PARTNERSWEST AFRICA NIGERIA
Rule of Law and Empowerment Initiative

info@partnersnigeria.org
@partnersnigeria
www.partnersnigeria.org
@partnersnigeria
Partners West Africa-Nigeria

A Policy Brief from the Promoting Informed Dialogues on Security Sector in Nigeria (PRIDES) project.

Rule of Law & Empowerment Initiative –Partners West Africa-Nigeria
1B Faith Crescent, Off Deeper Life Avenue, Kado, Abuja.
Phone: +234 (0) 8091257245

23rd September, 2017

Enhancing the use of Information, Communication and Technology (ICT) in Counterterrorism Policy and Practice

"The Internet is a prime example of how terrorists can behave in a truly transnational way; in response States need to think and function in an equally transnational manner[i]"

Executive Summary

There is a very good reason for which ICT is currently having a dramatic impact on human societies on a global scale. One area that such impact is felt is security in general and terrorism in particular. In the light of the foregoing, the United Nations General Assembly, through its Resolution 60/288, set up the Working Group on Countering the Use of the Internet for Terrorist Purposes[ii]. The goal was for Member States of the United Nations to "coordinate efforts at the international and regional levels to counter terrorism in all its forms and manifestations on the Internet" and "use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard".

In the case of Nigeria, since 2009, terrorist organisations such as the Jamaatu Ahlis-Sunna Liddaawati Wal Jihad (JAS), commonly referred to as Boko Haram (BH), leveraged on their access to ICT in transmitting information, mobilizing, recruitment and engaging in other forms of propaganda. Despite having a National Cybersecurity Strategy, the absence of a detailed and coordinated national action plan for the purpose of countering terrorism through the Internet and ICT in general, remain a major obstacle in Nigeria's current fight against terrorism.

Summary of Findings

(i) Nigeria only has a draft national communication strategy or policy, which constitute a key drawback for the country in its fight against terrorism;

(ii) The absence of a robust mechanism for coordination among all security and intelligence agencies, and their unwillingness to share intelligence seamlessly has hampered their effective response to terrorism.

(iii) The inability of Nigeria to ensure a centralized data-base of citizens remains a major security challenge, with specific reference to crime detection.

(iv) The use of open sourced email addresses and accounts such as '@gmail.com', '@hotmail.com', '@yahoo.com' among others, has negative national security implications for the country;

(v) The fact that there are no functional or operational short codes that would enable citizens to give intelligence and security related.

Summary of Recommendations

(i) The Federal Government of Nigeria should ensure a well thought out and proactive policy on counterterrorism, clearly defining how ICT acts as an enabler in its counterterrorism efforts;

(ii) The Office of the National Security Adviser (ONSA) should adopt a more proactive measure in coordinating the security and intelligence agencies towards better delivery of services related to counterterrorism;

(iii) From a national security standpoint, the ONSA should coordinate all efforts towards a centralized national database for all citizens in the country;

(iv) From a national security standpoint, security and intelligence agencies as well as all MDAs and the three arms of government should provide personalized dedicated email accounts in their official domains for all their staff and offices, as against the current use of open sourced emails that are liable to hacking;

(v) The security and intelligence agencies with ONSA in the lead, should work with the Nigerian Communication Commission (NCC), in establishing dedicated short codes that would aid citizens in providing intelligence and security related information promptly. The fact that these short codes are memorable makes it user-friendly for the citizens.

Background and Context

Apart from the Nigerian Civil War 1967 – 1970, Nigeria is currently facing one of its most existential threats since independence in the form of acts of terrorism by insurgent groups such as the BH. This adverse situation with an estimated 20,000 people killed and about 2 million others displaced, has placed Nigeria as one of the frontline states in the global war against terrorism.[iii]

One of the key force multipliers this terror group has used to its own advantage since 2009 is ICT. ICT became a veritable tool for crafting and disseminating messages and narratives for radicalizing as well as mobilizing and recruiting people that are remotely positioned from both the author and the uploader. In fact, much of the publicity gained by the group emanated from access to and use of ICT for its propaganda and indoctrination.

The use of ICT by terrorists is a phenomenon that has gained currency on a global scale. Its only by taking proactive and coordinated actions that leverage on the same ICT, though at a higher and more sophisticated level that the terrorists can be countered. The use of ICT in counterterrorism and national security on the whole has many benefits, which have to do with intelligence gathering and analysis as well as ensuring secure communication among others. In addition to the successes recorded in kinetic military operations against BH in the northeast, defeating terrorism in the ICT realm will go a long way in guaranteeing the success of the Nigerian state in its current fight against national, international, transnational and global security threats.

The prospects of information and intelligence sharing between and among security agencies are hampered by weaknesses that are associated with coordination, collaboration, coherence, and

unhealthy competition among security agencies. In this milieu, cyber-crimes are thriving and have become easy channels for criminals to defraud Nigeria and its citizens, as well as undermine the security of the country. In the case of BH, its members have used ICT for publicizing its ideology, intimidation and blackmail, recruitment of new members, coordinating, planning, and launching of attacks, as well as communication with its members and outsiders.

The role of ICT in improving human, national and transnational security has attracted a lot of attention recently. The digitalization of the database of criminal suspects would help in the tracking and apprehension of suspects in both civil and criminal investigations. Also, the use of digital criminal fingerprint database would help in tracking persons with multiple identities, bearing in mind, the centrality of ICT in cyber-crime, cyber-security and cyber-warfare among others. Generally, the presence of a secure national bio-metric data base of all citizens of certain ages will aid in no small way in accurate national planning and position security and intelligence agencies to conduct informed investigations and analyses for national security purposes.

Countries such as the United States, Sweden, Germany, Estonia and Israel have achieved giant strides in the use of ICT in surveillance, fraud detection, cyber-attacks and other military operations[iv]. In Pakistan, the Punjab Information Technology Board (PITB) developed Crime Mapping (CM) software that helps the police in conducting electronic crime investigation, devise better strategies to pre-empt, discover, and control criminal acts[v].

One of the successes recorded by Nigeria in the use of ICT is the biometric capturing of its citizens by key institutions and agencies such as the Federal Road Safety Commission (FRSC), Nigeria Immigration Service (NIS), National Identity Card Management Commission (NICMC), Independent National Electoral Commission (INEC), The Nigerian Telecommunication Companies, Federal Inland Revenue Service, as well as the Bank Verification Number (BVN). The key challenge lies in the inability of these databases to be synchronized and harmonized in order to have a central national database. In fact, the introduction of the BNV by the Central Bank of Nigeria (CBN) was both an economic and security decision. In these respects, the policy has helped in the centralization of customers identity on the economic side, while on the security side, the use of biometric technology in registering customers in the financial system, would help in tracking the end-to-end flow of funds as it relates to terrorism financing and other forms of financial crimes,

Key Findings

Despite the importance of ICT in the formulation of policies and strategies in counterterrorism efforts, the absence of a national action plan for the purpose of countering terrorism as well as the lack of a national communication strategy on the use of ICT for acts of terror, remain a major obstacle in Nigeria's current fight against terrorism.

Nigeria does not have a functional or operational short codes that would enable citizens to give information to the security and intelligence agencies. Such situation has become a major challenge in the context of efforts towards having a robust early warning and early response strategy for the country. By design, short codes, which are unique to each mobile operator, are easier to read and remember than the normal telephone numbers that are longer.

The use of generic addresses such as '@gmail.com', '@hotmail.com', '@yahoo.com' by

individuals and offices for official business among others, as against specialized email addresses within approved MDAs' domains, makes it difficult for information pertaining to national security to be protected. These are all open sourced email addresses that are vulnerable and susceptible to hacking by terrorists and other criminals.

The absence of functional or operational shot codes for citizens to promptly send information to security and intelligence agencies makes it difficult for effective feedback between citizens and these agencies. Despite the existence of a guideline on short code operation in Nigeria, as provided by the NCC, security and intelligence agencies have not been able to fully utilize such in the current fight against terrorism.

Recommendations

Since most ICT tools, from social networking sites to geospatial imaging among others, are mobile, flexible and integrative, security and intelligence agencies and other government actors in the security sector can take advantage of such tools to address critical security needs. This ought to be done with specific reference to countering terrorism, which constitute the single and biggest existential threat to Nigeria and Nigerians. There should be a well thought out and proactive policy on counterterrorism, clearly defining how ICT acts as an enabler. A group of determined, loyal and ICT savvy cadre of security professionals should drive this initiative.

ONSA should adopt more proactive measures in coordinating the security and intelligence agencies towards better delivery of services related to counterterrorism. It needs to be ensured that security agencies and other MDAs that are relevant actors in the sector desist from operative in stove pipes and appreciate the lessons learnt from 9/11 that dictate unquestionable coordination and collaboration vertically and horizontally within and between all agencies. ONSA should model the existing Nigerian e-Fraud Forum (NeFF) that is driven by the CBN in monitoring cyber-crimes[vi], in order to create a platform for the sharing of cyber security intelligence among the security agencies.

From a national security standpoint, the ONSA should coordinate all efforts towards a centralized national database for the country from the myriad of bio-data collected on individuals by all government agencies and departments as well as those private concerns under NCC. This will help in detecting crime easily, since no two people share the same identity. Also, the NPF should set up a National Forensic Laboratory in Abuja and operational laboratories for preliminary evaluation of evidence and analysis for investigation of crime at, at least three strategic locations across the country.

As part of efforts towards addressing the challenge posed by cyber-crime, the Federal Government of Nigeria through the agencies should launch a cyber-security initiative with mandate for ICT. The energies and professionalism of young persons engaged in fraudulent cyber activities should be transformed into legitimate cyber-security professionals who will carry out both offensive and defensive "legitimate" cyber tasks in pursuit of Nigeria's national interests. These individuals should be talent-spotted from universities and those ICT gurus that have fallen foul of the law and have come to the attention of intelligence and security agencies due to the "quality" of their work.

Security and intelligence agencies should collaborate with the NCC in the design and use of short codes for easy transmission of information and feedback with citizens. This is one of the most important ways that the gaps that exist in terms of

communication between government and citizens can be bridged. In the meantime, the architecture for the utility of the flood of information that will flow through the channel should be worked out and readied for implementation.

Conclusion

In order to effectively implement the counterterrorism strategy of the country, the security agencies must beef-up their capabilities for intelligence gathering, sorting, analysis and accurate interpretation within a deluge of unquantifiable chaff. The increasing uncontrolled use of open source platforms and social media tools would make the country and its citizens more vulnerable to terrorism, since terrorists also monitor the gaps in the national security and counterterrorism architecture to create havoc. If ICT is an enabler for terrorism, then, it can also be a key enabler for counterterrorism in Nigeria just like other in other climes. Although ICT as an enabler will boast security in the context of counterterrorism operations, it cannot function in a vacuum since greatest 'technology' is the human resource.

[i] This statement was made by Ban Ki-moon, the former Secretary General of the United Nations.

[ii] https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

[iii] Kwaja, A.M.C (2017) The benefits and challenges of de-radicalisation, rehabilitation and reintegration of repentant Boko Haram members in Nigeria, Working Paper, No.1, Centre for Peace and Security Studies, Modibbo Adama University of Technology, Yola, Adamawa State, Nigeria.

[iv] Kwaja, A.M.C (2017) Introduction of ICT within national environment in Nigeria: Tools for Coordination, Paper Presented at a Conference on Enhancing the Use of ICT in Counterterrorism Policy and Practice in Nigeria, organized by the Partners West Africa – Nigeria (PWA-Nigeria), Treasure Suites, Abuja, Nigeria, 23rd August 2017.

[v] See www.thediplomat.com/2016/12/how-pakistan-is-fighting-crime-and-corruption-with-technology.html

[vi] See https://www.proshareng.com/news/Frauds%20&%20Scandals/2015-Annual-Report-of-Nigeria-Electronic-Fraud-Forum-/31778