S PARTICULAR CHALLENGE**

Even before the internet, Nigeria was infamous for its scams, such as the “Nigerian prince” who has inherited wealth but needs someone’s bank account number in which to deposit the money. As a result, Nigeria has had a head start in addressing cyber security. In a June 2013 study by the *International Journal of Cognitive Research in Science, Engineering and Education*, researchers laid out the basic steps for any system to address cyber crime:

- Educate citizens to continually maintain and update their computer security systems. Corporations and organizations must also be required to learn best practices for effective computer management.
- Establish programs and information technology forums for young people, which not only equips a new generation to deal with cyber crime, but provides new jobs for a class of people that has been underemployed.
- Use address verification systems to ensure that the address on product order forms matches the address of a buyer’s billing statement.
- Employ interactive voice response terminals, a type of technology that collects a “voice





Source: Global Cybersecurity Index Report 2017

stamp” or voice authorization and verification from customers before orders are shipped.

- IP address tracking makes sure that the IP address on a customer’s order is from the same country included in the order’s billing and shipping addresses.
- Use video surveillance systems.
- Anti-virus and anti-spyware software prevent and stop computer viruses and restrict “back-door” intrusions into computer systems.
- Firewalls protect computer networks from unauthorized entry.
- Cryptography codes information so that it can be decoded only by the sender and the intended recipient.
- Cyber ethics and cyber legislation require internet service providers and their customers to take measures to protect themselves from cyber crimes.

## DEFENDING AGAINST CYBER CRIME

Landry Signé and Kevin Signé, writing for the Brookings Institution, say there are four steps that African businesses must take to deal with cyber crime. Although the steps are aimed at the business sector, they also are good practices for other sectors.

### 1. Design and deploy cyber resilience:

In its “State of Cybersecurity 2018” report, ISACA, formerly known as the Information Systems Audit and Control Association, said that four out of five security professionals worldwide believe that their enterprises were likely or very likely to experience a cyber attack during the year. Half of the respondents indicated that their organizations already had experienced an increase in attacks over the past year. Preventing or stopping cyber attacks begins at the executive level “by prioritizing and enacting procedures that will protect valuable assets and by integrating them as requirements into all business processes,” the Brookings report said. A company should raise its security measures by:

- Building its employees’ skills in information security.
- Securing its information systems and regularly updating its infrastructure.
- Using technologies for active surveillance.
- Implementing proactive detection and rapid response systems for security breaches and incidents.





# AFRICAN COUNTRIES LEAD THE WAY IN FIGHTING CYBER CRIME

ADF STAFF

In dealing with cyber crime, the nations of Africa are handicapped by a lack of local expertise and a lack of laws addressing the problem. But there are countries that are handling the issue head-on. The “Africa Cyber Security Report 2017” by cyber security firm Serianu said these countries excel in dealing with cyber crime:



## MAURITIUS

The tiny nation of Mauritius, with a population of just 1.2 million, has established itself as the information and communications technology leader in Africa. Government leaders say the country is championing the cause of a common cyber security law for all of Africa. Mauritius was among the first African countries to change privacy laws to comply with the European Union’s General Data Protection Regulation.

In its annual Global Cybersecurity Index for

2017, the International Telecommunication Union said Mauritius’ Botnet Tracking and Detection project allowed the country’s Computer Emergency Response Team to “proactively take measures to curtail threats on different networks within the country.”

“Capacity building is another area where Mauritius does well,” the index reported. “The government IT Security Unit has conducted 180 awareness sessions for some 2,000 civil servants in 32 government ministries and 20 years.”





## RWANDA

The index ranked Rwanda second in cyber security in Africa. Like Mauritius, Rwanda is pushing for continentwide security protocols.

Rwandan officials say their own protocols and laws stopped 8 million cyber attacks in 2017.

The index said that Rwanda “has a standalone cybersecurity policy addressing both the public and private sector” and is “committed to develop a stronger cybersecurity industry to ensure a resilient cyber space.”



## KENYA

The index ranked Kenya third on the continent, noting that the National Kenya Computer Incident

Response Team Coordination Centre was coordinating cyber security at national, regional and global levels. As the mobile money capital of Africa, Kenya enacted its Computer Misuse and Cybercrime law in May 2018.

On December 19, 2018, the Communications Authority of Kenya said that the number of cyber attacks detected in the country grew to 3.8 million between July and September 2018, an increase of 400,000 threats from the previous quarter. In early 2019, the center warned the public that it had detected “Emotet,” a malware program that was targeting network systems worldwide.



## NIGERIA

Nigeria ranks fourth in Africa in terms of cyber crime defense, despite having a worldwide reputation for cyber scams and other cyber crimes. The tech media company IDG said cyber crime has been “an image nightmare for the country.” Even with its security advances, Nigeria lost \$649 million in cyber crime-related activities in 2017, the highest amount on the continent.

However, the country is proposing a tax that would help agencies fight cyber crime. The 0.005 percent tax on telecom companies was proposed in the 2015 Cybercrime Act to train cyber security agents. Despite being Africa’s most populous country with nearly 200 million people, it has only 1,800 certified cyber security professionals.

- Performing regular security audits and penetration tests.

**2. Develop cyber security skills:** A shortage of experienced and skilled cyber security specialists may be the biggest problem facing the continent. Leaders in government and business must attract such specialists or find the means to train them. Keeping such specialists will be difficult. “African organizations must adopt effective strategies to face the brain drain of their most talented cyber-security profiles,” the authors wrote. “Indeed, as they gain the necessary skills, those specialists become increasingly mobile and may choose to relocate, especially to Europe and North America.” Currently, less than 1 percent of security skill management programs address experimental recruitment and talent retention. By 2020, the authors said, that figure will rise to 20 percent.

**3. Protect data integrity:** Protecting data may replace confidentiality as the primary goal of cyber security. Many recent cases of ransomware, in which software hijacks a computer system or data until a ransom is paid, have highlighted the importance of data integrity. In cases where ransoms were paid, none of the companies was able to confirm that it ultimately got all of its data back. Companies and other sectors must improve security measures to prevent ransomware attacks and massive data corruption.

In addition to regular data backup, there are new technologies that record transactions across several computers linked in a peer-to-peer network. Some countries, particularly in North Africa, already are exploring new technologies to handle security threats. The Brookings Institution said that information security spending in the Middle East and North Africa grew 11 percent in 2017, to a total of \$1.8 billion.

**4. Integrate cyber risk awareness into the decision process:** An organization’s cyber security goals, systems and assets should go beyond just the top management and the cyber security team. The goal is to “popularize cyber risk-aware culture at all levels.” The organization’s executives also “should be more aware of their accountability in case of a cyberattack and recognize the need for skilled managers to identify and act against potential cyber threats.”

ISACA says that worldwide, only 21 percent of chief information security officers report directly to the head of the company, while 63 percent report to the chief information officer. This structure means that these companies regard cyber security as more of a technical issue than a financial one, which ISACA says is a mistake. □



# COMPETITORS AND COMRADES



OSMA SHOWS THAT ATHLETIC COMPETITION  
AMONG SOLDIERS CAN HAVE A BROAD IMPACT

ADF STAFF • PHOTOS BY OSMA





The fifth African Military Boxing Championship (CAMBOXE) opens in Algeria in October 2018.





The Organization of Military Sports in Africa (OSMA) was created with a simple goal in mind: Build bridges of friendship through sports. Organizers believe athletic competition among Soldiers from across the continent can accomplish things that hours of drills, conferences and other military training cannot.

Competitors square off during CAMBOXE 2018 in Algiers, Algeria.







"It contributes to the broader effort of peace and develops the ideals of fraternity, hospitality, integration and mutual understanding that characterizes the African armed forces," Col. David Kadré of Burkina Faso, president of OSMa, told [journaldebrazza.com](http://journaldebrazza.com). "These ideals are dear to our African leaders for economic development and the emergence of our beloved continent."

Founded in 1994, OSMa is the African regional arm of the International Military Sports Council, a 71-year-old organization headquartered in Brussels. OSMa is headquartered in Yaoundé, Cameroon, and holds annual competitions in boxing, basketball, football and other sports. It has 45 member nations.

Competitors say the benefits of athletic competition can be felt well beyond the arena. Studies of military athletes have shown it can help Soldiers avoid noncombat injuries and recover from the psychological trauma of war.

In October 2018, about 100 boxers from 14 nations met in Algiers, Algeria, for the fifth African Military Boxing Championship (CAMBOXE). During five days of heated competition, participants not only boxed but discussed issues of mutual interest and gathered for social events and festivities. Algerian athletes won the

most medals, followed by Kenya and Tunisia.

Also in 2018, OSMa athletes participated in a cross-country race in Luanda, Angola, and a basketball championship in Brazzaville, Republic of the Congo, where the Congo took first place, followed by Morocco and Angola.

Kadré said the events, which are attended by fans from all walks of life, are a great way to promote civil-military relations. He believes it helps humanize Soldiers.

"A scene of amity between the people and the military is what a nation needs," he said. "It is only when the people and the army are one that we can say that there is a balanced relationship."

Kadré also hopes that an organization such as OSMa can repair the image of Africa's armies, which too often has been tarnished by indiscipline and accusations of violence against civilians. "Stories of war and destruction normally overshadow the good news. But sport is something that can be a means of change," he said.

"I hope African countries utilize sport as a medium of avoiding clashes and permit positive changes of development and friendship," Kadré said. "Which is exactly one of the top targets of OSMa, also something that the organization strongly acts for at a continental level." □






---

# TRAINING *for the New* BATTLEFIELD

*Simple, Low-Cost Measures Can Put  
Militaries on Road to Cyber Security*

---





**A** n employee, spending one of countless days in front of a computer screen, opened an email and clicked on a link. That began the invasion.

ADF STAFF

The worker, a computer technician at Saudi Aramco, a major Saudi Arabian oil company, presumably was well-schooled in the ways of careful computer use. But not, apparently, on August 15, 2012, during the holy month of Ramadan. The clicked link was all that hackers — calling themselves the “Cutting Sword of Justice” — needed to infiltrate one of the richest companies in the world.



In just a few hours, 35,000 company computers had been destroyed or partially wiped, according to a CNN report. Screens began to flicker. Computers shut down. Files disappeared. Company employees all over the world yanked cables out of servers and disconnected from the internet, hoping to halt the virus' destructive march.

Saudi Aramco's 9.5 million-barrel-per-day production continued, as did drilling and pumping. But the attack hurled administrative functions, such as supply management, shipping and contractual issues, into the technological stone age of paper and typewriters.

There was no internet, no corporate email service. Even the telephones went quiet. If a contract needed to be signed, workers faxed it — one page at a time. The company even had to turn away tanker trucks seeking refills. After more than two weeks of paralysis, Saudi Aramco was giving away oil to maintain domestic flows.

In the immediate aftermath of the attack, the company bought 50,000 new computer hard drives at once, paying above-market prices to get priority access. The purchase strangled global hard drive supplies.

"Everyone who bought a computer or hard drive from September 2012 to January 2013 had to pay a

slightly higher price," Chris Kubecka, a former security advisor to Saudi Aramco, told CNN.

One email. One link. One click. That's all it takes to lose a battle in cyberspace. No country is immune. No military can prepare too much.

China, North Korea and Russia already have shown a willingness and ability to attack other nations in the cyber realm, setting their sights on elections and infrastructure, to name two targets. Although many African nations may not seem to be high-profile targets, they cannot be complacent, said Dr. Jabu Mtsweni, research group leader for cyber warfare at South Africa's Council on Scientific and Industrial Research.

"The threats are vast," Mtsweni said, "and I think we are not immune to any of them."

### SOLUTION STARTS WITH TRAINING

Establishing solid training and teaching best practices is the best way to ensure that Africa's militaries are prepared for cyber threats. Experts agree that everyone can take steps to lessen the potential for a wide range of cyber threats, even if expert personnel and high-tech equipment are unavailable. Nations can deliver this training to Soldiers and officers through professional military education institutions.

Participants conduct a cyber security tabletop exercise during Africa Endeavor in Cape Verde in August 2018.

LT. CMDR. DESIREE FRAME/U.S. AFRICA COMMAND







Such military training academies exist across the continent, and many focus on an array of subjects, notably peacekeeping and war strategies. Cyber security has not yet achieved the status of other, more traditional, military instruction. That is largely due to a lack of awareness, Mtsweni said, and a lack of personnel with training, experience and interest in cyber security matters. Most African militaries, he said, have kept their focus on traditional, kinetic warfare tactics and strategies. Altering that mindset will require changes — and time.

“I think your first stage should start mostly at the recruitment stage,” Mtsweni told *ADF*. “In other words, when the military recruits, they need to start looking at recruiting for a digital age.”

This is easier said than done. People with cyber security skills are in short supply everywhere. Some degree of interest and proficiency is essential, because not everyone is inclined toward or talented in technology. Even setting up and delivering the training is not enough. There must be an opportunity to use and develop new skills.

Cyber-trained officers and Soldiers will become discouraged if they do not have an outlet for using their training. Mtsweni said those who are trained will need to be able to implement what they have learned.

#### **FINDING A CHAMPION**

Dr. Greg Conti, security strategist for IronNet Cybersecurity in the United States, directed the Cyber Research Center at the U.S. Military Academy at West Point and its Army Cyber Institute. He told *ADF* that the best way to start effective cyber security training is “with a senior leader champion.” The alternative is to wait for change to come from the grass roots. That will be slower and less likely in a military hierarchy.

Mtsweni agrees that finding a champion is key. “Everything rises or falls on leadership, so if there’s a leader who is a champion for cyber security, you will find that it is easier for the ground forces to follow through,” Mtsweni said. “And in the African context, you have less of that, because most of the colonels and generals, they are more





**As the use of computers and other electronic devices continues to spread in Africa, governments and militaries will have to bolster cyber security measures.**

you speak of cyber security, because that's not their training when they were training in the military. They were never really introduced to cyber security."

If a senior leader turns attention to cyber security, those in the lower ranks will follow. The leader doesn't even have to have technical proficiency or

of an old school where they grew up. In South Africa we say, 'They were born before technology.' They call them 'BTs,' so they were born before technology in the sense that it is very difficult for them to relate when

deep knowledge of the subject, just a realization of its importance and a commitment to addressing it with money, resources, space and continued attention. This, Conti said, will help others see the importance of cyber security and buy into it. The senior leader's priority will trickle down to others in the command structure.

From there, the leader needs to identify people with relevant talent and abilities, retain them and promote them. If a force can identify and empower a cyber security specialist and help them grow, the results will be "game changing," Conti said.

Once personnel are identified, there are training options that can achieve valuable results without





requiring huge expenditures. For example, there is a wealth of free cyber security information online. Or personnel could work from books that cost about \$30 each.

If more money is available, Conti said a military force could send someone for training, who then returns to brief colleagues and share materials. Such a person could become the “local expert” on cyber security at a one-time cost of several thousand dollars for travel and tuition.

#### **EFFECTIVE, LOW-COST TRAINING**

Cyber security knowledge and safe habits can be effective without costing a fortune. Training can be tailored to Soldiers and officers, depending on their experience and responsibilities. The key, Conti said, is delivering the right amount of cyber security training to the right people at the right point of their careers.

What a private needs

likely will differ from what a noncommissioned officer or commissioned officer needs.

Training can be targeted to the many, the some and the few, he said. The most important training for the largest number of people would focus on “cyber hygiene.” This entails all the fundamental steps everyone must take in cyberspace. Without them, everything else fails.

Some examples are keeping passwords private, changing passwords frequently, and not clicking on links or opening attachments in unsolicited or suspicious emails. Even taking a selfie with a cellphone during an operation and posting it on social media

sites can endanger a sensitive mission.

It’s also important to make sure that military computers are running clean versions of popular software. Conti told of how bazaars in Iraq sold Microsoft Office for \$1 to \$3. There is no doubt, he said, that such software is loaded with viruses, malware and other malicious code.

The next training would be for what Conti calls the “some” group. This includes enablers who work in the cyber realm occasionally, such as lawyers and policy-makers, military planners and those who build and operate computer networks. Training in the Center for Internet Security’s (CIS) top 20 basic controls would be helpful to this group, Conti said. The list includes inventory and control of hardware and software assets, email and web browser protections, malware defenses, wireless access control, account monitoring, and incident response and penetration testing, among other things.

The CIS list represents the industry’s “canonical set of best practices for securing your IT infrastructure,” Conti said, adding that the list probably can protect against 80 percent of low- and medium-level threats. People in the “some” group also could pursue additional certifications such as the Certified Information Systems Security Professional.

The “few” category includes what Conti calls “true cyber security specialists,” such as those who are hands-on keyboard operatives who handle offensive and defensive cyber capabilities. Their training would be highly specialized and would likely include expertise in signals intelligence and how to leverage it in cyber warfare operations, cyber policy and law, intelligence analysis, computer network exploitation, and how to integrate cyber into kinetic operations, and vice versa.

#### **AWARENESS GROWS**

Mtsweni said several African countries are beginning to show an increasing awareness of the importance of cyber security. He said nations such as Ghana, Kenya, Mauritius, Rwanda, Senegal and South Africa are showing a commitment to cyber security. Militaries typically take their cues from governments, so as governments continue to prioritize cyber security, national militaries are likely to follow.

However, it will take time to build national cyber security capabilities — perhaps five years or more, Mtsweni said.

Conti said the same is true regarding the training of military personnel. Attention to cyber security cannot be fleeting. “It needs to be part of a long-term vision.” □





ADF ILLUSTRATION



# *Countering* — the — MESSAGE

STOPPING ONLINE PROPAGANDA BY  
EXTREMISTS TAKES MORE THAN JUST  
SHUTTING DOWN THE MESSENGER

ADF STAFF

**F**or years, the blueprint for countering extremist propaganda was straightforward: Insist to followers that their beliefs are wrong and that they are suffering as a result. Tell them to abandon their cause and that they will have better lives if they change sides. Repeat the countermessages as often as necessary.

The only problem with countermessaging is that it rarely works.

Dr. Cristina Archetti, author of *"Terrorism, Communication and New Media: Explaining Radicalization in the Digital Age,"* says that developers of anti-extremist messaging need to abandon old models.

"To start with, from reports on how to counter online radicalization to governments' calls for taking extremist material off the internet, there is a strong focus on messaging," wrote Archetti. "Whether this means fighting the terrorists with the right countermessage or removing their extremist message, this approach reflects a woefully outdated

model of public-media interactions."

Archetti said that such a model, sometimes referred to as the "hypodermic needle" type of communication, was developed after World War I, when the victors believed they had won at least in part because of the persuasive powers of propaganda.

Such a model is now widely recognized as simplistic and naive. As Archetti noted, "We can all realize in the immediacy of our everyday lives that we do not buy every commodity advertising messages tell us to buy."

Today, extremists use the internet and social media to recruit followers, usually people in their teens and early 20s. The extremists use high-quality videos to convince these young people that they are victims of discrimination because of their beliefs.

"ISIS has proved fluent in YouTube, Twitter, Instagram, Tumblr, internet memes and other social media," reported *The Guardian* of the United Kingdom. "Amateur videos and images are also



being uploaded daily by its foot soldiers, which are then globally disseminated, both by ordinary users and mainstream news organizations hungry for images of a conflict their own cameras cannot access.”

These target audiences can be found in regions of the world where jobs for young people are few, and dissatisfaction with the government and the status quo is high. Governments and information tech specialists have been pulled into the fray, forced to try to stop the extremists’ messages while trying to develop countermessages.

## “It is vital to capitalize upon the potential contributions of all stakeholders, including internet companies and internet users.”

— “Countering Online Radicalisation, A Strategy for Action,”  
by Tim Stevens and Dr. Peter R. Neumann

But countermessaging is complicated. The messages must be worded in such a way that they sympathize with and relate to the target audience. Countermessages must have a personal touch, and they have to point out that the extremists’ doctrine is based on falsehoods and distortions.

### FIRST-INSTINCT APPROACHES

Researchers say that the first-instinct approaches to countering extremists’ messages on the internet have focused on technical solutions, with the theory that removing or blocking such material will fix the problem. In their 2009 study, “Countering Online Radicalisation, A Strategy for Action,” researchers Tim Stevens and Dr. Peter R. Neumann said such a technical approach is “bound to be crude, expensive and counterproductive.”

Stevens and Neumann said that any strategy aimed at countering online radicalization must create an environment in which the creation and consumption of such messages becomes not only more difficult technically, but also unacceptable and undesirable. They noted that governments alone cannot stop online extremist messaging. “It is vital to capitalize upon the potential contributions of all stakeholders, including internet companies and

internet users.” They also recommended:

- **Deterring producers:** The selective use of website and social media takedowns, along with the prosecutions of the producers responsible, “would signal that individuals engaged in online extremism are not beyond the law.”
- **Empowering online communities:** Creating an “internet users panel” to improve reporting mechanisms and complaints procedures would give users a voice in the anti-extremist strategy.
- **Reducing the appeal of the message:** “More attention must be paid to media literacy, and a comprehensive approach in this area is badly needed,” the authors wrote.
- **Promoting positive messages:** Establish an independent startup fund to provide money for “grassroots online projects” aimed at countering extremism. “The aim is to capitalize on the enthusiasm and goodwill of communities around the country who might be willing to invest time and commitment but need limited financial support in order to get their ideas on the net.”

Other experts also have recommended providing money for grassroots online projects. In “Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter it,” authors Ghaffar Hussain and Dr. Erin Marie Saltman urged the establishment of a central body that offers seed funding and training for grassroots online counterextremism.

“Challenging extremism online should be a joint effort between public, private and third sector stakeholders,” the authors said. They also suggested:

- **Establishing a forum** that deals with online extremism and brings stakeholders from key sectors together.
- **Improving digital literacy** and critical consumption skills in schools and communities.
- **Encouraging the establishment** of a social media outlet that clarifies government policies and debunks propaganda.
- **Conducting a mapping exercise** to explore current efforts to tackle extremism online and identify partners who could be given support to develop an effective online presence.
- **Conducting more research** into how extremists are using the internet to spread propaganda.





This girl escaped from Nigeria's Boko Haram extremist group, which operates from a region in which many are dissatisfied with the national government. REUTERS





A man repairs a computer in Khartoum, Sudan. Some extremist groups have tech-savvy messaging, so combating that will be a challenge as Africa becomes more connected online. REUTERS

## ACKNOWLEDGE THE GRIEVANCES

A common point in all strategies for countering extremists' messages is that no one specific counter-measure works in all cases.

In his report, "Online De-Radicalization? Countering Violent Extremist Narratives: Message, Messenger and Media Strategy," political scientist Omar Ashour said it is critical to "address every dimension as well as to tailor the message to different audiences, especially to young people and their concerns."

Extremists figured out years ago that going after today's youthful target audiences by posting long sermons on the internet was not working. Instead, they switched to modern propaganda — internet videos and short messages posted on social media. And they've gotten good at it.

A tailored counternarrative must avoid oversimplification, shallowness and generalizations, because such shortcuts invite what Ashour calls "strike-backs." The countermessages should be attractive and encouraging, but also acknowledge the validity of some — even all — of the grievances, such as a lack of jobs and economic opportunities. The countermesssage must offer alternative ways to address the grievances, while emphasizing "the legitimacy

and effectiveness of non-violent strategies."

Even though these approaches are not new, "the identity of the message-bearers makes a big difference," Ashour said. He mentioned an instance in which an Islamic group accepted counternarratives after rejecting them previously because they were finally delivered by people they knew and trusted.

After constructing the countermessages and coordinating with the chosen messengers, the next task is publicizing and promoting both of them in the media. Ashour notes that "many of the battles won by violent extremists were on media fronts." The media dimension of the counternarrative requires three steps:

- Analyze the counternarratives available and highlight their strengths and appropriateness for the audience in question. Evaluate the potential impact.
- If necessary, translate the message. Then summarize and simplify it, if needed, to suit the streamlined nature of some forms of media. Use texts and multimedia forms, such as online videos and audios.
- Introduce the messengers, their background and their experiences.



## DON'T TAKE SHORTCUTS

Countering online propaganda is not a simple, mass-media task. A U.S. State Department report, "Countering Extremist Speech Online," outlines six suggestions for confronting extremist recruiters:

- **Don't take shortcuts:** Although a strategy to counter extremist narratives online can be useful, community-level engagement remains the cornerstone of getting a message across. Counter the presence of recruiters in communities.
- **Use broader countermessaging:** It must be paired with technical solutions, including website shutdowns and content filtering. Shutting down websites is often temporary at best, because extremists simply start up new sites. Technical measures have their place, but they must be used surgically in support of larger prevention and countering of violent extremism measures.
- **Tailor your message to fit your audience:** Countermeasures that may seem persuasive and reasonable to moderates can backfire when used on an audience that is more politically charged. People responsible for composing countermessages must understand the perspectives of audiences that have already become at least partially radicalized.
- **Provide logical, honest alternatives to false extremist stories:** Research indicates that people are more likely to listen to and believe stories that provide honest alternatives to their beliefs. For example, when extremists promote false narratives, such as that the United States targets civilians in Iraq and Syria, it is not enough to deny the claim. An accurate countermassage must be provided.
- **The messenger matters:** Even moderate populations that reject most extremist ideology also will reject counterinformation from sources they do not trust. The countermessages must come from voices within their own communities. Those speakers must have influence and respect — qualities that often develop slowly.
- **Counter incorrect beliefs with affirming correct information:** Simply rejecting extremists' claims can have the opposite effect of reinforcing them. Countermessages must have accurate claims and facts that go beyond simple rebuttals.

## LOOK FOR THE REASONS

In *The Atlantic* magazine, staff writer Graeme Wood said that Westerners who accuse Muslims of blindly following "ancient scriptures" accomplish nothing in terms of getting to the roots of extremism. True scholars, he said, know better.

"Look instead, these scholars urged, to the conditions in which these ideologies arose — the bad governance, the shifting social mores, the humiliation of living in lands valued only for their oil," wrote Wood.

Another strategy, Ashour said, is to identify specific historical events to give the political dimension legitimacy. The narrative focuses on "the glorification of violent acts, including terrorism, as well as their perpetrators." An example would be the highly violent videos that some extremists have posted on the internet, which have included torture and beheadings.

The narrative emphasizes what it calls religiously legitimate actions or reactions to political grievances and social oppression. In the case of al-Qaida, those actions are emphasized as individual religious duties.

## FINDING OUT WHAT WORKS

Regardless of what approaches are used to counter extremists' messages, the results should be closely monitored. For instance, providing money for grassroots initiatives without determining whether they are effective is wasteful.

"There can be no question that many of the projects that might receive support will be unsuccessful," wrote Neumann and Stevens. "This should come as no surprise. The internet, after all, is a hugely dynamic environment, and it is not at all clear why certain websites fail while others succeed. Even if it was possible to find an explanation, new technologies and modes of interaction might soon make it irrelevant."

The two authors added that they encountered "a tremendous amount of interest and goodwill" in doing their research. "The internet industry, for example, may have concerns about heavy-handed government regulation, but it seems quite ready to make a positive contribution where this is possible and constructive. Such expressions of intent should be actively drawn upon in constructing a truly comprehensive strategy."

They noted that anti-extremist messengers need to be open to evolving technologies and modes of interaction.

"The rise of user-generated content, for example, is often seen as a danger, because much of the material involved in online radicalization is made available in this way," they wrote, adding "not only is user-generated content here to stay, if properly understood it can become a powerful force in countering radicalization." □





AFP/GETTY IMAGES

# 'NIGERIAN MONA LISA' FINDS ITS WAY HOME

REUTERS

**T**he "Nigerian Mona Lisa," a painting lost for more than 40 years and found in a London apartment in 2018, has been exhibited in Nigeria for the first time since it disappeared.

*Tutu*, a painting by Nigeria's best-known modern artist, Ben Enwonwu, was painted in 1974. It appeared at an art show in Lagos the next year, but its whereabouts after that were unknown, until it resurfaced in north London.

The owners, who wished to remain anonymous, had called in an expert in modern and contemporary African art to identify their painting. He recognized Enwonwu's portrait.

The owners put the portrait up for sale, and it was auctioned for \$1.57 million to an anonymous buyer. The sale made it the highest-valued work of Nigerian modern art sold at auction.

It was loaned to the Art X Lagos fair for display in Nigeria.

*Tutu* is referred to as the "Nigerian Mona Lisa" by virtue of its disappearance and re-emergence, and it is the first work of a modern Nigerian artist to sell for more than \$1 million. The original *Mona Lisa*, Leonardo da Vinci's painting, was stolen from the Louvre in 1911. The thief, Vincenzo Peruggia, eventually took it to Italy, where it was recovered and in 1914 returned to the Louvre.

The Nigerian painting is a portrait of Adetutu Ademiluyi, a granddaughter of a traditional ruler from the Yoruba ethnic group. It holds special significance in Nigeria as a symbol of national reconciliation after the 1967-70 Biafran War.

Enwonwu belonged to the Igbo ethnic group, the largest in the southeastern region of Nigeria, which had tried to secede under the name of Biafra. The Yoruba, whose homeland is in the southwest, were mostly on the opposing side in the war.

Enwonwu painted three versions of the portrait. Prints first made in the 1970s have been in circulation ever since, and the images are familiar to many Nigerians. Enwonwu died in 1994.

# ANGOLA WINS

## WORLD AMPUTEE CUP

BBC NEWS AT [BBC.CO.UK/NEWS](http://BBC.CO.UK/NEWS)

Angola won the 2018 Amputee Football World Cup in Mexico, beating Turkey 5-4 in a penalty shootout.

The match ended 0-0 after normal time, and the deadlock could not be broken in extra time. The deciding shoot-out proved just as tense, with both teams scoring from their first four penalties.

Amputee football is played with seven competitors on each team — six outfielders and one goalkeeper. Outfielders each have one leg amputation, and goalkeepers have an arm amputation. Outfielders use forearm crutches and play without artificial limbs.

Angola, which finished as runner-up at the last World Cup, sealed its championship victory, thanks to a winning spot-kick from Henio Guilerme.

Nigeria and Kenya also represented Africa at the competition. Liberia and Ghana, which also qualified to play in Mexico, withdrew before the start of the tournament after Liberia reportedly failed to secure visas on time. Ghana faced financial difficulties.

Angola finished 2018 ranked first out of 22 teams in the world. Kenya was ranked 12th, and Nigeria was ranked 19th.



REUTERS



## POWERHOUSE — OF TALENT SHOWCASED AT — AWARDS SHOW

AGENCE FRANCE-PRESSE

**N**igeria's Davido won the All Africa Music Awards (AFRIMA) trophy for artist of the year, leading a strong showing for West Africa's Afrobeats stars.

Ghanaian artist Wiyaala performs at the 2018 All Africa Music Awards.

AFP/GETTY IMAGES

Musicians from across the continent traveled to the Accra International Conference Centre in Ghana's capital in November 2018 to walk the red carpet and celebrate a year of big hits.

Betty G from Ethiopia took home album of the year, and best African DJ went to Afrotronix, who has roots in Chad.

Nigerian rapper Falz won the award for best rapper after courting controversy this year when he released *This is Nigeria*, which skewered modern Nigeria. It was based on the Childish Gambino hit, *This is America*.

*Akwaaba*, an infectious collaboration between GuiltyBeatz, Mr. Eazi, Patapaa and Pappy Kojo, won song of the year and best African collaboration. Nigeria's 2Baba won for best African pop, Ghana's Stonebwoy for best reggae, and South Africa's Sibusiso Mashiloane for best jazz.

Kuami Eugene, a Ghanaian crooner, was named "most promising" artist in Africa.

AFRIMA has carved out a space as a platform to showcase the innovative and prolific African music industry that has exploded in the past decade. After a 15-year career in banking and marketing, Nigerian Mike Dada established the awards as Africa's version of the Grammys. The 2018 edition was the fourth ceremony.





# Egypt, Sudan

## Join Forces to Secure Border

REUTERS

**E**gypt and Sudan, two countries facing cross-border threats from militias operating in Libya, have agreed to set up joint military patrols along their border.

The patrols eventually may lead to joint forces in the border region to “combat terrorism, cross-border crimes, control the border and combat all manifestations of evasion,” Sudanese Chief of Staff Kamal Abdul Maarouf told reporters.

He said the two militaries would form a strategic partnership in all fields, especially intelligence and operational cooperation and training.

The countries also agreed to joint

investments, Abdul Maarouf said, and allowing Egypt to establish agricultural and animal production projects in Sudan.

Relations between Egypt and Sudan have improved markedly despite persistent tensions over a Nile dam that Ethiopia is building. Egypt sees the project as a threat to its water supply, but Sudan backs it because of its need for electricity.

The two countries have a shared interest in restoring peace to Libya, which has been riven by internal strife since dictator Moammar Gadhafi was toppled in 2011. The resulting power vacuum has allowed rival militias and armed Islamist groups to grow.

**A Sudanese honor guard welcomes Egypt's minister of defense.** AFP/GETTY IMAGES



# SENEGAL

## LAUNCHES CYBER SECURITY SCHOOL

AGENCE FRANCE-PRESSE

Senegal has inaugurated a cyber security school that aims to strengthen West Africa's defense against computer hackers and prevent the internet from being used to fund terror or distribute propaganda.

Senegalese Foreign Minister Sidiki Kaba and French counterpart Jean-Yves Le Drian opened the National Cyber Security School on the sidelines of an annual regional security conference in Dakar.

The school will train security services, the judiciary and private businesses in combating cyber crime. Backed by France, it will have a "regional vocational role" in helping other West African countries, French officials said.

The school, which was proposed at an earlier security conference, initially will be based in Dakar at the National School of Administration before moving to Diamnadio, a new town being built about 30 kilometers from the capital.

Senegal has an internet penetration rate of more than 50 percent and has tried to be a continental cyber security leader. It was the first country to ratify the African Union Convention on Cyber Security and Data Protection.



U.S. STATE DEPARTMENT

## U.S. DIPLOMATIC MISSION TO SOMALIA RETURNS

BBC NEWS AT [BBC.CO.UK/NEWS](http://BBC.CO.UK/NEWS)

The United States has re-established a diplomatic presence in Somalia for the first time in nearly 30 years.

The Department of State said the historic event reflected the security progress the East African nation has made. Ambassador Donald Yamamoto is heading the diplomatic mission in Mogadishu, which previously had been based in Nairobi.

The U.S. closed its embassy in Somalia in January 1991 amid fighting between rebels and the government and had to airlift out its ambassador and staff. Commenting on the latest move, State Department spokeswoman Heather Nauert said: "Our return demonstrates the United States' commitment to further advance stability, democracy and economic development

Donald Yamamoto, U.S. ambassador to Somalia, left, meets with Somali President Mohamed Abdullahi Mohamed.

that are in the interest of both nations."

The extremist group al-Shabaab was forced out of the capital in August 2011 after an offensive spearheaded by African Union troops. Security has improved in Mogadishu, although al-Shabaab extremists remain a threat.

Along with the diplomatic presence, the U.S. Agency for International Development announced more than \$900 million in new investment in the country. This includes \$420 million for humanitarian assistance and money for programs aimed at job creation, good governance, debt relief and education.





## SADC MISSION HELPS STABILIZE LESOTHO

AGENCE FRANCE-PRESSE

**S**oldiers who were sent to Lesotho in 2017 after the country's top Army commander was killed withdrew from the area in November 2018. The Southern African Development Community (SADC), a regional bloc, deployed a force to the landlocked kingdom after an Army commander was shot dead in barracks by officers from a perceived rival faction. The region feared further instability.

The seven-nation SADC force, which included 207 military personnel, 15 intelligence officers and 24 police officers, was deployed for six months and extended to a year. The mission was to "strengthen peace and security," SADC spokeswoman Barbara Lopi said.

At a ceremony to mark the end of the mission, SADC Executive Secretary Stergomena Lawrence Tax hailed progress in restoring security. "There is significant improvement in the working relations amongst the various security agencies, the government and civil society," she said.

Prime Minister Thomas Thabane said the SADC mission left Lesotho "with the confidence that our security agencies would now respect civilian authority and conduct their services as mandated by the constitution."

Known as Africa's Switzerland because of its mountainous scenery, Lesotho has a long history of political instability. It suffered coups in 1986 and 1991.

A Basotho man rides along the road leading to the Maluti Mountains in Lesotho.

AFP/GETTY IMAGES



## PRESIDENT OF COMOROS GREETES TRAINED RECRUITS

ADF STAFF

**T**raining for Comoran Soldiers and gendarmes can be tough — out of more than 900 people who enrolled in a training class, only 541 completed the course.

The training started in 2018 in Itsundzu and was called "Feta 2018." The class produced 263 Soldiers and 278 gendarmes. Comoran President Azali Assoumani congratulated the recruits at their February 2019 graduation and told them that they had not only learned new technical and tactical skills, but also the rules of being a Soldier, committed to the rule of law and international law.

The top five trainees of the gendarmerie and those of the Comoran Defense Force were honored with certificates during the ceremony.



Comoran President Azali Assoumani AFP/GETTY IMAGES

The mufti of the republic, a Muslim religious leader, also attended the ceremony. The Comoran newspaper *Al-watwan* reported that the mufti called on the new Soldiers to take responsibility to protect the country, the president and the flag, and to work for the good of the people.

The small archipelago country with fewer than 1 million citizens maintains military and police forces totaling more than 1,000 members.

# JOINT OPERATION

## CRACKS DOWN ON TRANSNATIONAL CRIME



Burkinabe gendarmes patrol the city of Ouahigouya in the north of the country. AFP/GETTY IMAGES

ADF STAFF

Burkina Faso, Côte d'Ivoire and Ghana launched a joint security operation called Koudanlgou II in the southern and western areas of Burkina Faso. More than 2,000 security personnel from the three countries were involved in the operation in November 2018, which was designed to crack down on transnational crime such as terrorism, smuggling and drug trafficking.

In a news conference after the event in Bouna, Côte d'Ivoire, officials said the operation led to 150 arrests, 11 confiscated vehicles and seized arms, ammunition, cannabis and liquor, the Burkinabe news website Bafujii Infos reported. Security forces also offered health services to local populations, painted a school and repaired a road.

Burkinabe Minister of Security Clément Pègwendé Sawadogo said the operation reinforced a partnership among the Soldiers of the three countries and helped them coordinate efforts and learn about the region where the three countries meet.

Benin, Burkina Faso, Ghana and Togo held a round-table discussion in May 2018 that included security chiefs and heads of relevant departments to discuss strengthening ties to combat cross-border crime.

## ETHIOPIAN AIR FORCE

### *Deals Blow to Al-Shabaab*

ADF STAFF

**E**thiopia's Air Force bombed an al-Shabaab encampment, killing two of the group's leaders.

The January 24, 2019, bombing run in Bur Haybe, east of Baidoa, lasted about 45 minutes, Africa News reported, citing the Ethiopian Broadcasting Corp. The strikes killed al-Shabaab's regional operations chief and an explosives expert in addition to 35 al-Shabaab fighters. The airstrike took out four military trucks and five high-caliber weapons, Africa News reported.

Reports from a week earlier indicated that Ethiopian troops had been ambushed by al-Shabaab in Baidoa and sustained casualties.

Ethiopia formally joined the African Union Mission in Somalia (AMISOM) in 2014 although its military had made



Ethiopian National Defence Forces troops serving in the African Union Mission in Somalia arrive in Kismayo, Somalia. AMISOM

security contributions to the regional effort earlier. In February 2019, AMISOM named Ethiopian Lt. Gen. Tigabu Yilma Wondimhune the force commander of the five-nation mission. "This mission is a challenging one, but we are up to the task," Tigabu said.





# Uganda is World's Most Active Nation

BBC NEWS AT [BBC.CO.UK/NEWS](http://BBC.CO.UK/NEWS)

A report on physical inactivity across the globe found that Uganda is the world's most active nation.

The study, published in the medical journal *The Lancet*, is a compilation of surveys done in 168 countries. It highlights the health dangers of not doing enough exercise.

It found that just 5.5 percent of Ugandans do not do enough physical activity — defined as at least 150 minutes of moderate-intensity or 75 minutes of vigorous-intensity physical activity per week.

People in Lesotho, Mozambique,



Tanzania and Togo are also doing quite well in terms of getting enough exercise.

In comparison, people in American Samoa, Iraq, Kuwait and Saudi Arabia seem to be living more

sedentary lives. About a quarter of the world's population doesn't get enough exercise.

In Kuwait, 67 percent of the population are not active enough, the report says. Mauritania, with a figure of 41.3 percent, is the least active country in Sub-Saharan Africa.

So what is Uganda getting right? People in rural Uganda, where most of the population lives, are active on their farms, says the BBC's Patience Atuhaire. But, she says, in urban areas people are becoming more sedentary, especially as they get wealthier.

---

---

## Program Brings Education Improvements to Madagascar

WORLD BANK

**M**adagascar's public education spending fell in 2009 after a political crisis, putting thousands of children at risk of having to leave school. Others had to drop out because their families could no longer afford to educate them. With a sharp drop in foreign financing, public spending on education had fallen since 2010. Nationwide, few schools were built, teacher and student materials were not supplied, and many schools did not receive government funding.

Emergency funding is helping to overhaul basic education. The Madagascar Emergency Support to Education for All project aims to keep children in primary school by reducing costs to families, paying subsidies to teachers and providing school kits to students.

The project, launched in 2013 by the World Bank, has shored up a crumbling education system.

By the end of the four-year project, it had deployed in 12 Malagasy regions, reaching more than 2 million people. The project enrolled nearly 1.9 million children in school, paid 20,000 teachers and distributed more than 5 million school kits. In Madagascar's three drought-stricken regions in the south, the project enabled more than 100,000 children to eat in school cafeterias. The project built more than 260 classrooms and trained 50,000 teachers.

It paved the way for the new \$100 million Basic Education Support Project funded by the World Bank



Students attend school in Madagascar's Androy region.

AFP/GETTY IMAGES

and the Global Partnership for Education. The project improves learning in the first two years of education in Madagascar.

The new project aims to reach more than 4.7 million beneficiaries. That includes enrolling 4.6 million children in primary school and 80,000 children in early learning centers, and training 35,000 primary school teachers, 6,500 pre-primary community educators, 4,000 community-school board members, and 20,000 principals and local supervisors.

# South African Kids Learn to Code

AGENCE FRANCE-PRESSE

It's Wednesday, 2 p.m. sharp in the densely populated South African township of Ivory Park —time for about 60 11-year-olds to duel at their local coding club.

Armed with basic coding blocks, inventor kits, laptops and inexhaustible imaginations, the six primary school teams compete. The coding club kids use electronic boards to make temporary circuits and prototypes to devise solutions for problems they've identified in their community.

"We are making an incubator machine that helps children who are born premature and those who are sick," said student Sifiso Ngobeni. Competitors from another school are tackling the scourge of missing children.

Coding is the instruction that a robot or computer program reads and then executes. At the coding clubs, students learn to design the code to make it happen. Although access to schooling has increased in South Africa since the end of

apartheid, the education system often fails to make the grade.

"The fact that we still have 80 percent of teachers using chalks and blackboards in this day and age is a serious cause for great concern," education activist Hendrick Makaneta said. "It cannot be correct that the class of 2018 still looks exactly like the class of 1918."

In a country where more than 50 percent of young people are unemployed, coding clubs also boost the chances of finding a job.

Although most of the Ivory Park pupils are familiar with using smartphones, smart TVs and the internet, coding and understanding algorithms is another challenge altogether.

A 2018 report by McKinsey highlights that 45 percent of all current tasks could be automated with present technology. Innumerable aspects of life, from science to engineering, and financial services to law or art, will depend on coding.

## REPORT SAYS AFRICANS LIVING LONGER, HEALTHIER

VOICE OF AMERICA

The World Health Organization (WHO) says Africans are living longer and healthier lives. But the WHO warns that millions on the continent still face the challenge of chronic diseases.

News of the improvement came at a conference in Dakar, Senegal, where WHO representatives met with officials from 47 African countries.

Healthy life expectancy on the continent — the number of years at peak health a person experiences — rose from 44.4 years at the turn of the century to 53.8 years in 2015. Overall life expectancy climbed from 50.8 years to 61.2.

Matshidiso Moeti, the WHO's regional director for Africa, said that two factors were mostly responsible for the change. "What produced this result is a huge increase in access to treatment [of] HIV-AIDS and in the better prevention and management of malaria," Moeti said.

But the WHO says the type of disease that most commonly affects Africans also is changing.

Although the number of deaths from diarrheal disease, respiratory infections and HIV is falling, chronic conditions, such as cancer and heart disease, are claiming more lives.

Death rates from noncommunicable diseases have remained steady since 2000 while the other top 10 causes of mortality in Africa have fallen by 40 percent.

The WHO says health services in Africa must adapt to the new health challenges. Humphrey Karamagi, a WHO coordinator, says the health needs of African youth are too often overlooked. "The kind of health challenges that adolescents face are quite different from what we have been used to responding to — drug use, adolescent obesity and so on."



Students work with robotics kits at a meeting of the Robotics and Coding Club at a South African school. AFP/GETTY IMAGES



# AFRICA LOOKS *to Boost Tourism*

AGENCE FRANCE-PRESSE

**A**frica draws just 5 percent of the world's tourists despite boasting attractions ranging from the Great Pyramids and Victoria Falls to wildlife safaris and endless strips of pristine beaches.

But the continent's huge potential can be unlocked by eco-tourism, cultural experiences, domestic travel and political stability, said experts at an African tourism conference in Cape Town, South Africa.

"When you look at the success stories, it's those countries who've embraced trends," said the African Tourism Association's managing director, Naledi Khabo. "When you look at some countries which have made sustainability a focal point, like Tanzania or Rwanda, they're very attractive for certain travelers."

Eco-friendly safaris and carbon-neutral lodging draw increasing numbers of tourists from Europe and North America. The number of tourists visiting Tanzania has more than doubled since 2006 to more than 1 million, contributing 14 percent of the country's gross domestic product, according to the website Tanzania Invest.

South Africa has witnessed a boom of experience-based tours, taking travelers to disadvantaged township and rural communities, as well as wine farms and game lodges.

Tourism is a major employer of poor South Africans and accounts for nearly 700,000 jobs — a rare success story in a

country with an unemployment rate of almost 27 percent.

Although many African destinations have courted foreign visitors' hard currency, Kenya has invested heavily in promoting "staycations." The country moved to promote domestic travel after foreign arrivals dipped in the wake of recent violent unrest and criminal attacks.

"We have managed to develop the domestic market," said Kenyan Tourism Minister Najib Balala. "Twenty-one percent of Airbnb occupancy is domestic market. It's benefiting us."

Tourism, now the second-largest

driver of Kenya's growth, was worth \$1.2 billion in 2017.

Many countries on the continent have struggled to woo foreign visitors fearful of political instability and violence. Rwanda is one country that has successfully transformed its global image. The small East African nation, torn apart by genocide in 1994, has since established itself as a high-end destination.

"Tourism is the number one foreign exchange earner, which is amazing to see in a country like Rwanda," said Rosette Rugamba, who headed Rwanda Tourism from 2003 to 2010. "It is a huge contributor to the image-building of our country."

Mount Bisoke volcano in Rwanda THE ASSOCIATED PRESS



Dancers perform for tourists in Kinigi, northern Rwanda.

AFP/GETTY IMAGES





## EAST AFRICA MAKES COMMERCE EASIER

VOICE OF AMERICA

An international money transfer company has launched an online service for East Africans to send and receive money more easily. Analysts say WorldRemit will lower the cost of transferring money and boost African economies.

Africa has become a thriving market for money transfer companies as its telecommunication facilities improve and its economies grow.

WorldRemit, a British-based company, handles the transfer of at least \$1.6 billion to Africa each year. The co-founder and head of WorldRemit, Ismail Ahmed, said money transfers in Africa have changed over the years.

"When we launched our services, 99 percent of remittances were cash, both on the sending and receiving side," he said. "But today, that is changing fast, and in the next few years we think as much as 50 to 60 percent of international remittances would move from traditional physical cash, traditional remittances, to digital. And that's why our services have grown very fast in the last few years."

Ahmed said that, as transactions become digital, the cost of each transfer comes down, and tracking money becomes easier.

"It's easier for businesses and individuals to move [money] within countries but also across countries," he said. "It's easier to fight financial crime because once the transaction becomes digital, there is an audit trail, compared to cash where there is no audit trail."

Gerrishon Ikiara, an international economic affairs lecturer at the University of Nairobi, said digital money transfers will boost trade within Africa. However, he noted, some countries still lack the necessary connections.

"Obviously, the main challenge is the level of infrastructure, because a country without the good infrastructure in terms of electricity and telecommunication infrastructure will make it a bit difficult," Ikiara said.

## MOROCCO UNVEILS **FASTEST TRAIN** ON THE CONTINENT

REUTERS

**M**orocco has inaugurated Africa's fastest train, which promises to cut in half the traveling times between the commercial and industrial hubs of Casablanca and Tangier.

King Mohammed VI and French President Emmanuel Macron boarded the train for the inaugural trip from Tangier to the capital, Rabat, in November 2018. The train ultimately will run at 320 kilometers per hour, greatly reducing the time it takes to make the 200-kilometer journey between the two cities.

It is about twice as fast as South Africa's high-speed Gautrain, which links Johannesburg's international airport to the city's financial district of Sandton.

The state news agency MAP said the line took seven years to build and cost 22.9 billion dirhams (\$2.4 billion).

Morocco's national railway operator, Office National des Chemins de Fer Marocain, obtained 12 high-speed trains from French manufacturer Alstom, the website Railway Technology reported.

The trains are designed to suit Morocco's climate and environment and are capable of carrying 533 passengers.

The trains are equipped with the latest features to ensure passenger comfort. They also feature bilingual digital passenger information systems, offering information in Arabic and French.





# The MUTAPA EMPIRE

ADF STAFF

The kingdom of Zimbabwe fell into decline in the early 15th century. Some historians say the region was starving. Others say that the kingdom's warrior prince, Nyatsimba Mutota, left the landlocked region in search of salt, a priceless commodity at that time.

The prince is said to have found salt among a tribe of elephant hunters near the Zambezi River about 300 kilometers to the north. He took control of the region, which included some gold deposits. He took over most of the Zambezi River Valley, establishing the Empire of Mutapa, also known as Monomotapa, and established his capital at Zvongombe.

Historian David Chanaiwa says the empire was somewhat informal and depended on the "charisma, well-being and political wisdom" of its ruler. Mutota ruled his empire with a light touch, avoiding

meddling in the lives of his subjects.

The kingdom had no known historian, so little information about it is available. But Portuguese travelers gave accounts of the capital, describing it as being built mostly from clay, wood and thatch. The capital was surrounded by a wooden stockade that was so big, it took about an hour to walk around it. Inside the stockade were three buildings. One was where the prince held court. Another housed his wives and advisors — about 3,000 people in all. The third building housed his pages and bodyguards, who had been recruited from among the young single men throughout the kingdom. Those young men were groomed to later serve as bureaucrats and Soldiers.

Mutota's son Mwened Matope inherited the kingdom and began expanding it by a series of military campaigns. At its peak, his kingdom included the entire Zambezi River Valley. What are now Angola, Zambia, Zimbabwe and part of Mozambique stretching to the Indian Ocean were part of the empire. Matope took the title *mwenemutapa*, which means "lord of the plundered lands." His regal attire included a finely crafted ivory-handled hoe as part of his belt that symbolized peace through the ability to draw wealth from the earth. Matope made it clear to his people that he was a divine king, the "God of the Sun."

Matope expanded his riches through taxation and long-distance trade. He established markets along the Zambezi River. He almost undoubtedly conducted commerce across the Indian Ocean, probably trading with China and India.

It was a fairly short-lived kingdom. By the mid-1500s, it began to decline politically, militarily and culturally. Its central government became weak and fragmented, and provincial governors took more power. The leaders of one province broke away from the kingdom completely. The Portuguese, who had long been a presence in the region, overran the kingdom and appointed their own choice as ruler.

By the time the Portuguese killed the last ruler of the Mutapa in battle in 1917, the kingdom was a mere fraction of its former glory.



Nyatsimba Mutota, 15th century Zimbabwean king

THE BRITISH MUSEUM



# CLUES

- 1 The Carthaginians founded this site as a trading post, and it was permanently settled in the fourth century B.C.
- 2 After the fall of Carthage, the city came under Roman rule. Baths, temples and fountains remain from this time.
- 3 The city ceased to exist soon after the Arab conquest of 635.
- 4 Excavation has uncovered more than half of the ancient city, including a theater.





# 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](mailto: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



### STAY CONNECTED

Follow *ADF* on Facebook and Twitter and visit us online at: [adf-magazine.com](http://adf-magazine.com)