Cyber Security Experts Association of Nigeria (CSEAN)
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Faculty of Computational Sciences & Informatics - Academic City University College, Accra, Ghana
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
ICT University Foundations USA

Proceedings of the Cyber Secure Nigeria Conference – 2023

Evaluating Government Strategies for Child Online Protection

Moses Joshua
Cybersecurity Education Initiative (CYSED)
E-mail: mosesjoshua72@gmail.com
Phone: +234 806 701 7054

ABSTRACT

This study examines the current state of the Nigerian Government's child online protection strategies, and it evaluates their implementation and effectiveness in protecting children in this digital age using a comprehensive evaluation framework. It also highlights the importance of evaluating online child protection in the context of Sustainable Development Goals (SDGs). The finding reveals the strength and weaknesses of the existing approach by the government and the challenges faced by the government in implementing effective strategies. Recommendations are provided to improve the current strategy adopted by the Nigerian Government, such as enhancing a strong policy framework, improving international cooperation, investing in education and awareness, public-private partnership and regular evaluation and adaptation. The study concludes by emphasising the importance of continuous assessment by the government to address the evolving threat landscape ton Child Online Protection and calls for a more comprehensive multidimensional approach involving the government, civil society organisations, and private companies to create a safer digital world for children.

Keywords: Online Safety, Child Online Protection, Government Strategies, Personal Data Management, Internet Security

Proceedings Citation Format
Moses Joshua (2023): Evaluating Government Strategies for Child Online Protection. Proceedings of the Cyber Secure Nigeria Conference. Nigerian Army Resource Centre (NARC) Abuja, Nigeria. 11-12th July, 2023. Pp 125-134.
https://cybersecurenigeria.org/conference-proceedings/volume-2-2023/. dx.doi.org/10.22624/AIMS/CSEAN-SMART2023P115

1.. INTRODUCTION

In today's interconnected world, digital innovations have revolutionised various sectors, including education, agriculture, e-commerce, banking, and finance. These advancements have

significantly contributed to the development and growth of nations, making work more efficient, communication is more effective, and businesses thriving seamlessly.
However, along with these digital innovations, a growing threat looms: "Cyber Threats." These threats pose significant challenges and disruptions to global operations, with estimated predicted business losses to reach a staggering $10.5 trillion in 2025 (Calif, 2020). This is a concern not only for individual countries but also for Nigeria, a nation with a burgeoning digital economy that contributed 18.44 per cent to its GDP in Q2 2022. (Pantami, 2022). While digital innovations hold immense potential for enhancing economic and social affairs and achieving the United Nations' Sustainable Development Goals (SDGs), they also expose users to potential harm. Cybersecurity emerges as a critical tool in combating these cyber threats and ensuring the safety and well-being of individuals and organisations relying on digital innovations. By providing digital safety measures, cybersecurity plays a pivotal role in both protecting against malicious activities and fostering a conducive environment for users to fully leverage the benefits of digital technologies.

1.1 Evaluating Government Strategies For Child Online Protection Safety

This paper delves into the crucial topic of evaluating government strategies for child online protection safety. It sheds light on the imperative of safeguarding children from the dangers they may encounter while harnessing the tremendous benefits of the internet. According to United Nations (2020), Global connectivity is being driven by youth, with 75% of those aged 15 to 24 expected to be online in 2022, compared to 65% of the rest of the world's population. Additionally, kids are using the internet more than ever before. However, it is vital to recognise and address the dangers that children may face during their online activities. In today's rapidly evolving world, harm has taken on new forms, particularly in the digital realm. This paper will specifically evaluate the strategies implemented by the Nigerian government to promote online safety for children. By examining and assessing these government strategies, this paper aims to shed light on their effectiveness and identify areas that may require improvement. It is essential to critically analyse the measures in place to protect children online, as they play a significant role in shaping the safety and security of the younger generation in the digital age.

1.2 Research Objective

The effective implementation of government strategies for child online protection safety is crucial in mitigating the exploitation of children in the virtual space. Without comprehensive and robust control measures put in place by governments, the persistent occurrence of such exploitation poses a significant threat, necessitating urgent action to safeguard children from online harm.

2. CHILD ONLINE PROTECTION AND ITS SIGNIFICANCE IN THE DIGITAL AGE.

The threat to children on the internet is a pressing global issue, particularly in countries like Nigeria, where over 60% of the population is under 25 years old (Akinyemi 2022), with approximately 9 out of 10 teenagers having internet access (Monyei, 2018); children are vulnerable to faceless individuals who exploit them through sexual coercion, kidnapping facilitated by online interactions with strangers, cyberbullying leading to detrimental effects like depression and loneliness, recruitment by extremist or terrorist groups taking advantage of social media platforms to propagate harmful ideologies, and the potential for young people

themselves to engage in harmful activities such as cyberbullying, pornography consumption, and criminal behaviour.

2.1 The Risks and Challenges Faced by Children In The Online Environment.

Children face numerous risks and challenges while navigating the online environment, and these issues have far-reaching consequences that extend beyond the individual child. Some of the key challenges they encounter include cyberbullying, encounters with online predators, inappropriate content, privacy and data security, and online scams. To address these challenges, strategies to promote online safety must strike a balance between safeguarding children from harm and preserving the educational and health benefits of digital technologies. Such strategies should encompass measures to protect against exposure to violence, exploitation, and abuse and ensure privacy protection.

2.2 The Role of Governments In Ensuring Child Online Safety.

Governments bear the responsibility of safeguarding children in both the physical and virtual realms, recognising the profound integration of new technologies into the lives of young people. The demarcation between real-world and online events is becoming increasingly blurred and inconsequential, as the two domains are intricately interconnected and interdependent. Through its Child Online Protection (COP) guidelines, the ITU has been actively promoting Child Online Safety. These recommendations, which were first presented in 2009 and updated in July 2020, offer a thorough foundation for developing a secure and empowered online environment for kids. In numerous Member States, they have been instrumental in creating national plans for protecting children online. To strengthen their child online protection strategies and policies, numerous nations in Africa, the Arab world, Asia Pacific, and Europe have embraced the ITU guidelines. The ITU Child Online Protection Guidelines can be referenced to highlight the role of the government in child online protection. These guidelines emphasise the following roles and responsibilities of government:

Legislation and Regulation: To address Child Online safety, governments enact and enforce laws, rules, and policies. As part of this, platforms must establish safety measures, restrict the age range at which users can access specific online materials, and address problems like cyberbullying, child exploitation, and online grooming. Governments try to make sure that the legal system keeps up with new developments in technology and changing online hazards.

Awareness and Education: The government needs to foster child online safety among children, parents, teachers, and the public, as well as educate people about the dangers of the internet. They create and promote educational projects, campaigns, and programs to increase awareness of online child safety, responsible digital citizenship, and the potential risks of navigating the internet.

Industry Collaboration: Governments work together with internet service providers, social media platforms, and technology firms to set industry standards, conduct guidelines, and best practices for safeguarding children online. They promote the implementation of safety features, content control systems, and reporting tools on platforms. Governments may also encourage industry engagement and keep an eye on whether established rules are being followed.

Reporting and Helplines: Governments set up and promote reporting mechanisms, hotlines, and helplines where children, parents, and the public can voice concerns about online safety or get help. They make certain that these channels are freely available and private and offer the proper help and direction to those who require it.

Law enforcement and investigation: Governments provide funding to law enforcement organisations tasked with looking into and bringing to justice those who engage in online child exploitation, abuse, or harassment. To combat transnational crime and enhance information exchange, they work with foreign partners. Governments aim to improve law enforcement officers' specialised training and investigation capabilities.

Research and Data Collection: To better understand how new internet risks, trends, and technologies affect kids, governments engage in research. They gather information on incidents involving internet safety, the frequency of dangers, and the efficiency of interventions. Evidence-based policies and methods for the protection of children online are aided by this research.

International Collaboration: Governments work together internationally and form partnerships to solve the worldwide issue of children's online safety. They collaborate with international organisations like the United Nations and Interpol to create global frameworks, projects, and standards by participating in international conferences, exchanging best practices, and working together.

3. EVALUATION FRAMEWORK

The proposed evaluation framework for assessing the effectiveness of government strategies for child online protection safety includes the following key elements.

Policy and Legislation: Evaluating the adequacy and comprehensiveness of the legislative measures and policy implemented by the government to address child online protection.

Implementation and Enforcement: Examining the effectiveness of implementing and enforcing the policies and laws relating to child online safety, including allocation of resources, capacity building and collaboration with relevant stakeholders for effective implementation of the laws and policies.

Education and Awareness: Assessing the availability, effectiveness and impact of educational programs and awareness campaigns aimed at children, parents, educators, and other relevant stakeholders.

Technological Measures: Evaluating the effectiveness, accessibility, accuracy and efficiency of technological tools and solutions implemented to enhance online child protection, such as age verification mechanisms, content filtering, and reporting mechanisms.

Partnerships and Collaboration: Examining the extent of collaboration between the government, industry, civil society organisations, and international bodies in addressing child online protection.

Data and Research: Assessing the availability and quality of data for research on online child protection. This will evaluate the monitoring and evaluation mechanisms in place to measure the impact of government strategies for online child protection.

International Cooperation: Evaluating the government's level of engagement and collaboration with international organisations, initiatives, and frameworks used in addressing child online protection.

Continuous Improvement: Assessing the government's dedication to continual strategy evaluation, modification, and improvement considering new trends, technological developments, and changing security dangers in the digital sphere.

The framework places a strong emphasis on the necessity of assessing the comprehensiveness and alignment of policies, the efficiency of enforcement and implementation efforts, the impact of educational programs and awareness campaigns, the effectiveness of technological tools, the strength of partnerships, the accessibility of data and research, the participation in global initiatives, and the dedication to continuous improvement.

4. CASE STUDIES

Country	Government Strategy	Strengths	Weaknesses	Outcomes
United Kingdom	Age-Appropriate Design Code (2019)	Focus on child protection and best interests	Compliance challenges for the industry	Improved online safety for children
New Zealand	Harmful Digital Communications Act (reviewed 2017)	Criminalises cyber abuse and harmful communication	Enforcement and monitoring challenges	Increased reporting and deterrence of abuse
Australia	eSafety Commissioner (established in 2015)	Dedicated government agency for online safety	Limited enforcement powers in some cases	Effective investigations and removal of harm
Canada	National Strategy for the Protection of Children from Sexual Exploitation on the Internet	Comprehensive strategy addressing child exploitation	Coordination and implementation challenges	Enhanced protection and support for children

4.1 Key Findings: The Current State Of Child Online Protection Strategies In Nigeria

The table below provides an overview of the current state of Nigeria's government strategy for online child protection. It denotes key aspects as highlighted in the evaluation framework: Policy and legislation, implementation and enforcement, education and awareness, technological measures, partnerships and collaboration, data and research, international cooperation and continuous improvements.

Component	State of Nigeria's Government Strategy for Child Online Protection
Policy and Legislation.	1. The Child Rights Act (2003) has been adopted by 34 out of 36 states in Nigeria. (TheCable, 2022). This domesticates the rights of children in the country. 2. The Nigeria Data Protection Regulation (2019) made provisions for child data privacy right under Part 2.4 and Part 3.1 3. The CYBERCRIME (PROHIBITION, PREVENTION, ETC) ACT of (2015) provides a legal framework for addressing cyber-related offences, including child pornography and cyberstalking. 4. The most important policy for the protection of Child Online Protection is the "National Strategy for Child Online Protection" - A comprehensive National Strategy for Child Online Protection is not released by the Ministry of Communication and Digital Economy.
Implementation and Enforcement	There have been few prosecutions specifically related to child exploitation under the existing laws rather than Child Online Protection.
Education and Awareness	The Nigerian Communications Commission (NUC), which is a government arm in Nigeria, recently launched an initiative to educate children and caregivers using indigenous languages following the ITU guideline. Efforts are also underway to incorporate online safety into the curriculum (Premium Times, 2019)
Technological measures	Aside from the traditional exploitation of children in Nigeria, which has provision for hotlines, there are no mechanisms for reporting online child threats. Content filtering is done primarily by social media platforms.
Partnerships and Collaboration	There are few but effective collaborations with national organisations such as the CSOs, International bodies such as ITU in terms of advancing Child Online Protection in Nigeria. It is worthy of note that the country has ratified the Budapest Convention on Cybercrime but is yet to join the Malabo Convention, which all have a component of child protection in the digital age.
Continuous Improvements	As a country with advancement in the digital economy, there is a commitment to increasing the overall sector of digital technology, including security. However, the operationalisation of Child Online Protection will determine the nation's commitment to continuous improvement in that area.

5. CHALLENGES AND FUTURE DIRECTIONS

Protecting children online has become very imperative and demands concerted efforts on all fronts

Fig 1: A Mother Examining Contents being viewed online by a Child
Source: https://www.istockphoto.com/photo/caring-mom-providing-childrens-online-privacy-protection-gm1199684762-343340861

Governments face several challenges in implementing effective child online protection strategies. These challenges include:

Rapid technological advancement: The constantly shifting digital environment makes it difficult for governments to stay on top of new internet hazards and adjust their strategy. Constantly emerging platforms, apps, and online habits necessitate ongoing monitoring and changes to address possible online threats.

Complexities related to jurisdiction: The internet's global reach creates problems for both jurisdiction and law enforcement. Due to the international nature of online crimes, it is challenging for governments to efficiently investigate and prosecute offenders. To resolve cross-border concerns, government participation and cooperation are essential.

Limited capacity and resources: Governments may experience resource shortages in terms of both financial and human capital. Adequate resources, qualified personnel, and a strong infrastructure are needed to implement comprehensive kid online protection plans that can successfully monitor, look into, and address online dangers.

Freedom of expression: This must coexist with respect for people's rights to privacy and freedom of expression, and child online protection programs must strike this balance. Finding the correct balance can be challenging since authorities must protect online security without overly limiting internet use or violating people's rights.

6. RECOMMENDATIONS FOR IMPROVING GOVERNMENT STRATEGIES AND ADDRESSING FUTURE CHALLENGES.

Government can follow the recommendations below to improve its strategies for online child protection.

Strengthen legislation and policy frameworks: Governments should enact comprehensive laws and policies specifically addressing child online protection, including clear guidelines on child online behaviour, age verification mechanisms, and consequences for offenders. Regular updates to these laws and legislation are necessary to keep pace with evolving online risks.

Enhance international cooperation: Collaboration and information sharing are important for Governments to address cross-border online offences that relate to child exploitation. This could include joint investigations, extradition agreements, and sharing best practices in combating child online risks.

Invest in education and awareness programs: Governments should prioritise educational initiatives that promote digital literacy, responsible online behaviour, and awareness of online risks among children, parents, educators, and communities. Education is key to empowering children to navigate the online world safely and enabling adults to effectively support and protect them.

Foster public-private partnerships: Collaboration with Civil Society Organizations (CSOs) and industry stakeholders, including technology companies, social media platforms, and internet service providers (ISPs), is crucial in developing and implementing effective child online protection strategies.

Regular evaluation and adaptation: Technology keeps improving; Hence, Governments should regularly assess the effectiveness of their child online protection strategies through comprehensive evaluations and engage in continuous improvement.

7. CONCLUSION

In conclusion, the paper discussed the importance of evaluating government strategies for child online protection safety and highlighted key points related to this topic. It emphasised the challenges faced by governments in implementing effective strategies and the impact of emerging technologies on child online safety and provided recommendations for improving government strategies and addressing future challenges. Evaluating government strategies for child online protection safety is crucial in the context of achieving sustainable development goals. The safety and well-being of children in the online environment are fundamental to their overall development and participation in society. By evaluating strategies, governments can identify strengths, weaknesses, and areas for improvement, leading to more targeted and effective interventions. This evaluation process ensures that efforts are aligned with the evolving nature of online risks and the changing needs of children.

REFERENCES

1. Akinyemi, A. I. (2022). Nigeria's large, youthful population could be an asset or a burden. Retrieved from https://www.premiumtimesng.com/news/top-news/544043-nigerias-large-youthful-population-could-be-an-asset-or-a-burden.html?tztc=1
2. Calif, S. (2020). Cybercrime to cost the world $10.5 trillion annually by 2025. Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
3. CHILD'S RIGHT ACT. (2003). Your preschool child's speech and language development. Retrieved from https://placng.org/lawsofnigeria/laws/C50.pdf
4. Esafety Commissioner (2016). eSafety Commissioner. Retrieved from https://www.infrastructure.gov.au/media-technology-communications/internet/online-safety/esafety-commissioner.
5. ITU (2020). ITU 2020 Guidelines on Child Online Protection (COP) respond to new challenges and significant shifts in the digital landscape. Retrieved from https://www.itu.int/en/mediacentre/Pages/pr10-2020-Guidelines-Child-Online-Protecion.aspx
6. Harmful Digital Communications Act (2015). Retrieved from https://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html
7. Introduction to the Children's code. (2018). Retrieved from https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/
8. Monyei, C. (2018). Children's online safety in Nigeria: The Government's Critical Role. Parenting for a Digital Future. Retrieved from https://blogs.lse.ac.uk/parenting4digitalfuture/2018/09/12/childrens-online-safety-in-nigeria/
9. Monyei, C. (2019). International Telecommunications Union (ITU) Child Online Protection (COP) Africa Forum. Retrieved from https://www.itu.int/en/ITU-D/Regional-Presence/Africa/Documents/COP%20Workshop%20Ghana%202019/Presentations/new/LAPT%20Presentation.pdf.
10. National strategy for child exploitation prevention and interdiction (2023). Project Safe Childhood. Retrieved from https://www.justice.gov/psc/national-strategy-child-exploitation-prevention-and-interdiction

11. TheCable. (2022). Child rights act has now adopted in 34 states, says the minister. Retrieved from https://www.thecable.ng/child-rights-act-now-adopted-in-34-states-says-minister
12. Nigeria Cybercrime (Prohibition, Prevention, etc.) Act, 2015. Retrieved from https://lawpadi.com/wp-content/uploads/2015/08/CyberCrime_ProhibitionPreventionetc_Act_2015.pdf
13. Pantami, I. I. (2022). "18.44% ICT contribution to GDP in Q2, highest ever." Retrieved from https://www.thisdaylive.com/index.php/2022/08/29/18-44-ict-contribution-to-gdp-in-q2-highest-ever
14. Premium Times (2019). Google, PPDC, NERDC partner on online safety initiatives for Nigerians. Retrieved from https://www.premiumtimesng.com/news/more-news/310419-google-ppdc-nerdc-partner-on-online-safety-initiatives-for-nigerians.html
15. United Nations. (n.d.). Child and youth safety online. United Nations. Retrieved from https://www.un.org/en/global-issues/child-and-youth-safety-online