

# Empowering Nigeria Against Digital Threats

## 1. Program Synopsis

The "Empowering Nigeria Against Digital Threats" program aims to bolster the resilience of Nigerian civil society, journalists, and human rights defenders against online attacks, including spyware, censorship, and digital harassment. By leveraging capacity-building initiatives, advanced digital tools, and advocacy for legal reform, this program will address systemic vulnerabilities and ensure a sustainable, rights-based digital ecosystem in Nigeria. The program will engage key stakeholders such as civil society organizations (CSOs), legal entities, and technology providers to maximize impact and scalability.

**Funding Request:** \$2,500,000 over 24 Months

## 2. Participating Organization Partners

1. **Paradigm Initiative:** Renowned for their work on digital rights and inclusion across Africa, and extensive experience in cybersecurity training, policy advocacy, and community mobilization.
2. **Connected Development:** Mobilizing grassroots communities for digital security training and capacity building.
3. **Media Rights Agenda:** Providing legal support and promoting policy advocacy to protect journalists and media practitioners from digital threats.
4. **Cybersafe Foundation:** Delivering technical expertise for cybersecurity awareness and incident response.

## 3. Program Objectives, Activities, and Expected Results

This activity will enhance the digital security capabilities of civil society by equipping civil society organizations, journalists, and activists with the tools and knowledge necessary to safeguard their digital operations against malicious attacks. By addressing key vulnerabilities, this initiative will enable these groups to operate securely in an increasingly hostile online environment.

- **Activities:**
  - Conduct 50 digital security workshops in Nigeria to teach best practices and counter online threats.
  - Distribute 10,000 digital safety toolkits tailored to address specific threats.
  - Establish a 24/7 Digital Security Helpline for real-time support and incident response.
  - Develop an online training platform featuring interactive courses on digital security.
- **Expected Results:**
  - Over 5,000 individuals trained to identify and mitigate digital threats.
  - Increased adoption of secure communication tools, reducing at-risk group vulnerability.
  - Greater awareness and responsiveness to digital security issues in civil society networks.

**Objective 2: Counteract and Mitigate Digital Repression** This objective seeks to address the tactics used by oppressive entities to suppress freedoms online, including spyware deployment,

# Empowering Nigeria Against Digital Threats

denial-of-service attacks, and harassment campaigns. By countering these actions, the program aims to protect human rights defenders and promote digital freedom.

- **Activities:**

- Develop and deploy counter-surveillance tools to identify and neutralize spyware threats.
- Partner with technology firms to monitor, analyze, and report denial-of-service attacks.
- Create an incident reporting platform for victims of online harassment and digital attacks.
- Conduct threat analysis workshops to help stakeholders anticipate and prepare for digital repression.

- **Expected Results:**

- Reduction in spyware-related incidents in targeted groups, enhancing operational safety.
- Improved capacity to detect and mitigate DoS attacks, ensuring operational continuity.
- Establish a robust mechanism for documenting and addressing digital harassment cases.

**Objective 3: Advocate for Legal and Policy Reforms** This objective emphasizes the need for a stronger legal framework to combat digital repression. By engaging with policymakers and stakeholders, the program will advocate for the adoption of laws and policies that protect digital rights.

- **Activities:**

- Work with legal experts to draft model laws addressing spyware and online harassment.
- Organize five high-level roundtables with government officials, civil society leaders, and international partners to discuss digital rights.
- Publish and disseminate three policy briefs on Nigeria's digital security framework gaps.
- Train 50 legal practitioners on defending digital rights cases in Nigerian courts.

- **Expected Results:**

- Enactment or strengthening of two national policies to safeguard digital rights and combat online attacks.
- Improved legal accountability mechanisms to hold perpetrators of digital repression accountable.
- Increased capacity of the legal system to address and prioritize digital rights violations.

**Objective 4: Promote Public Awareness and Community Resilience** To build a digitally resilient society, this objective will enhance public understanding of digital threats and encourage proactive measures to mitigate risks. It will leverage community engagement to foster a culture of digital security.

- **Activities:**

- Launch a nationwide digital literacy campaign using social media, radio, and television.
- Translate and distribute educational materials on digital rights into five local languages.
- Host an annual Digital Security Week featuring community-led events and workshops.

# Empowering Nigeria Against Digital Threats

- Create a "Digital Resilience Champion" program to train community leaders in digital security advocacy.
- **Expected Results:**
  - Public awareness of digital threats and rights increased among 1 million Nigerians, empowering them to take preventive action.
  - Strengthened grassroots mobilization to address online attacks, fostering their resilience.
  - Establishment of a network of trained community advocates promoting digital security at the local level.

## 4. Expertise and Capacity of the Applicants

- **Paradigm Initiative:** Paradigm Initiative has over a decade of experience advancing digital rights and inclusion across Africa. The organization has successfully implemented programs such as the Digital Rights and Freedom Act advocacy in Nigeria. With a robust network of partners and proven expertise in managing U.S. government grants, Paradigm Initiative is well-positioned to lead ENDT.
- **Connected Development (CODE):** CODE specializes in engaging marginalized communities through innovative approaches. Their track record includes successful implementation of grassroots campaigns that combine offline and online strategies, making them invaluable for reaching underserved populations.
- **Media Rights Agenda (MRA):** MRA's legal advocacy efforts have been instrumental in shaping Nigeria's media landscape. Their capacity to navigate the legal and policy environment will ensure the program's advocacy components are impactful.
- **Cybersafe Foundation:** As a leading organization in cybersecurity education, Cybersafe Foundation has trained thousands of Nigerians in online safety and incident response. Their technical expertise will strengthen the program's cybersecurity initiatives.

## 5. Conclusion

The "Empowering Nigeria Against Digital Threats" program aligns with the objectives of DRL's Internet Freedom initiative by addressing acute repressive threats and building sustainable resilience among vulnerable populations. Through robust partnerships, targeted activities, and measurable outcomes, this program will foster a secure digital environment in Nigeria and serve as a replicable model for similar contexts globally.

# Empowering Nigeria Against Digital Threats

## Notes on this draft.

This is a draft proposal created by ChatGPT using the prompt below. It was developed by ICTworks to [show you the power of Generative AI to support your proposal process](#).

This draft should NOT be the basis of your application. It is for demonstration purposes only.

Anything created by Generative AI **must always** be reviewed line by line and heavily edited by knowledgeable staff who take full responsibility for the output. [Think of Generative AI as an overeager graduate assistant](#).

## ChatGPT Prompt:

Analyze the uploaded document [[IF APS RSOI 24-25.pdf](#)]

Develop a compliant proposal that will focus on Funding Theme #2: Prevent and Remedy Online Attacks (Digital Security). This activity will take place in Nigeria. The proposal should be 1500 words long and include:

1. A synopsis of the program, including a brief statement on how the program will have a demonstrated impact and engage relevant stakeholders.
2. A leading organization and three potential local partners. Choose the best organization to lead this effort and 3 strong partners that can help. These should be real organizations.
3. A concise breakdown explicitly identifying the program's objectives and the activities and expected results that contribute to each objective.
4. A brief description of the applicants that demonstrates the applicants' expertise and capacity to implement the program and manage a U.S. government award.