HM Government

Africa Cyber Programme

Protecting the most vulnerable in Africa from cyber threats

Project Summaries

-

22 September 2023 - FINAL

The UK Government's Africa Cyber Programme

Protecting the most vulnerable in Africa from cyber threats

Millions of people remain excluded from the digital economy giving rise to a damaging global digital divide. Anything that prevents those excluded from getting online, such as issues around security, exacerbates that divide further.

Middle-income countries in Africa are keen for their citizens and businesses to harness the potential of digital access to boost economic development. Digital access for their citizens is growing fast but improvements in cybersecurity typically lag far behind. This gap is fertile ground for cybercrime. The harm caused by cybercrime acts as a brake on development. As well as causing direct economic loss, it reduces trust in technology and the internet, particularly among the economically vulnerable.

As ever, the impact of crime is felt most keenly by those who have the least.

African governments are acting to shore up their cyber defences, making their systems and infrastructure more resilient and educating their populations on how to remain cybersecure, but this is a substantial challenge.

Over a 16month programme October 2022 to March 2024, the FCDO, through its Africa Cyber Programme (ACP) is investing £3m to select, design and implement projects to improve cyber capability and reduce harm in Kenya, Nigeria and South Africa.

HM Government

UKaid from the British people

Backed by £3 million of UK aid from the Conflict, Stability and Security Fund, the ACP is a major UK government investment that builds on the £10m successfully invested in the Digital Access Programme (DAP) Pillar 2 – Trust and resilience. The DAP programme was the UK's largest ever overseas cyber capacity building investment. The ACP will contribute to the UK and FCDO's vision of 'thriving, open digital societies powered by trusted technologies, with the UK leading efforts to uphold a free, open, peaceful and secure cyberspace'.

6 main projects are being designed for Africa. These include supporting the South African Police Service (SAPS) by developing and delivering a course for Detectives to help them solve cyber crime, improving Kenyan citizen's awareness of cyber threats and the governments' strategy for addressing this, including providing a specific toolkit for SMEs to use, and in Nigeria supporting judges, prosecutors and law enforcement officers with digital evidence handling and digital forensic training to strengthen their capacity to prosecute cybercrimes.

In each instance, the ambition is to build sustained capability that allows national partner governments to better protect their citizens online or to defend their critical national infrastructure from cyber threats.

Ultimately, the ACP builds on the UK's cybersecurity experience to help these countries improve safe digital access, bring excluded populations into the digital economy, reduce poverty and stimulate inclusive economic growth.

The Africa Cyber Programme following on from the Digital Access Programme is a UK Government Programme which catalyses inclusive, affordable, safe and secure digital access for underserved populations in Africa; promoting digital ecosystems that stimulate innovations for local development challenges and creating local skilled jobs.

Overview of Projects (To date)

UK
Central Coordination & alignment with UK objectives

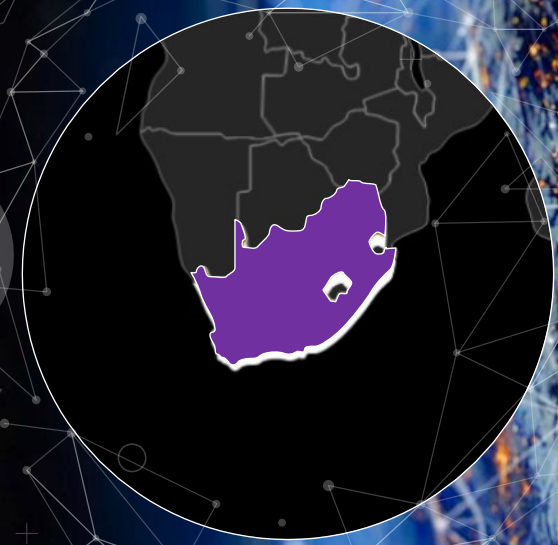
Nigeria
- *Improving the prosecution of cybercrime in Nigeria*
- *Defending Nigeria's critical infrastructure from cyber threats*
- *Cyber Hygiene Benchmarking*

Kenya
- *Improving the prosecution of cyber crime in Kenya*
- *Raising awareness of cybersecurity across Kenya*

South Africa
- *Improving the prosecution of cyber crime in South Africa*
- *Providing a cyber career for underprivileged students*

UKaid
from the British people

South Africa



Improving the prosecution of cyber crime in South Africa

Why are we delivering this work?

On 26th May 2021, the South African President signed the Cybercrimes Act 19 into Law. The bill is intended to act as a deterrent for cyber-crime and criminals. While the South African Police Service (SAPS) is empowered to act against cybercrimes, a lack of cybercrime training and awareness of the newly implemented Cybercrimes Act may cause challenges to their ability to investigate cybercrime and bring criminals to justice.

Using local suppliers, the project aims to ensure that members of the South African Police Service (SAPS) receive training in aspects relating to the detection, prevention, and investigation of cybercrimes. The project aims to develop and implement accredited training programmes for members of the South African Police Service (SAPS) primarily involved with the detection, prevention, and investigation of cybercrimes. The project will assist the South African Police service in meeting requirements defined in Chapter 8, Section 55 of The South African Cybercrimes Act 19 of 2022. The project will aim to create cybercrime material and workshops that can be utilised by the SAPS to deliver training to 10,000 staff.

SA1

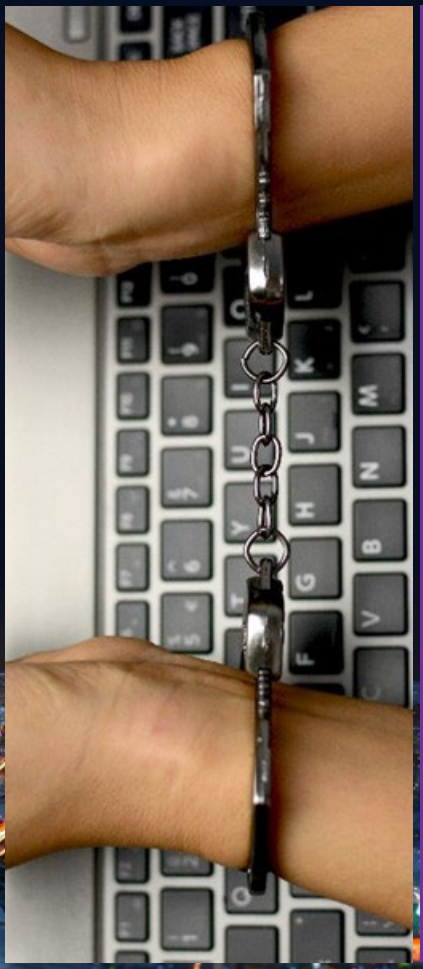
Cybercrime training for the South African Police Service (SAPS)

Who are we working with?

- South African Police Service (SAPS)
- KPMG South Africa
- Key delivery partner is VizStrat Solutions, a local supplier specialised in cyber crime training

What is being delivered?

- Analysis will be conducted on SAPS knowledge gaps and training needs to update the SAPS cybercrime needs analysis and previously defined training framework
- Two-week practical cybercrime workshop
- Awareness session to SAPS leadership to aid senior SAPS stakeholders in understanding the threats and opportunities that arise within cyber security
- Draft international protocols guidelines that will assist with the provision as well as request of electronic evidence/articles across the borders of the Republic
- Delivery of train the trainer sessions to SAPS recruits on Cybercrime Act



Providing a cyber career for underprivileged students

Why are we delivering this work?

An increasing number of companies are trying to implement internship programmes to resolve their issue of IT Skill shortfalls. However candidates coming out of the South African education system do not have the IT and soft skills foundation required to be successful IT interns. This results in few interns being appointed into permanent positions.

This project will help bridge the cyber skills gap and aid students to integrate successfully into a professional working environment in Cape Town. It will equip candidates with the skills and tools to design a sustainable career (that will positively impact their home-life and community); and will also provide a pool of well-equipped and skilled candidates that match what companies require.

This will result in an increased digital and cyber knowledge of young candidates that helps bridge the skills gap and increases employment in underprivileged areas. This in turn will provide businesses with trained resource to better equip their cybersecurity teams, increasing their capabilities to defend against cyber threats.

SA2

Cyber training for underprivileged school leavers

Who are we working with?

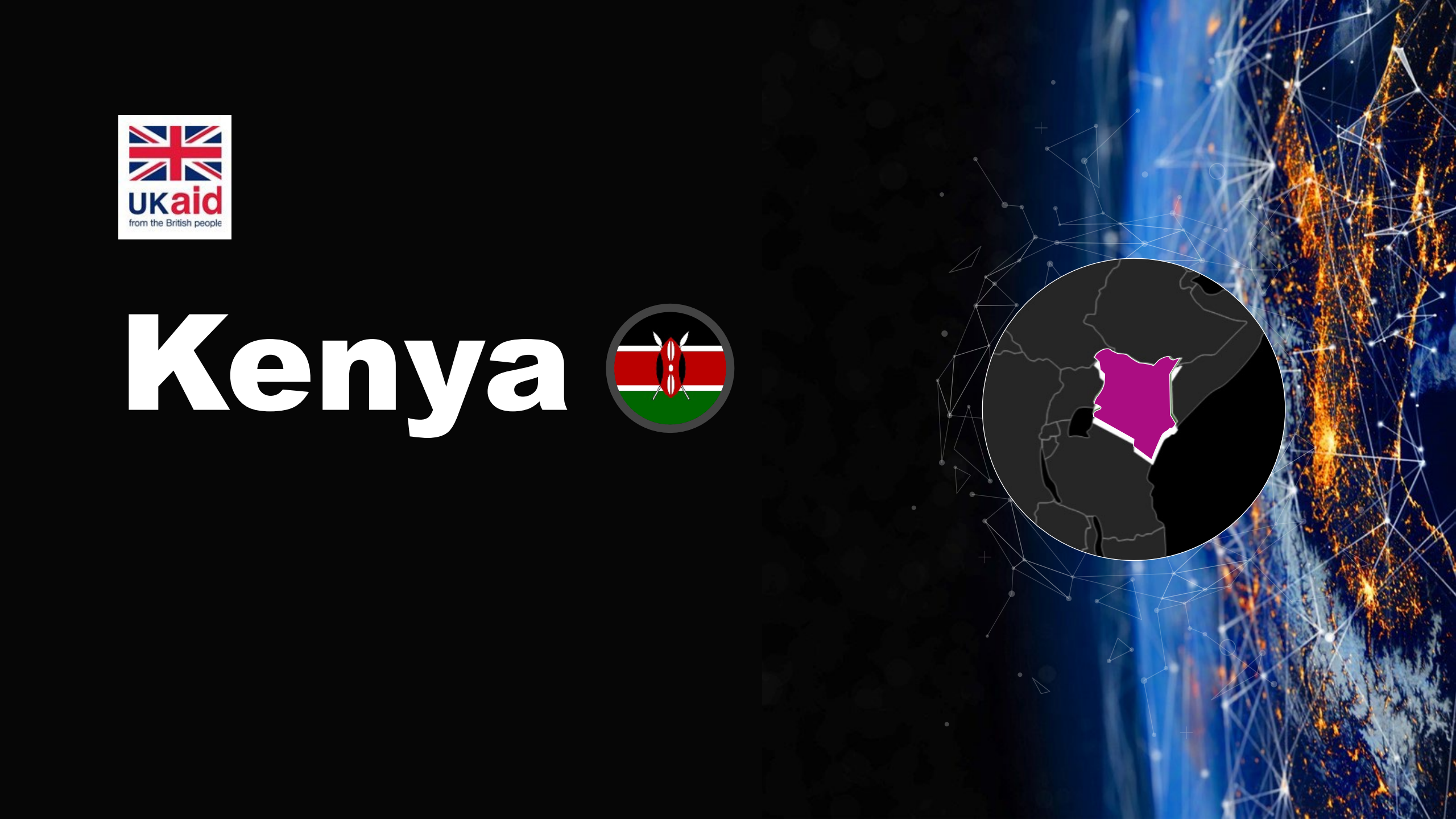
- KPMG South Africa
- MiDO Academy
- KnowBe4

What is being delivered?

- MiDO Cyber Intern Readiness Programme will support 20 school leavers over 12 months. Participants will gain valuable digital, cyber and business skills to allow them to succeed in the Cyber and IT market.
- The curriculum is develop a well-rounded skill set that prepares students for a career in IT and enhances overall employability and adaptability.
- The blended curriculum is structured to cover foundational digital skills e.g. basic computer literacy, digital literacy, and communications skills, as well as cyber-specific technical skills covering CompTIA Security+ SYO-601, CompTIA Network+, and CompTIA A+ certifications.

UKaid
from the British people

Kenya



Improving the prosecution of cyber crime in Kenya

Why are we delivering this work?

Cybercrime is a prevalent issue in Kenya, and the 2022 National Cybersecurity Strategy has identified the prevention of cybercrimes as a core priority for the Kenyan government over the coming years. Kenya has adapted various policies, operational and administrative initiatives to improve national cybersecurity. In an effort to strengthen the cybersecurity legislative framework, the Computer Misuse and Cybercrimes Act was enacted in 2018, which in turn established the National Computer and Cybercrimes Coordination Committee (NC4) to coordinate cybersecurity efforts. This legislation is currently the overarching law for the protection of Critical Information Infrastructures and management of cybercrime in Kenya. Whilst the mitigation of cybercrimes is a core priority of the legislation, the level of cybercrime in Kenya continues to be high. It is therefore paramount that law enforcement have sufficient knowledge and understanding of cybersecurity, particularly in domains pertinent to digital crimes, to ensure that appropriate action can be taken to enable cybercrimes to be successfully investigated and prosecuted.

The project will deliver training for a selected cohort of Judges, Prosecutors and Law Enforcement officers to provide them with the content and skills required to strengthen their capacity to prosecute cybercrimes. This aims to increase successful prosecutions and act as a deterrent for cybercrime.

KE1

Digital forensics and evidence handling training for Judges, Prosecutors and Specialist Law Enforcement officers

Who are we working with?

- Directorate of Criminal Investigations (DCI) Kenya
- Office of the Director of Public Prosecutions (ODPP) Kenya
- Key delivery partners are UK suppliers, PGI and CYSIAM

What is being delivered?

- A tailored Digital Forensics and Digital Evidence Handling training course
- Two five-day Digital Forensics training workshops delivered to the Department for Criminal Investigations (specialist law enforcement officers)
- Two two-day Digital Evidence Handling Workshops for Judges and Prosecutors
- A cyber resilience scenario via the 4D Insight simulation platform for Judges and Prosecutors

Raising awareness of cybersecurity across Kenya

Why are we delivering this work?

In August 2022, the Government of Kenya (GoK) published its second National Cybersecurity Strategy, with the ultimate purpose of building a secure, resilient and trusted cyberspace for the people of Kenya through a coordinated approach, whilst capitalising on the benefits of a digital economy. The strategy is intended to serve as a roadmap to address new challenges and emerging threats in the cybersecurity domain.

Statistics indicate that the number of cyber threats detected in Kenya has significantly increased in the last 3 years – the strategy highlights that over 140 million cyber threats were detected in July – September 2021 as compared to 4,589 in the same period in 2017. Despite a growing number of incidents, governance of cyberspace in Kenya has remained largely uncoordinated with little clear structure. While Kenya has enacted various policies and laws, regular review and update is necessary in order to effectively address emerging risks and threats. As a result, the GoK has identified cybersecurity as a national economic and security challenge and priority which the strategy seeks to address.

SMEs are the driving force of Kenya's economy, contributing up to 40% of Kenya's GDP. Their importance is underlined in the Kenya Vision 2030 as they offer the most potential for GDP growth and employment prospects. However, limited cyber security guidance and standards for SMEs currently exists.

KE2

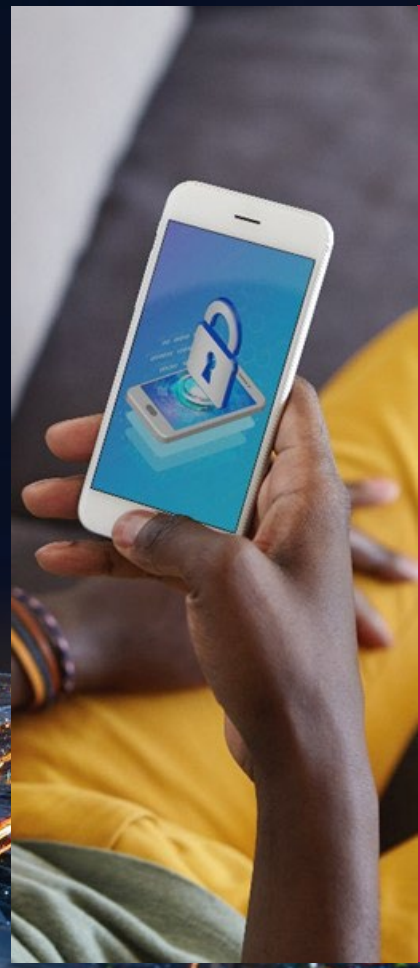
Educating Kenyan citizens on how to protect themselves against cyber harms

Who are we working with?

- Communications Authority (CA), Government of Kenya
- Computer and Cybercrimes Coordination Committee (NC4)
- KICTANET, Kenyan ICT Think Tank
- Global Cyber Alliance

What is being delivered?

- A cyber security toolkit tailored to suit SMEs
- A toolkit communications plan to spread the message widely and maximise toolkit use
- An SME 'Train the Trainer' programme so trainers can spread the message on cyber hygiene and sustain the benefits of the toolkit
- A cyber hygiene awareness campaign aligned to Government of Kenya priorities, designed to raise public awareness of the Government's Transformational Digital Agenda (GoTDA) which aims to promote safe digital access for the most vulnerable groups across Kenya



UKaid
from the British people

Nigeria

Improving the prosecution of cybercrime in Nigeria

Why are we delivering this work?

Given the size of the challenge, the Nigerian Police Force (NPF) currently have insufficient ability to investigate cybercrime and bring criminals to justice. This is in part caused by the shortage of digital forensics capability as well as a lack of defined processes to report and manage incidents. There are also systemic issues amongst Judges and Prosecutors which reduces the likelihood that cybercrimes can be successfully prosecuted.

Currently there is a limited number of individuals with sufficient knowledge of digital forensics and critical evidence required for cybercrime cases.

The project aims to train a select cohort of National Judicial Institute (NJI) Judges, Prosecutors and Law Enforcement. This will provide them with the content and skills required to strengthen their capacity to prosecute cybercrimes. This will increase the number of successful prosecutions and act as a deterrent for cybercrime.

NG1

Digital forensics and evidence handling training for Judges, Prosecutors and Specialist Law Enforcement officers

Who are we working with?

- Nigerian Police Force (Cybercrime Unit)
- National Judicial Institute (NJI)
- Federal Ministry of Justice (FMoJ)
- Office of the National Security Advisor (ONSA)
- UK delivery partners PGI and CYSIAM

What is being delivered?

- A tailored Digital Forensics and Digital Evidence Handling training course
- 5 Day Digital Forensics training workshop to the Police Cybercrime Unit (specialist law enforcement officers)
- Two-day Digital Evidence Handling Workshop for Judges and Prosecutors
- A cyber resilience scenario via the 4D Insight simulation platform for Judges and Prosecutors

Defending Nigeria's critical infrastructure from cyber threats

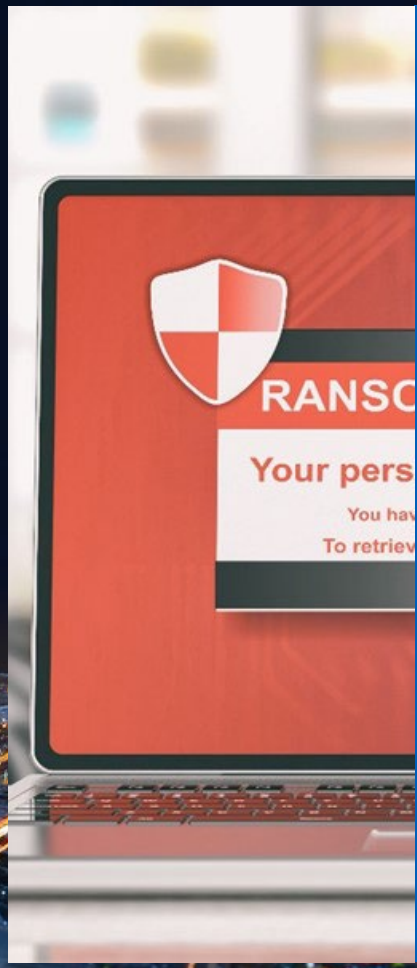
Why are we delivering this work?

A resilient Critical National Information Infrastructure (CNII) is key to societal resilience to threats and harms. It underpins the provision of many services to citizens. Failure of infrastructure can lead to many harms including physical, social and economic. By increasing Nigeria's capability to regulate CNII, this should improve resilience across the wider CNII and therefore reduce harms.

This project aims to increase Nigeria's ability to protect its Critical National Information Infrastructure (CNII) by establishing CNII cyber maturity governance and by building the capacity of Nigeria's CNII regulators and operators to respond to CNII incidents. This will improve the resilience of Nigeria's critical national information infrastructure thereby reducing harms to the vulnerable.

NG2

Critical National Infrastructure Protection



Who are we working with?

- Office of the National Security Advisor (ONSA)
- Nigeria CNII Regulators
- Nigeria CNII Operators
- KMPG Nigeria

What is being delivered?

- A tabletop simulation of a major cyber-attack on Nigerian Telco sector to understand current state incident response. Post incident report to provide recommendations to assist with preparation for a live event.
- A CNII Cyber Maturity Review Policy.
- A CNII Cyber Maturity Framework and guidelines for applying it effectively.
- CNII Cyber Maturity Policy and Framework training for ONSA and chosen Regulators.
- A pilot of a CNII Cyber Maturity review for a selected operator within the Telecommunications sector. This will act as a model for future assessments conducted by Independent Reviewers, allowing CNII operators and ONSA to autonomously review CNII maturity.

Strengthening the cybercrime defences of Nigerian businesses

Why are we delivering this work?

In today's rapidly moving online threat landscape, it is more important than ever for organisations to have a cyber hygiene routine which protects them from everyday breaches from opportunistic cyber criminals. When good cyber hygiene is properly integrated into an organisation, with the right behaviours and daily routines, organisations are able to protect themselves against the most common cyber attacks. This project scope and aims are developed in alignment with requests of support from the Federal Government of Nigeria.

The project aims to assess the current level of cyber hygiene awareness across Nigeria. The project will identify a suggested scope for a national cyber benchmark. It also aims to understand the challenges, benefits and considerations of implementing such a benchmark, through a government backed scheme in Nigeria.

The Federal Government of Nigeria (FGN) aims to determine the right scope for a cyber certification scheme for organisations (including Small, Medium and Micro Enterprise SMMEs) to certify their level of cyber hygiene. For instance, FGN would like to explore the possibility to develop a scheme similar to the UK NCSC Cyber Essentials and Cyber Essential plus, which provides organisations with cyber hygiene practices to protect themselves and their customers and ultimately citizens from cyber attacks. This also helps to demonstrate organisations' commitment to cyber security.

NGT3

Cyber Hygiene Benchmarking

Who are we working with?

- Office of the National Security Advisor (ONSA)
- KMPG Nigeria

What is being delivered?

- An online survey to collect information on baseline knowledge of cyber security in Nigeria
- A summary report assessing the current level of cyber hygiene awareness in Nigeria.
- A feasibility study providing considerations to design and develop a cyber benchmark requirement scheme in Nigeria.
- A community workshop to present the findings of the report back to stakeholders who engaged with the work.