UK Government's Global Digital Access Programme (DAP) - Pillar 2 Trust & Resilience Project summaries

Pillar 2: Protecting the most vulnerable from cyber crime

Closedown 18 November 2022 v9

The UK Government's Global Digital Access Programme

Protecting the most vulnerable 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 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.

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.

During a two-year period from October 2020, the FCDO, through its Digital Access Programme (DAP) – Pillar 2 Trust & Resilience, has implemented 16 projects to improve cyber capability and reduce harm in five countries – Brazil, Kenya, Nigeria, South Africa and Indonesia.

HM Government

UKaid from the British people

Backed by £10 million of UK aid from the Conflict, Stability and Security Fund, the DAP Pillar 2 is the UK government's largest ever overseas cyber capacity building project. These projects 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'.

The 16 projects included helping Nigerian law enforcement to develop its digital forensic capability; enabling Kenya's government to better protect its citizens' data; assisting the delivery of cybersecurity education in Brazil's schools; developing cybersecurity regulation for Indonesia's banking sector; and improving the South African police's ability to prosecute cyber criminals.

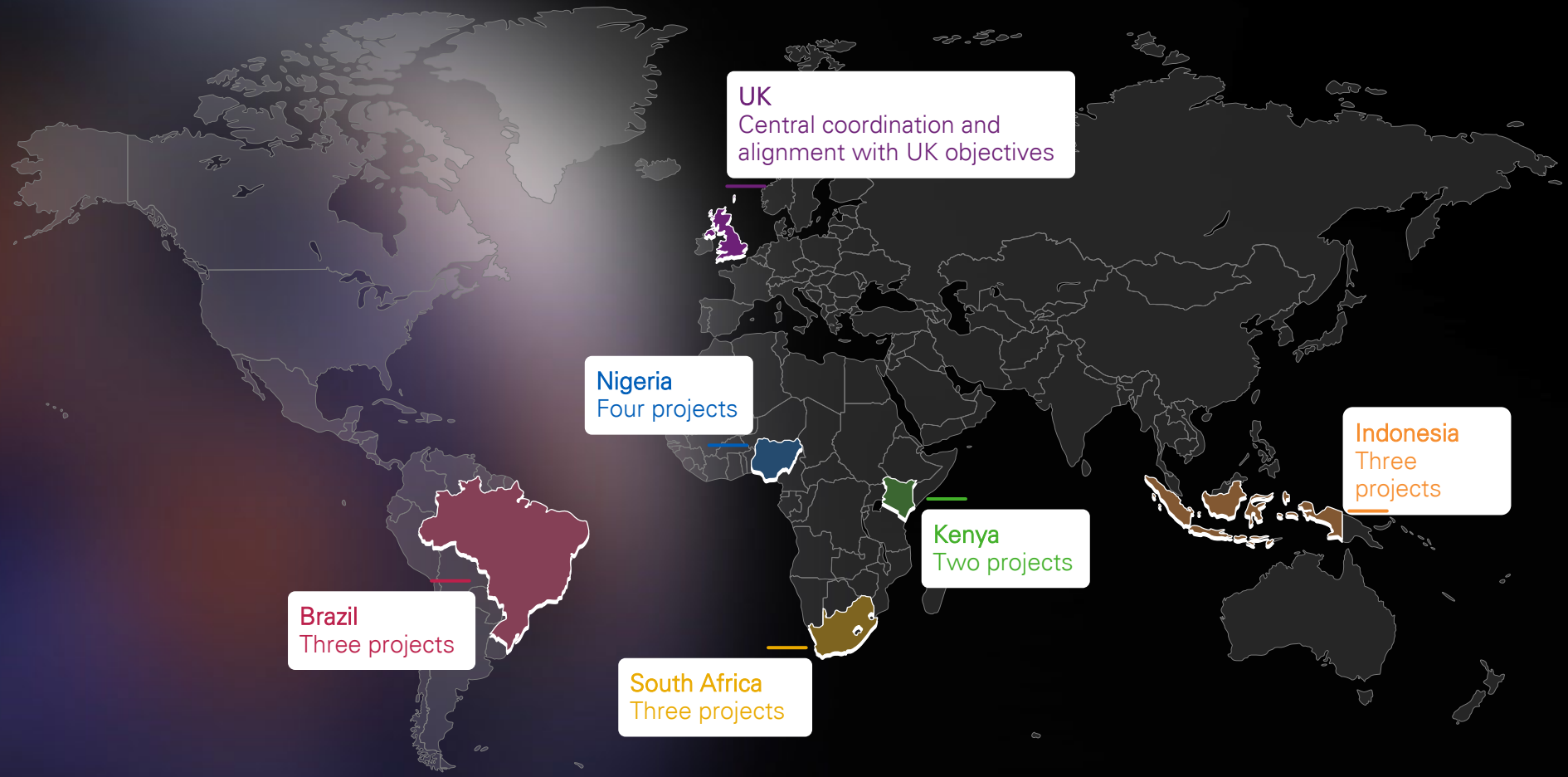
In each instance, the ambition was to build sustained capability that allowed national partner governments to better protect their citizens online or to defend their critical national infrastructure from cyber threats.

Ultimately, the DAP built on the UK's cybersecurity experience to help these countries improve safe digital access, bringing excluded populations into the digital economy, reducing poverty and stimulating inclusive economic growth.

The Digital Access Programme is a UK Government Programme which catalyses inclusive, affordable, safe and secure digital access for underserved populations in these countries; and promotes digital ecosystems that stimulate innovations for local development challenges and create local skilled jobs. It has three "pillars", covering cybersecurity; models and enablers for digital access; and stimulating local digital economies.

Document Classification: Official

Overview of Projects (To date)



Document Classification: Official

Who's benefitted from the programme

Brazil

- Users of e-government services
- Teachers and school children
- Ministry of Education (MEC)
- State Secretariats for;
- Pernambuco;
- Bahia; and
- Distrito Federal.
- Institutional Security Cabinet of the President of the Republic (GSI-PR)
- Social Communication Office to the Special Advisory Team for Information Security (AssESI – GSI)
- Special Secretariat for Social Communication (SECOM)
- Brazil's Special Secretariat of De-bureaucratisation, Management, and Digital Government (SGD) part of the Brazilian Ministry of Economy

South Africa

- South African Police Service (SAPS), incl. Serial and Electronic Crimes Unit (SECI)
- Directorate for Priority Crime Investigation (DPCI)
- SMMEs (small micro medium enterprises), including women-led SMMEs, Incubator Hubs and rural communities.
- Cybersecurity Hub and National Computer Security Incident Response Team (CSHUB-CSIRT) from the Department of Communications and Digital Technologies (DCDT)
- Small Enterprise Development Agency (SEDA)
- Sector CSIRTs, including South African Banking Risk Information Centre (SABRIC), Communications and Risk Information Centre (COMRIC), Internet Service Providers' Association (ISPA) and the Association for Savings and Investment South Africa (ASISA)
- South African Reserve Bank (SARB)
- Various private organisations from Banking, Insurance, Telecommunications and High Education sector

Nigeria

- Nigeria's Office of the National Security Advisor (ONSA)
- Nigerian Law Enforcement
- National Judicial Institute (NJI)
- Federal Ministry of
- Development Agency of Nigeria (SMEDAN)
- Critical National Infrastructure providers including the Financial Sector and Telecommunications
- National Information Technology Development Agency (NITDA)
- Groups vulnerable to cybercrime (children, women SMEs)
- Nigerian Communications Commission (NCC)
- Communications and Digital Economy
- Office for ICT Innovation and Entrepreneurship (OIIE)

Indonesia

- National Cyber and Cryptography Agency (BSSN)
- Ministry of Health (MoH)
- Financial Conduct Authority (OJK)
- Indonesian cybersecurity professionals
- Ministry of Communication and Information Technology (KOMINFO)
- Indonesian healthcare institutions and financial institutions
- Health Social Security Agency
- Ministry of Energy and Mineral Resources
- Ministry of Transportation
- Bank of Indonesia
- Ministry of Industry
- Ministry of Communication and Information
- Ministry of Defence
- Ministry of Agriculture

Kenya

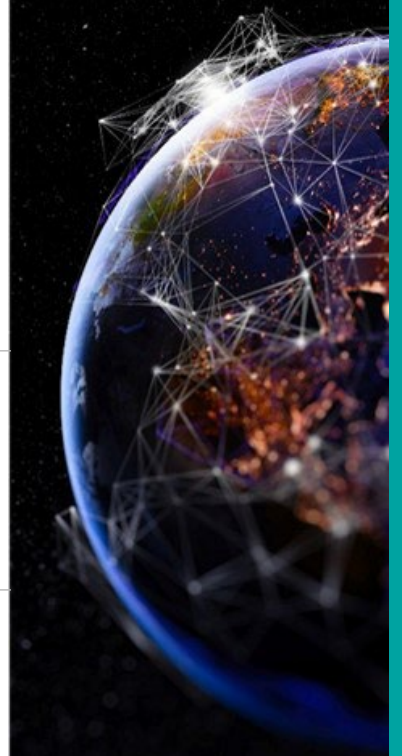
- Information and Communication Technology Authority (ICTA)
- Office of the Data Protection Officer Kenya (ODPC)
- Communications Authority Kenya
- Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) and other international donors

Document Classification: Official

Who made it happen - The Delivery Team – FCDO & KPMG supported by:

HM Government

UKaid from the British people



VizStrat Solutions

Torchlight

Strathmore University

TONICA.AG Lead your conversation

CYBER CAPACITY UNIT

orange Ink

CS2

SERIANU

Safer net

INFORMATION TECHNOLOGY COURSES

WomHub CONNECT | CULTIVATE | CONVERT

Home Office

Queen Mary University of London

Katagonia

GLOBAL CYBER ALLIANCE

CYSIAM

cybersafe. FOUNDATION

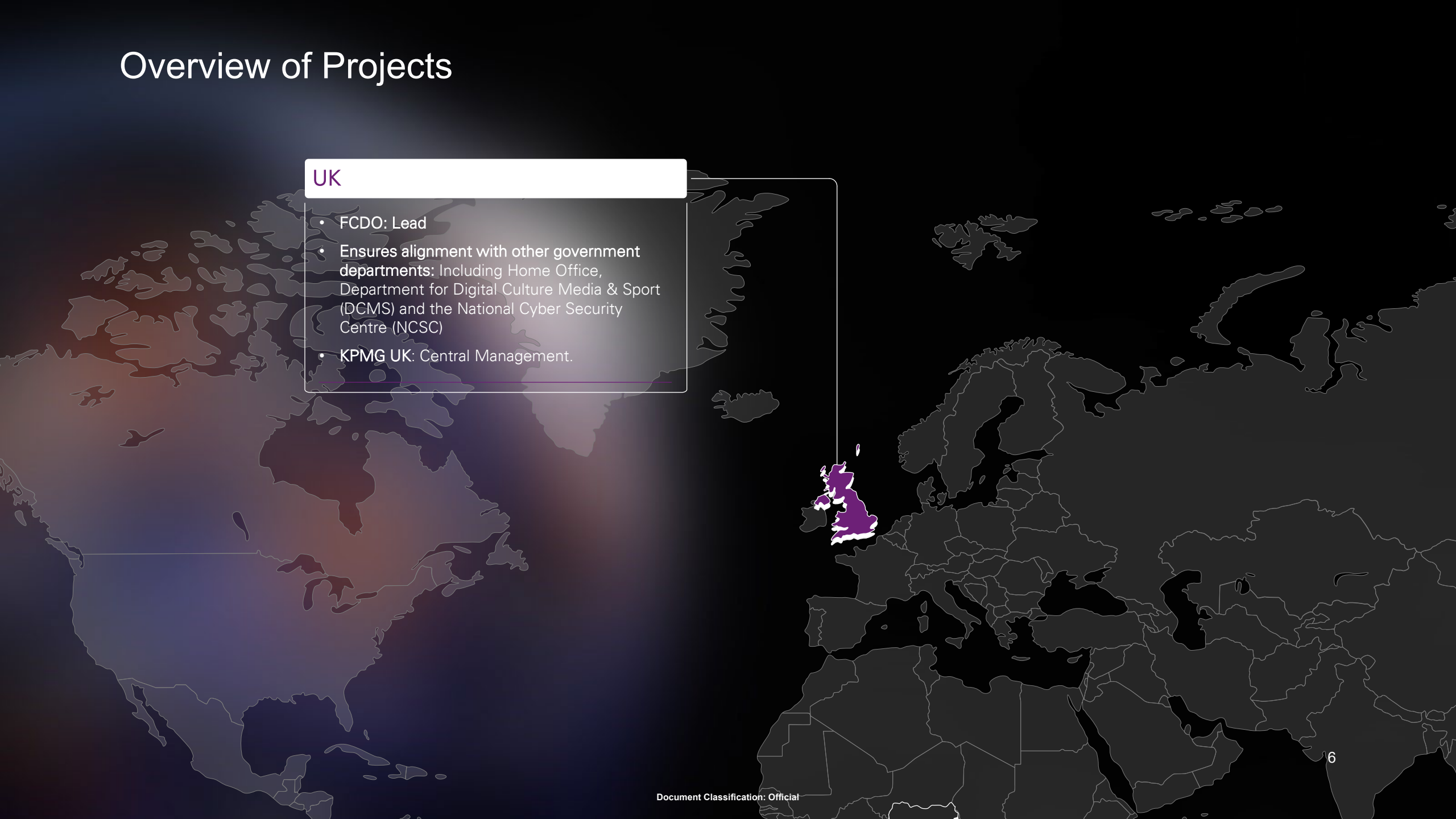
Social Development Direct

CHATHAM HOUSE

Overview of Projects

UK

- FCDO: Lead
- **Ensures alignment with other government departments:** Including Home Office, Department for Digital Culture Media & Sport (DCMS) and the National Cyber Security Centre (NCSC)
- **KPMG UK**: Central Management.



Document Classification: Official

Overview of Projects (To date)

South Africa Projects

- **Cybercrime Awareness & Skills for Law Enforcement** – Providing specialist cybercrime investigation skills
- **Cybersecurity and Data Protection Toolkit for SMEs –** Strengthening the cybercrime defences of South African small businesses
- **Training for Incident Response Teams (CSIRTs)** – Improving South Africa's response to national cyber threats

Document Classification: Official

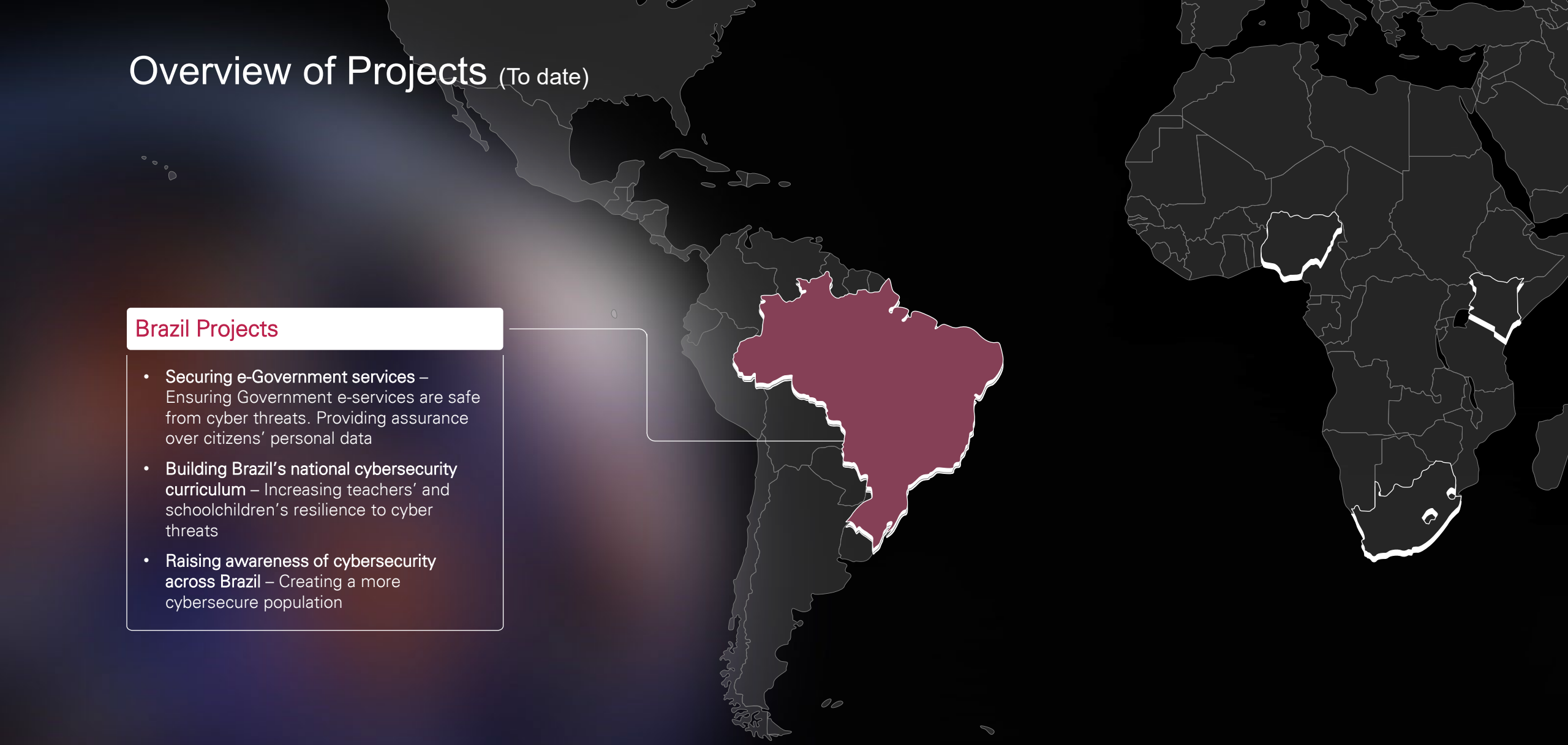
Overview of Projects (To date)

Indonesia Projects

- **Developing cybersecurity regulation for the banking sector** – Better protecting citizens' sensitive banking data
- **Improving Telemedicine cybersecurity** – Securing a vital healthcare platform and increasing patients' trust
- **Government Cyber Security Training** – Delivering vital cyber skills at the heart of government

Document Classification: Official

Overview of Projects (To date)

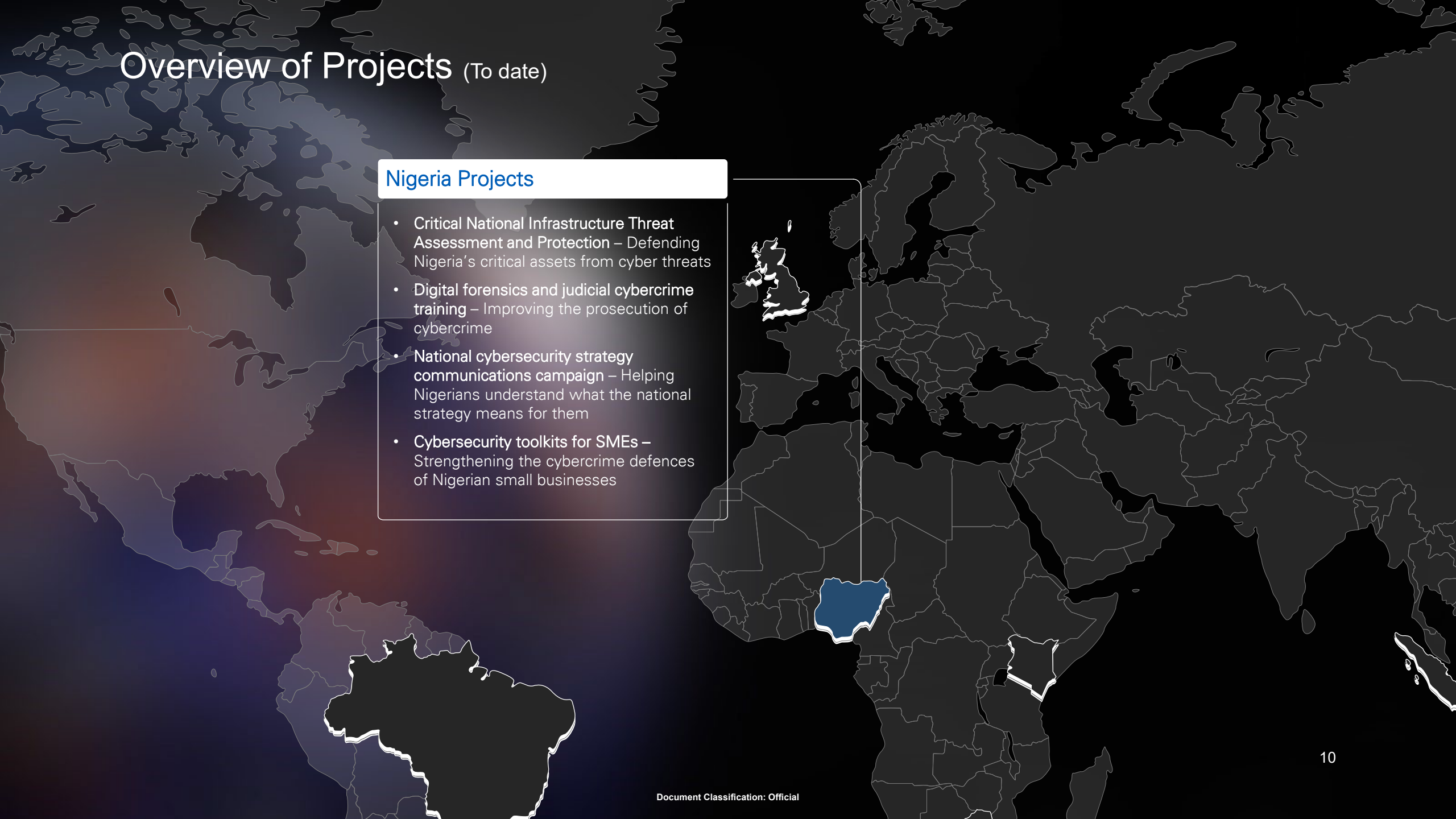


Brazil Projects

- **Securing e-Government services** – Ensuring Government e-services are safe from cyber threats. Providing assurance over citizens' personal data
- **Building Brazil's national cybersecurity curriculum** – Increasing teachers' and schoolchildren's resilience to cyber threats
- **Raising awareness of cybersecurity across Brazil** – Creating a more cybersecure population

Document Classification: Official

Overview of Projects (To date)

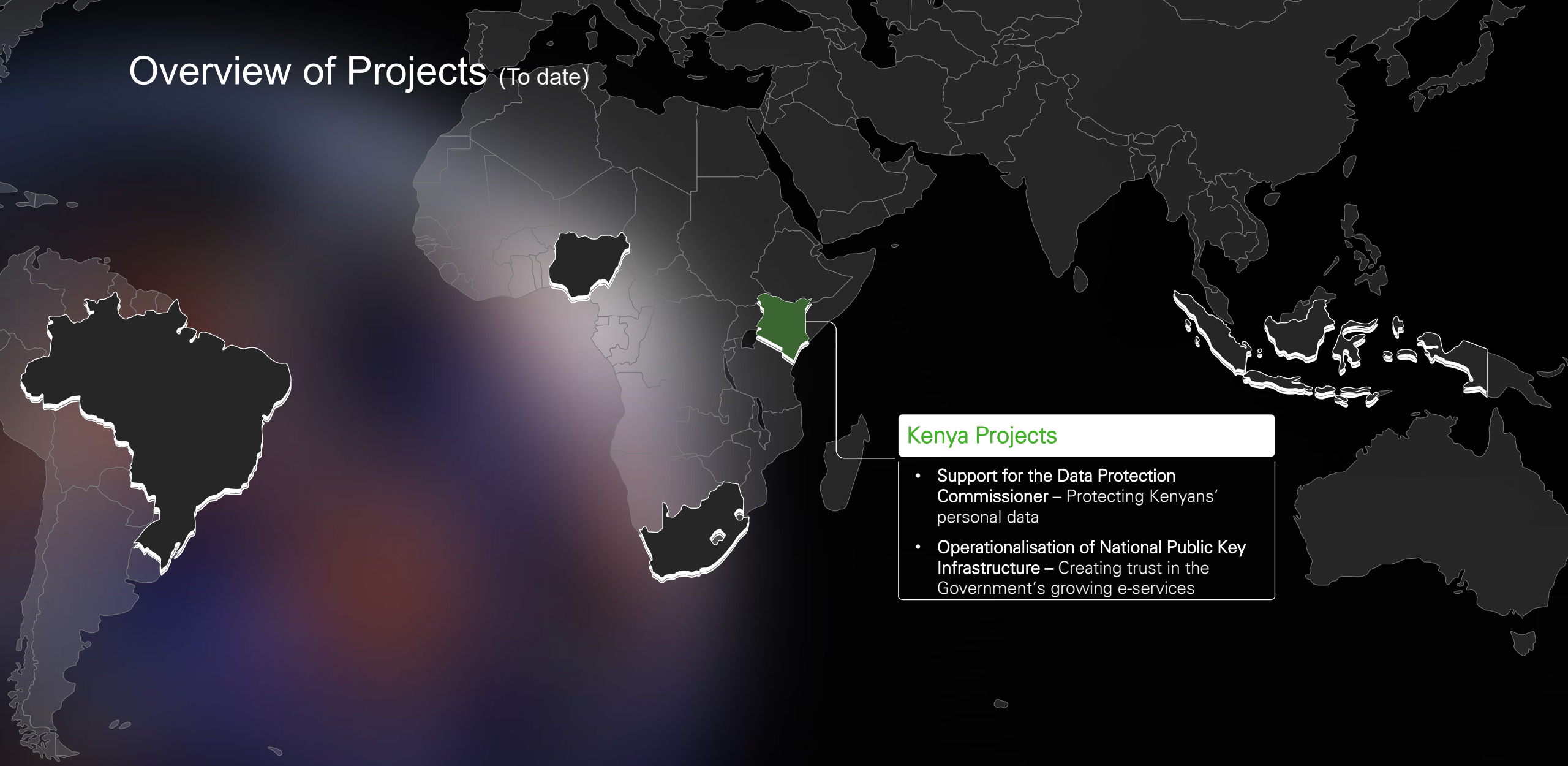


Nigeria Projects

- **Critical National Infrastructure Threat Assessment and Protection** – Defending Nigeria's critical assets from cyber threats
- **Digital forensics and judicial cybercrime training** – Improving the prosecution of cybercrime
- **National cybersecurity strategy communications campaign** – Helping Nigerians understand what the national strategy means for them
- **Cybersecurity toolkits for SMEs** – Strengthening the cybercrime defences of Nigerian small businesses

Document Classification: Official

Overview of Projects (To date)



Kenya Projects

- **Support for the Data Protection Commissioner** – Protecting Kenyans' personal data
- **Operationalisation of National Public Key Infrastructure –** Creating trust in the Government's growing e-services

Document Classification: Official

South Africa

Cybercrime awareness and skills for law enforcement

Why did we deliver this work?

In South Africa, the responsibility for pursuing national priority crimes – such as organised crime, corruption and serious commercial crime - rests with the Directorate for Priority Crime Investigations (DPCI).

As with the broader South African Police Service (SAPS), the DPCI's resources are stretched thin. there is a significant backlog of cases involving cybercrime, or where there is a need to examine digital evidence.

This project was therefore designed to improve the specialist cybercrime investigation skills and digital forensic capabilities of selected DPCI officers. It would also deliver basic cyber awareness training to all SAPS officers. This training would explore what cybercrime is and how best to respond to, and escalate, reports of cybercrime. It was also designed to ensure that officers were more sensitive to reports of gender-based online violence.

The first burst of training activity was undertaken with specialist DPCI cybercrime officers in October and November 2021. This explored open source intelligence, the tools and techniques for making best use of it and the related legislation that officers need to be aware of.

The project's focus then turned to working with the SAPS HR Development unit to develop a cybercrime training curriculum. Providing entry-level training as well as more specialist instruction, this covered topics from basic digital forensics through to open-source intelligence. An accompanying train-the-trainer course was also created.

The project team helped develop the Standard Operating Procedures for how officers should use the powers available to them within the Cybercrimes Act. The team also shared insights from the UK police, regarding the lessons learned from creating an app that advises officers of the procedures and protocols to be observed at a digital crime scene.

SA1

Providing specialist cybercrime investigation skills

Who did we work with?

- The South African Police Service (SAPS), including its Directorate for Priority Crime Investigation (DPCI)
- VizStrat Solutions, a local supplier chaired by Advocate Jacqueline Fick, an expert in cybercrime legislation and cyber risks and threats
- CYSIAM, a UK supplier specialising in digital forensics and open-source intelligence training

What was delivered?

- A two-day workshop, jointly led by a local think tank, exploring the scope of the Cybercrimes Act and its implementation challenges.
- A one-day training course on the Cybercrimes Act, aimed at all 150,950 SAPS officers and new recruits, and a two-day train-the-trainer course. This training was delivered to over 2,300 police officers who reported an increase of their knowledge of 30% to 62% across all areas.
- A policy and framework for digital forensics and open source intelligence training. Following the specialist training, capability increased 23 times meaning the SAPS now have an abundance of officers able to deliver in these areas.
- Basic and specialist training activities and manuals, covering the detection, prevention and investigation of cybercrimes.
- The development of Standard Operating Procedures for using the powers in the Cybercrimes Act, guided by a public consultation exercise.

Document Classification: Official

Cybersecurity and data protection toolkits for SMMEs

Why did we deliver this work?

Small, medium and micro-sized enterprises (SMMEs) play a crucial role in the South African economy. They account for 98% of South African businesses, employ 50-60% of the total workforce and contribute 39% of GDP.

Growing numbers of these businesses have gravitated towards trading online in recent years, exposing them to cyber risks that their owners have never encountered before. Many have neither the knowledge nor the funds to implement the controls and procedures they need to protect their businesses.

In addition, the introduction of the Protection of Personal Information Act has placed further pressure on these businesses to effectively protect personal data online. Failure to do so can result in a hefty fine.

Keen to provide free, easily accessible training and resources, the project team partnered with the Global Cyber Alliance to develop an online cybersecurity and data protection toolkit.

Developing and launching the toolkit was the first step. The team then embarked on a comprehensive campaign to encourage SMEs to use the toolkit, including a cyber roadshow, a communications campaign and a train-the-trainer programme. This raised awareness of the toolkit and trained others in how to deploy it.

Throughout delivery, the team was able to tap into the networks of partners like WomHub, SEDA and Launch League to distribute the toolkit and raise awareness of the issues it covered. As a result, training was delivered to over 600 business owners, trainers and facilitators in just nine months.

SA4

Strengthening the cybercrime defences of South African small businesses

Who did we work with?

- The Cybersecurity Hub and National Computer Security Incident Response Team (CSIRT) from the Department of Communications and Digital Technologies
- The Information Regulator (South Africa)
- WomHub, a boutique pan-African incubator for female founders in STEM
- The Small Enterprise Development Agency (SEDA)

What was delivered?

- Cybersecurity and data protection toolkits and basic cyber hygiene training for South African SMMEs, aligned to the UK Cyber Essentials scheme and international good practice, underpinned by regulation and incentives.
- A series of webinars and virtual roadshows to disseminate the toolkits and expand SMMEs' knowledge of high priority cybersecurity topics. Over 400 SMME's attended with 100% rating the toolkits 'Very Useful' or 'Useful'.
- A train-the-trainer programme for incubator hub managers, delivered in partnership with SEDA.
- A nationwide communications campaign, featuring radio ads and op-ed commentary, to disseminate the toolkits to the wider South African community and to raise awareness of the importance of good cyber hygiene. Since rollout, these toolkits have received 6,359 online hits.

Document Classification: Official

Training for Incident Response Teams (CSIRTs)

Why did we deliver this work?

Assessments of South Africa's cyber maturity identified incident response capability as a critical area for development.

The basics are all in place - a Cybersecurity Hub, which is the national Computer Security Incident Response Team (CSIRT) for the private sector; another government CSIRT which serves government departments; and several industry sector equivalents. This project was therefore designed to build on that existing infrastructure by improving the capability for coordinating a national cyber incident response.

Three simulation events were delivered in late 2021, testing different sectors' responses to a cyber incident. This revealed strengths and weaknesses in terms of leadership, coordination and communication. Every decision was analysed to determine what worked, what didn't and how the response protocols might need to be amended.

The outputs of this were explored in a face-to-face incident response day in February 2022; considering lessons learned, recommended actions, contingency planning and the articulation of roles and responsibilities. Recommended next steps were provided to the South African government in March 2022.

Further work was subsequently undertaken to raise awareness of the challenges involved in delivering a successful incident response. Training and a free webinar were made available, targeting all sector CSIRTs and any other interested parties.

SA10

Improving South Africa's response to national cyber threats

Who did we work with?

- The Cybersecurity Hub and National CSIRT from the Department of Communications and Digital Technologies
- Sector CSIRTs, the South African Reserve Bank (SARB) and the South African Police Service (SAPS)
- CYSIAM, a UK CREST-registered and accredited critical security incident response company

What was delivered?

- Three scenario-based incident response exercises involving the national and sector CSIRTs, followed up with post-exercise reports and a recommendations roadmap. The training was delivered to over 100 participants covering Government (CSHUB-CSIRT), sector CSIRTs (incl. FS, Telco, Higher education and CSIR) and regulators (SARB, PASA).
- A focused workshop where recommendations from the incident response simulations were presented and discussed with the CSIRTs and other stakeholders, including SARB and SAPS.
- Training on how to design and deliver future incident response simulation exercises.
- A free advice webinar on the challenges of responding appropriately to a cyber incident.

Document Classification: Official

Indonesia

Developing cybersecurity regulation for the banking sector

Why did we deliver this work?

Prompted by Indonesia's national cyber security strategy, the country's Financial Services Authority (OJK) is currently working on new legislation to improve information security across the country's banking sector.

Within this project, the DAP team worked closely with OJK to refine a consultation document. This articulated the stringent data protection and cybersecurity standards that banks would need to adhere to and the specific controls they would be expected to have in place.

To better understand the impact of the proposed legislation, a test exercise was initiated with eight banks during the spring of 2022. The eight were selected as a representative cross-section of the Indonesian banking sector, spanning different customer demographics, geographical coverage and levels of cyber maturity.

Each bank was assessed against the cyber regulations outlined within the proposed legislation. This presented a handy test of the new regulations, the banks' current levels of preparedness and the ability of OJK staff to undertake these security reviews.

The recommendations that emerged from this pilot activity were used to help refine the new regulatory framework, which is expected to become law by the end of 2022. A final piece of work was subsequently undertaken to determine what further training OJK staff might need in order to perform these assessments annually, across all the country's banks.

IN1

Better protecting citizens' sensitive banking data

Who did we work with?

- KPMG Indonesia
- Indonesia's Financial Services Authority (OJK)
- Eight Indonesian banks

What was delivered?

- A framework to help financial institutions assess their current levels of IT risk.
- A cyber maturity framework, including detailed control requirements for financial institutions wanting to assess their current cyber maturity level.
- Pilot testing of the newly developed cyber maturity assessment was delivered to 8 banks. This protects some 180 million citizens banking data to date.
- Recommendations for refining the framework, based on feedback from the pilot activity.
- A training needs analysis, leading to recommendations for further OJK staff training.

Document Classification: Official

Improving telemedicine cybersecurity

Why did we deliver this work?

Indonesia has the world's fourth largest population (over 270 million), of whom just under half are dispersed across more than 17,000 islands. For them, physical access to healthcare professionals can prove challenging, making telemedicine an important part of the country's health system.

With rural and vulnerable communities in mind, the Indonesian government has, for some time, been encouraging the use of telemedicine for both online consultations and treatments. In the 12 months to March 2020, the usage of Indonesian telemedicine apps doubled. Covid accelerated that growth still further as the country's health system came under pressure.

As demand for telemedicine grew, so did the urgency for wanting to make the telemedicine platforms secure. This project was designed, in collaboration with our UK consortium member Cyber Capacity Unit, to improve those platforms' cyber defences, reassuring Indonesians that their data was secure, increasing healthcare coverage in rural areas and reducing the strain on healthcare facilities.

However, what began as a project focused on telemedicine quickly grew to consider the healthcare sector as a whole, with the Ministry of Health seizing the opportunity to improve its cybersecurity posture more broadly across its entire portfolio.

This work led to the establishment of a new information security framework that provides a baseline set of cybersecurity controls. This was tested across five healthcare facilities, assessing the controls they had in place around patient data.

Guidance was provided on how to undertake data privacy impact assessments and a cyberattack simulation was conducted for the ministry's new Computer Security Incident Response Team (CSIRT), leading to the creation of a comprehensive playbook on how to respond to such attacks in future.

IN5

Securing a vital healthcare platform and increasing patients' trust

Who did we work with?

- Cyber Capacity Unit
- KPMG Indonesia
- The Ministry of Health
- The National Cyber and Cryptography Agency (BSSN)
- The Ministry of Communication and Information Technology
- The Health and Social Security Agency
- Five healthcare facilities across Indonesia

What was delivered?

- A security framework for the healthcare sector, taking into account key legislative arrangements. The session was delivered to participants from 5 different vertical hospitals serving approximately 500,000 patients. This framework has the potential to roll out to 11,388 healthcare facilities across Indonesia, including 2,962 hospitals and 7,588 primary health care centres, serving the population of 260million.
- A privacy impact assessment methodology for electronic medical records and telemedicine patient data.
- Two incident response exercises, leading to recommendations on how best to establish a new cross Indonesia Ministry of Health CSIRT. The session was the first of its kind to be delivered in a foreign language and was delivered to the Ministry of Health's CERT and IT teams. Feedback from the sessions showed an excellent average satisfaction rating of 83%.
- A comprehensive incident response malware playbook.

Document Classification: Official

Government cybersecurity training

Why did we deliver this work?

Nine government ministries currently have a portfolio which encompasses some of Indonesia's critical national infrastructure (CNI) assets. Together, they are responsible for delivering information security policies and regulations to keep those assets and their data secure. However, they typically lack the necessary in-house specialist skills and knowledge to do this effectively.

The opening phase of this project therefore involved working with the National Cyber and Cryptography Agency (BSSN), coordinating activities to help plug this information security skills gap. The immediate response was to put 200 officials through a training programme focused on six internationally recognised information standards.

Next, the project considered the government's broader ongoing training requirements, creating a government security skills framework and a formalised learning and development programme.

A host of internationally recognised courses were identified and used to build a comprehensive learning pathway, aligned to the roles, departments and competencies highlighted within the skills framework. Work then began to determine how best to operationalise this across BSSN and the other ministries.

By improving government officials' cyber policy capabilities, the ambition is for them to produce better, more robust, information security frameworks. In turn, this should lead to better cyber practices among the CNI operators themselves and data being managed more securely.

IN9

Delivering vital cyber skills at the heart of Government

Who did we work with?

- KPMG Indonesia
- Social Development Direct & Chatham House
- Multimatics
- The National Cyber and Cryptography Agency (BSSN)
- Nine ministries responsible for critical national infrastructure, including the Ministries of Health, Defence and Industry

What was delivered?

- A three-day cyber practitioner course, delivered by Chatham House to 200 participants from the nine ministries, including a gender and social inclusion element delivered by Social Development Direct.
- A five-day ISO training course covering six international information security standards, delivered by leading local training supplier, Multimatics.
- ISO27001:2013 Lead Auditor training and certification for 19 BSSN officials. In total over 400 members of the Indonesian government participated in the cyber security courses.
- A government security skills framework that identifies cyber security roles and defines their expected skills, proficiency levels and relevant training courses.

Document Classification: Official

GREAT for PARTNERSHIP
BRITAIN & NORTHERN IRELAND

Brazil

Raising awareness of cybersecurity across Brazil

Why did we deliver this work?

When the Brazilian government launched E-Ciber, its first ever national cybersecurity strategy, it knew it needed to improve public awareness of the cyber threats that Brazilians now face. This meant tackling the issue at an early age in schools but also within the broader adult population, especially among vulnerable groups.

Across the country, online sexual exploitation, discrimination, cyber bullying and abuses of personal data are on the rise. Many of these cyber harms directly affect vulnerable members of society, including women, young people, under-represented minority groups and the elderly.

This project aimed to improve the government's in-house capability for designing and executing public awareness campaigns to highlight the importance of being cybersecure and providing citizens with some basic cyber hygiene guidance.

This meant providing the relatively new communications team at GSI-PR, Brazil's Institutional Security Cabinet, with training and advice on campaign planning and execution.

Drawing on international best practice, a framework for planning communications campaigns was created. A Brazilian communications agency, Tonica, was engaged to assist with this, creating a series of educational videos on different elements of the framework and following up with detailed training on campaign planning.

Suitably equipped, GSI-PR now has the capability to run its own national campaigns, as the department looks to improve Brazil's cyber maturity. As evidence of this, as the project drew to a close, a host of materials were created for a new awareness campaign, scheduled to go live after the Brazilian Presidential election.

BR1

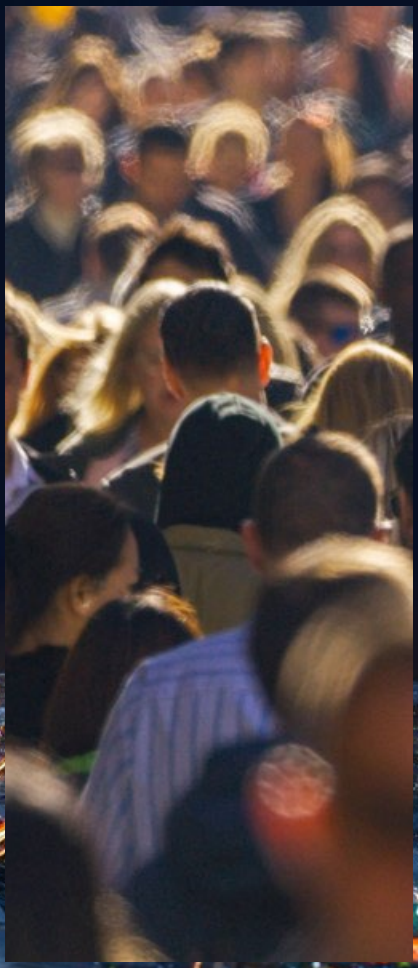
Creating a more cybersecure population

Who did we work with?

- Institutional Security Cabinet of the President of the Republic (GSI-PR)
- GSI-PR Social Communication Office GSI-ASSESSORIA DE COMUNICAÇÃO
- Tonica, a Brazilian communications agency
- KPMG Brazil

What was delivered?

- A review of existing models and methodologies for running awareness campaigns; knowledge sharing activities; and lessons learned from other campaigns.
- A framework and a strategic action plan for running awareness campaigns, based on existing models and tailored to GSI-PR's specific requirements and needs.
- Campaign materials, including media content assets on topics such as device protection, digital rights and safe online gaming, as well as a cartoon character to act as a central campaign motif. These materials have the potential to reach 120 million people across Brazil.



Document Classification: Official

Securing e-Government services

Why did we deliver this work?

To reduce bureaucracy and provide more efficient access to public services, Brazil is currently digitising all its government services. It's a huge undertaking, involving more than 250 government departments and thousands of apps, webpages and online processes.

Such a wholescale shift to online services could expose citizens to cyber harms unless security and privacy concerns are comprehensively addressed when new services are being designed. With a suitable Security by Design framework in place however, everything from access controls, firewalls and encryption through to governance and privacy considerations can be addressed from the outset.

Such a framework provides reassurance over the safety of citizens' personal data and safeguards services' integrity and availability. The latter is a particularly important consideration for Brazil's large, remote, rural communities with limited physical access to public services.

Having understood the technical requirements of the government's various online services, the project team developed the framework and an action plan for its implementation. Training was created to demonstrate how the framework should be used, alongside a rating mechanism for retrospectively evaluating the security of services that had already been digitised.

A dedicated government Cybersecurity Week in February 2022 presented the ideal opportunity to train over 70 departments on how to implement the framework's technical controls.

The team subsequently worked on consolidating all of the government's existing cyber and privacy controls. This led to the creation of a single, automated controls framework. This will now be used with all government departments to help them better understand their own cyber maturity and how to improve it.

BR3

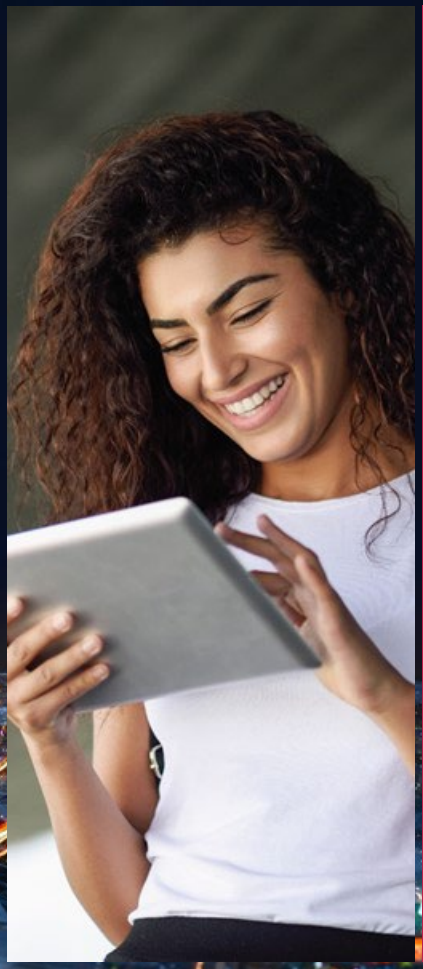
Ensuring Government e-services are safer from cyber threats. Providing assurance over citizens' personal data

Who did we work with?

- Brazil's Ministry of Economy – Special Secretariat of De-bureaucratisation, Management, and Digital Government (SGD)
- KPMG Brazil

What was delivered?

- An assessment of the maturity of SGD's current approach to Security by Design, identifying where improvements were required.
- A Security by Design framework for SGD to use in its digitisation programme (and more widely where desired). SDG are set to promote this framework to a further 70 government bodies.
- E-Government services, created with these new Security by Design procedures.
- Two knowledge sharing workshops; one with the UK government on Security by Design and one with KPMG and CYSIAM on government incident responses. These workshops were attended by 222 participants from over 70 different government organisations.
- A new framework that SGD can use to implement additional security and privacy measures and controls in government organisations.



Document Classification: Official

Building Brazil's national cybersecurity curriculum

Why did we deliver this work?

When Brazil launched its first ever national cybersecurity strategy, one of its main objectives was to improve cyber awareness and education across the country.

Young children are exposed to any number of cyber harms but by improving their cyber awareness while at school, the government wanted to help them securely navigate cyberspace, recognising potential risks and knowing how to avoid them.

This project was designed to bring greater consistency and effectiveness to the way that digital skills are taught in Brazilian schools. This meant curating a toolkit of suitably high quality resources, helping teachers deliver the curriculum to the best of their ability.

Initially, research was undertaken with schools in three states; Pernambuco, Bahia and Brazil's Federal District. This helped paint a detailed picture of the cyber harms that children face and the barriers that teachers encounter when trying to deliver cyber education. The research findings helped determine the resources that needed to feature within the toolkit.

Once all the desired materials had been collated (and tailored where necessary), a beta version of the toolkit was tested with teachers, ahead of a full launch to all schools via the three states' educational platforms in September. The toolkit, featuring 40 hours of lesson plans and support materials, spread across five themed modules, was subsequently made available on a couple of national platforms as well.

A communications campaign was created to raise awareness of the toolkit's availability among teachers. Work was also undertaken to raise the project's profile with influential government stakeholders. The project rounded off with a report on future cyber trends, to be taken into account when updating the toolkit materials in future years.

BR7/9

Increasing teachers' and schoolchildren's resilience to cyber threats

Who did we work with?

- Brazil's Ministry of Education and partner State Secretariats for Education
- SaferNet, a Brazilian NGO that focuses on cybercrime and human rights violations
- Tonica, a Brazilian communications agency
- KPMG Brazil

What was delivered?

- Research into teachers' and pupils' experiences of online harms. Set against an assessment of available teaching materials and the gaps that existed, this helped inform the design of toolkit.
- Knowledge sharing workshops to collate relevant toolkit and training materials.
- A beta version of the toolkit, tested with schools in the pilot states, and a full launch version, incorporating teachers' feedback from the pilot phase. The toolkit was tested across 5 different schools, covering 252 students and 6 professors. This has the potential, with rollout to be applied by all 197,500 Brazilian schools increasing the resilience to cyber threats of some 52 million school children
- Awareness-raising communications activities, targeting teachers and government stakeholders.
- A future cyber trends report, with recommendations on how to incorporate its insights into future iterations of the toolkit.

Document Classification: Official

Nigeria

Critical national infrastructure threat assessment and protection

Why did we deliver this work?

When a critical national infrastructure (CNI) asset fails, the impact of losing the service it provides, such as electricity or water, can be devastating, especially for vulnerable groups.

Previously, Nigeria had no central regulator and so lacked a single consistent approach to regulating its CNI. The government's understanding of what constituted its CNI was relatively under-developed, as was its appreciation of the cyber threats posed to those assets and how to mitigate them.

Nigeria's Office of the National Security Adviser (ONSA) wanted to rectify this by developing a framework for identifying its CNI and protecting it from cyberattacks. Within this project, Nigerian CNI providers and UK subject matter experts combined to help ONSA understand the current maturity of Nigerian CNI regulation and to develop the functional requirements for a new regulation operating model.

This work was accompanied by a report on international regulation best practice and an analysis of sector-specific threats to CNI providers. A simulation exercise was also conducted with one CNI sector to understand its current procedures for coordinating its response to a cyber attack.

All of this fed into the development of a functional requirements report for the operation of Nigerian CNI and an implementation plan, designed to help ONSA achieve its CNI regulation objectives.

In parallel, the Home Office trained ONSA and providers from three CNI sectors in how to complete a national cyber risk assessment. Building this capability will allow Nigeria to run its own future assessments of how CNI providers are managing cybersecurity risk and to identify where improvements could be made.

NG1

Defending Nigeria's critical assets from major cyber threats

Who did we work with?

- The Office of the National Security Advisor (ONSA)
- Nigerian CNI providers (Financial Services, Telecommunications and Defence)
- Home Office
- Chatham House
- CYSIAM

What was delivered?

- An assessment of current Nigerian CNI regulation, providing a review of how CNI is regulated.
- A report on international CNI regulation good practice.
- A threat analysis report, examining sector specific threats to Nigeria.
- A cyber resilience exercise with leading CNI stakeholders.
- Functional requirements report for CNI regulation
- National cyber risk assessments for three sectors outlined above, piloting an approach that can be replicated across all Nigerian CNI providers.

Document Classification: Official

Cybersecurity toolkits for SMEs

Why did we deliver this work?

Small and medium-sized enterprises (SMEs) in Nigeria are critically important to the country's economy. However, they often have insufficient security measures in place to protect them from the growing threat of cybercrime. Attacks against them can cause significant financial hardship or even force them to stop trading. With SMEs responsible for the majority of Nigerian employment, the fallout from successful attacks can be significant.

Without a better understanding of cybersecurity threats or access to suitable resources, SMEs were likely to continue without effective controls in place, making them vulnerable to attacks. This project was therefore designed to provide SMEs with the free, easily accessible resources they needed to be more cyber resilient.

To do this, the project team partnered with the UK-based Global Cyber Alliance to produce develop a free online cybersecurity toolkit. This was tailored to the Nigerian business environment and cyber threat landscape and used relatable, real-life examples. It was accompanied by a vulnerability assessment tool, helping SMEs better understand their current cyber maturity and posture.

The toolkit was made available via the networks of partner organisations such as the Cybersafe Foundation, SMEDAN and ONSA. As well as a pilot and main launch event, train-the-trainer sessions were also held for Nigerian organisations and government departments who support local SMEs. This activity resulted in training being delivered to over 150 business owners, trainers and facilitators in just six months.

NG4

Strengthening the cybercrime defences of Nigerian small businesses

Who did we work with?

- The Development Agency of Nigeria (SMEDAN)
- The National Information Technology Development Office (NITDA)
- The Office of the National Security Advisor (ONSA)
- The CyberSafe Foundation, a Nigerian NGO that specialises in working with Nigerian SMEs.
- Social Development Direct (SDD), a UK organisation ensuring social inclusion, equality and human rights are central to UK Aid programmes

What was delivered?

- A cybersecurity toolkit, developed through consultation with stakeholders including government departments and local NGOs. By the end of September 2022, the toolkit had been accessed 18,596 times.
- A communications strategy and implementation plan for the dissemination of the toolkit to local NGOs.
- A pilot launch of the toolkit, with cyber e-learning provided to female-owned SMEs. The Future Females Business School was sufficiently impressed that they included the toolkit in the graduation ceremony of over 100 female entrepreneurs from agnostic and GreenTech programmes.
- A hybrid main launch event, attended by over 100 delegates.
- Train-the-trainer sessions with ten organisations that support Nigerian SMEs.
- A one-day train-the-trainer workshop delivered with SMEDAN.
- Workshops and conferences to distribute, and raise awareness of, the toolkit among NGOs and SMEs.

Document Classification: Official

Digital forensics and judicial cybercrime training

Why did we deliver this work?

Introduced in 2015, the Cybercrimes Act was Nigeria's first piece of legislation designed specifically to tackle cybercrime. Despite this, levels of cybercrime remained high. The Nigerian government subsequently highlighted a need to improve law enforcement agencies' capability for combating cybercrime.

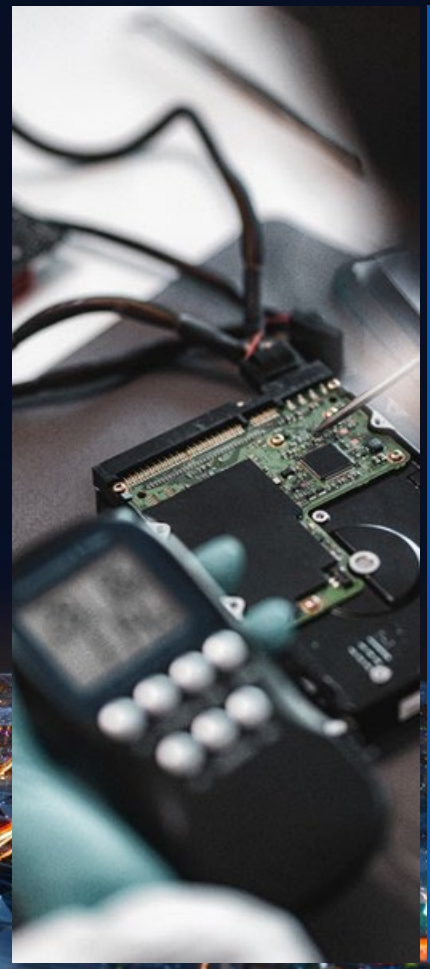
It was identified that these agencies needed to improve their digital forensics skills and processes in order to keep pace with the ever-shifting nature of cybercrime. In addition, there were a limited number of judges and prosecutors with sufficient knowledge of cybercrime, reducing the likelihood of a successful prosecution of those cases that do make it to court.

The work on this project involved significant analysis to explore Nigeria's ability to investigate cybercrime. A training needs analysis was completed across both law enforcement and the judiciary. This resulted in two sets of tailored training materials being produced by CYSIAM.

Digital forensics training was subsequently delivered to law enforcement organisations in July, including a session on digital privacy and gender-based violence. Training materials for the judiciary are expected to be integrated into their annual training programme for future years. Sessions were also held with the government to help define a vision for future training in this area.

NG7

Improving the prosecution of cybercrime



Who did we work with?

- Nigerian law enforcement agencies
- The National Judicial Institute (NJI)
- The Office of the National Security Advisor (ONSA)
- CYSIAM
- Social Development Direct (SDD)

What was delivered?

- A cybercrime training needs analysis, which was used to inform the subsequent design of training materials for cybercrime and digital forensics.
- An international best practice guide for digital evidence handling
- Training courses, modules and workshops for Nigeria's specialist cybercrime unit, judges and prosecutors, covering topics such as digital data sources and exploitation, data integrity, chain of custody and attribution.
- Professional digital forensics training for 15 members of staff from seven different law enforcement organisations, including awareness training on digital privacy and online gender-based violence.
- A report outlining further available training resources and a roadmap for implementing a future training strategy.

Document Classification: Official

National cybersecurity strategy communications campaign

Why did we deliver this work?

In 2021, Nigeria's Office of the National Security Adviser (ONSA) launched an updated version of its National Cybersecurity Policy and Strategy (NCPS). Keen to raise awareness of this new strategy, ONSA wanted to deploy a substantial communications campaign.

The campaign would need to highlight what had changed within the NCPS, why this mattered and what people might be expected to do differently as a result. A broad mix of different audiences, from other government agencies and critical industry sectors through to the general population, would be targeted.

To help deliver the campaign, a UK-based strategic communications agency, Torchlight, was engaged. Torchlight developed Thrive Online, a national awareness raising campaign, advising citizens how to better protect themselves online. A website was populated with advice guides and supporting articles while an extensive programme of Facebook Thrive Online account activity and radio adverts drove traffic to the site.

Final evaluation suggests that the campaign reached 10% of the Nigerian population; some 20 million people. As the project concluded, support was provided to the ONSA communications team to ensure they could maintain the campaign momentum built up over the previous months.

NG18

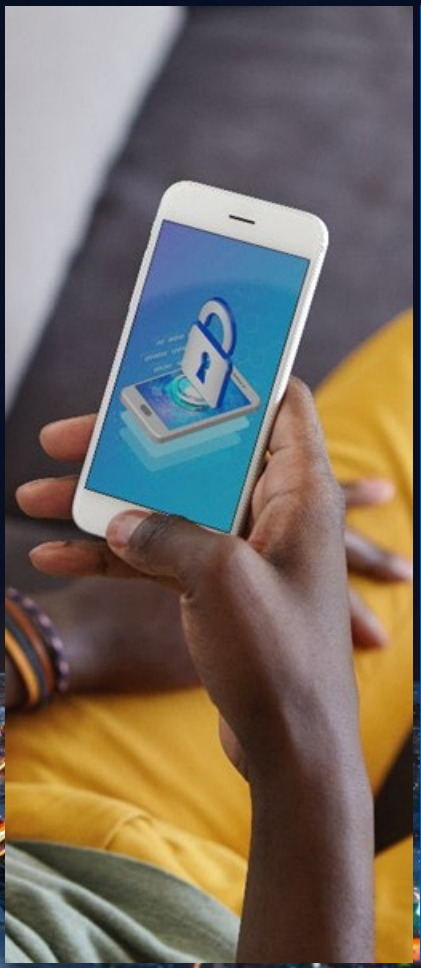
Helping Nigerians understand what the strategy means for them

Who did we work with?

- The Office of the National Security Advisor (ONSA)
- Social Development Direct (SDD)
- Torchlight, a UK-based a security consultancy

What was delivered?

- A multi-channel communications campaign to raise awareness of the Nigerian cybersecurity strategy. The campaign reached some 20 million people, 10% of the Nigerian population. 92% of those surveyed feeling that they can better protect themselves online as a result.
- Support to ONSA to deliver future strategic communications campaigns of its own.



Document Classification: Official

Kenya

Supporting the Data Protection Commissioner

Why did we deliver this work?

Kenya's Data Protection Act became law in 2019, leading a year later to the creation of the Office of the Data Protection Commissioner (ODPC) and the appointment of its first Commissioner. This aimed to improve the security of Kenyan citizens' and organisations' confidential data.

Kenya had previously suffered from significant data breaches and frequent cases of crimes stemming from the abuse of personal data, including fraud, identity theft, stalking and even kidnap. As ever, vulnerable groups were particularly at risk, unaware of how their data was even being used, let alone protected.

This project was designed to accelerate making the ODPC operational by helping to develop its initial three-year strategy. Following the strategy's launch in January 2022, work began on translating the strategy into a sustainable, operational framework that could deliver tangible changes in the way organisations handled personal data.

However, this wasn't just about deciding how to hold organisations to account. Instead, the ODPC wanted to use this as an opportunity to challenge organisations to think more carefully about the data they hold and how and why it needs to be protected.

To assist with this, the ODPC began to increase its operational capacity and budget. Making these investments just ahead of the general election that was held in August 2022 demonstrated the high priority that the government now places on data protection.

KE1

Protecting Kenyans' personal data

Who did we work with?

- The Office of the Data Protection Commissioner (ODPC)
- The Kenyan Communications Authority
- Various Kenyan civil society organisations
- Social Development Direct (SDD)
- Strathmore University
- KPMG Kenya

What did we deliver?

- Support to the ODPC, allowing it to prioritise and accelerate its operational goals.
- A data protection strategy and roadmap for 2022-2025 that is aimed to support over 30million citizens that are currently online, some 60% of the total population.
- Knowledge transfer activities to equip ODPC staff to deliver the priority elements of the strategy.

Document Classification: Official

Operationalising a national Public Key Infrastructure

Why did we deliver this work?

As the Kenyan government looks to expand the e-services it offers to citizens, cybersecurity is a critical consideration to ensure these services are secure. In response to this, the government is now working to create a Public Key Infrastructure (PKI) system, in line with international best practice guidelines.

A PKI system ensures trustworthy, secure online communication by creating, storing and distributing digital certificates. An effective PKI plays a vital role in securing online transactions by delivering confidentiality, integrity and authentication across the government's digital platforms.

The responsibility for creating the PKI sits with Kenya's ICT Authority (ICTA). For this project, cyber specialists from the UK, Kenya and South Africa partnered with ICTA to design the policies governing the PKI. Internationally accepted guidance was contextualised, creating policies and a framework to meet the Kenyan government's particular requirements.

Two workshops played an important part in helping to achieve this, eliciting technical feedback on early versions of the policies. They also made sure that all stakeholders understood every aspect of the policies, what they meant in practical terms and what this required of ICTA.

Attention then turned to the operational plan required to implement the new PKI. A further workshop, attended by 13 government departments, was held to promote the PKI system across government, demonstrating its value and exploring how and why it needs to be deployed.

One last session was also held with the ICTA Board to take them through the final policy drafts, ensuring they were sufficiently comfortable with the policies to sign off on them, thereby allowing the PKI to launch.

KE2

Creating trust in the Government's growing e-services

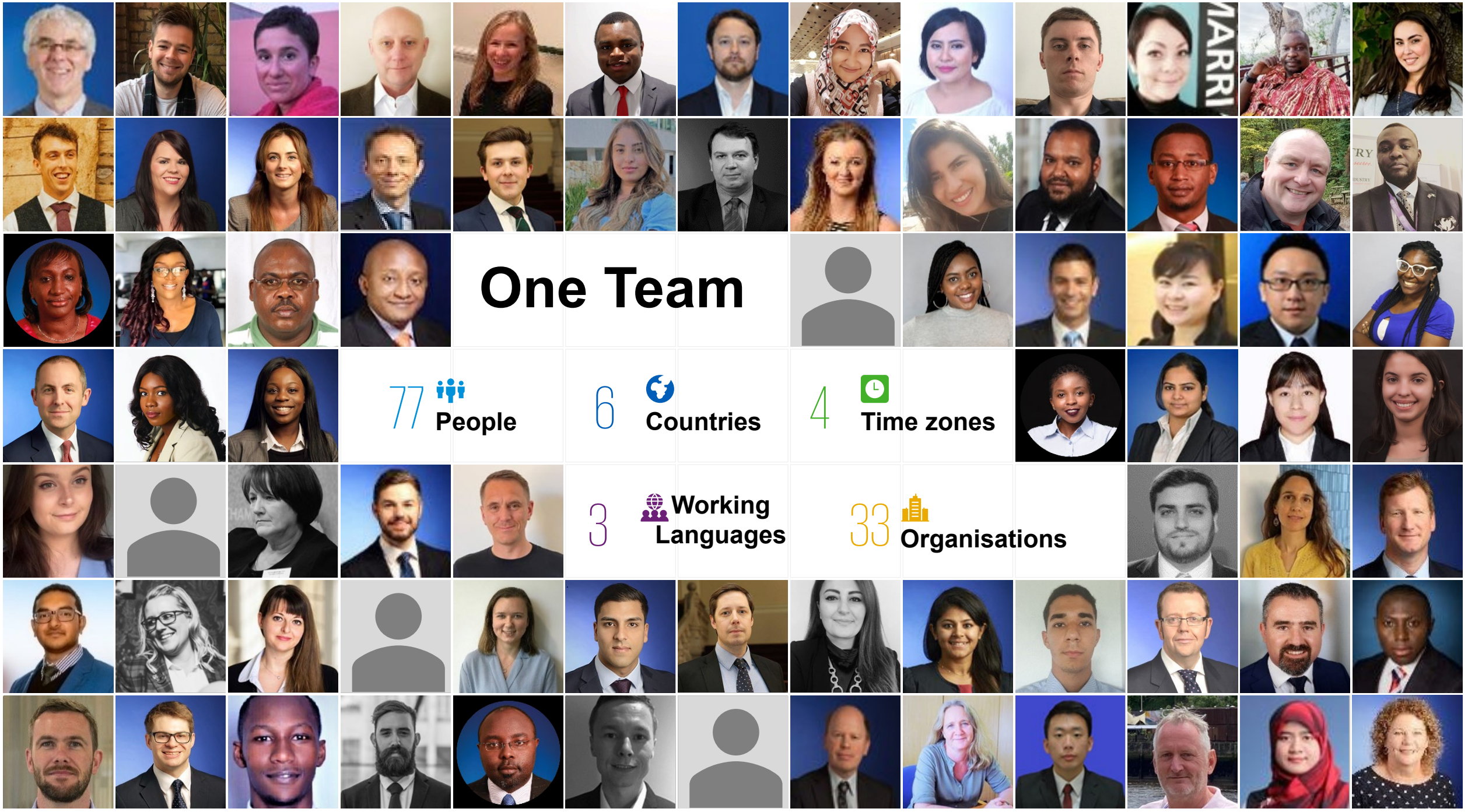
Who did we work with?

- The Information and Communication Technology Authority (ICTA)
- Serianu
- KPMG Kenya
- Social Development Direct (SDD)

What did we deliver?

- Support to ICTA, helping them to develop 12 PKI policies in line with international best practice.
- Training workshops designed to develop ICTA's PKI technical capacity and to secure departmental buy-in.
- A stakeholder workshop, presenting the PKI to 13 government departments.
- The socialisation of the final policy drafts with the ICTA Board to gain sign-off and enable the launch of the PKI.

Document Classification: Official


One Team
77 People
6 Countries
4 Time zones
3 Working Languages
33 Organisations