EXTREMISM

ISTOCK

ONLINE *in* NIGERIA

The country tries to counter Boko Haram's adept use of social media

TOMMY VICTOR UDOH, *Nigerian Defense Space Agency*

Social media refers to the wide range of Internet-based and mobile services that allows users to participate in online exchanges and online communities or contribute user-created content. The kinds of Internet services commonly associated with social media include blogs, wikis, social bookmarking, Twitter and YouTube, among others. Social media technologies provide a wide range of flexibility, adaptability and usability.

Terrorists and insurgent groups — in the case of Nigeria, the Boko Haram terrorist group — exploit social media for nefarious activities. This article offers an overview of Boko Haram terrorist activities in Nigeria, highlights the group's use of social media, considers government initiatives for countering terrorism using social media, and considers the wider challenges associated with terrorist use of social media.

BOKO HARAM ACTIVITIES IN NIGERIA

The *jamaa'atu ahl as-sunnah lida'wati wal jihad,* popularly known as Boko Haram, is a pseudo-Islamic terrorist group based in northeastern Nigeria. The group's nickname colloquially translates into "Western education is sinful." Thus, the group is opposed to Western education, ideologies and systems such as democracy.

Boko Haram was created in 2002 by Mohammad Yusuf, a radical Islamist cleric from Maiduguri, Borno state. The Boko Haram sect came to prominence in 2009 when it participated in sectarian violence in northern Nigeria. Yusuf was killed that year and replaced as leader by Abubakar Shekau.

Boko Haram has killed thousands of innocent citizens, destroyed numerous properties, including the United Nations building in Abuja, and abducted citizens, including the Chibok students. Boko Haram activities later spread to neighboring countries such as Chad, Niger and Cameroon.

The group has pledged allegiance to the Islamic State of Iraq and al-Sham (ISIS) and intends to represent that group's interests in the West African subregion. Though Boko Haram claims to oppose Western education, the group uses the Internet and social media to interact and promote its activities.

Use of social media

Once ISIS accepted Boko Haram's allegiance, its online activities expanded to copy ISIS' techniques. Subsequently, the groups adopted social media platforms such as Facebook, Twitter and YouTube because of their cheapness, convenience and enormous reach beyond borders or nationality. Social media has enabled Boko Haram to release messages directly to its audience without intermediaries. Like most terrorist groups, Boko Haram uses cyberspace — especially social media — for recruitment, propaganda, fundraising and communication.

Recruitment

With the help of the Internet, Boko Haram gets wide access to vulnerable young people. Social media is used to entice the audience. To reach more recruits and evade media platform policies, Boko Haram began addressing the public informally. For instance, it targeted Twitter users who appear open to its ideas. Although some are lured into participating in terrorist acts for financial gain, many recruits from rich and middle class families are enticed by the extreme material the group spreads online.

Propaganda

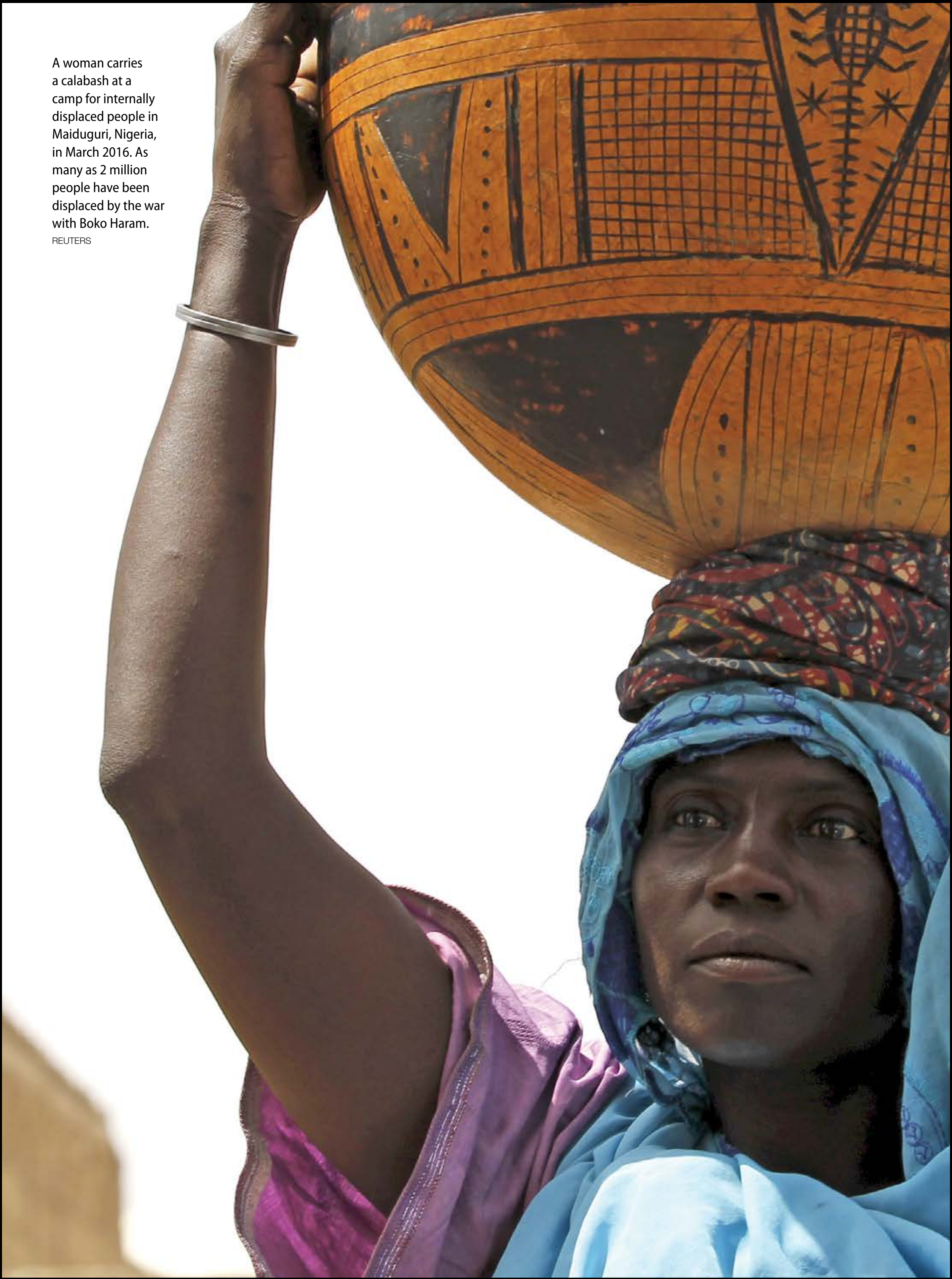
At the onset, Boko Haram disseminated its propaganda through radio messages and distributed its footage to international media such as Agence France-Presse through the use of middlemen. Later, the group graduated to Twitter, where it posted videos and photos showing the killing and beheading of security agents. Similar clips were posted on YouTube and translated into Arabic, presumably to capture a larger audience. The pictures and clips sometimes feature idyllic scenes of villages and people living their lives seemingly without fear and pledging support and allegiance to the group.

Fundraising

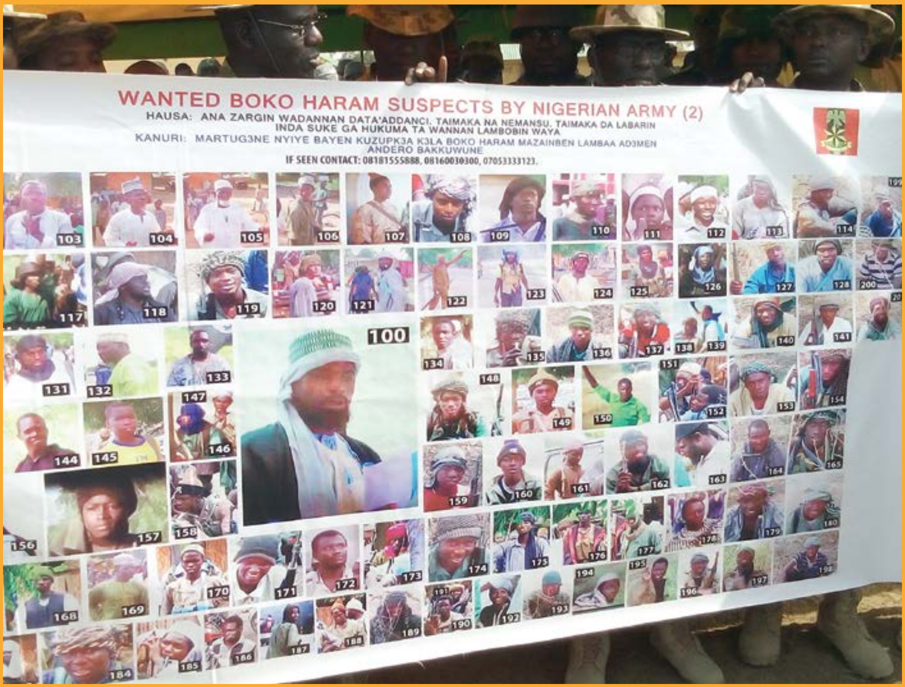
As the size, scope and structure of terrorist organizations have evolved, so too have their methods of raising and managing money. The rapid expansion of social media has been exploited by terrorist groups to raise funds from sympathetic individuals and organizations globally. Widespread access to the Internet and its relative anonymity encourages exploitation by terrorist fundraisers. Innocent citizens have been lured via social media and kidnapped to sometimes be exchanged for ransom from relatives or employers. The group also uses social media fundraising with prepaid cards and large-scale crowdfunding schemes using e-wallets. The money is used to recruit, motivate and train volunteers; procure arms, ammunition and explosives; spread propaganda; and conduct research and development.

Communication

Social media is becoming the primary means of keeping in touch with one another and with traditional media sources and channels of public



A woman carries a calabash at a camp for internally displaced people in Maiduguri, Nigeria, in March 2016. As many as 2 million people have been displaced by the war with Boko Haram.
REUTERS


WANTED BOKO HARAM SUSPECTS BY NIGERIAN ARMY (2)
HAUSA: ANA ZARGIN WADANNAN DATA'ADDANCI. TAIMAKA NA NEMANSU, TAIMAKA DA LABARIN INDA SUKE GA HUKUMA TA WANNAN LAMBOBIN WAYA
KANURI: MARTUG3NE NYIYE BAYEN KUZUPK3A K3LA BOKO HARAM MAZAINBEN LAMBAA AD3MEN ANDERO BAKKUWUNE
IF SEEN CONTACT: 08181555888, 08160030300, 07053333123.
100

Pictures of 100 wanted Boko Haram suspects are displayed on a poster released by the Nigerian Army in the northeastern town of Damboa in February 2016. AFP/GETTY IMAGES

communication. Social media allows this generation to experience the full reality of English poet John Milton's view of the "free market of ideas" where falsehood and truth are seemingly published concurrently by new media users. Boko Haram employs communications platforms such as Skype, chat groups, Instagram, Twitter, Facebook and WhatsApp. The terrorist group chooses these channels of communication because of their low cost, ease of use, and anonymity. Communication can reach those near or far and links terrorists groups to ISIS to share ideas or raise money.

COUNTERING TERRORIST SOCIAL MEDIA USE

Financial intelligence gathering

The Bank Verification Number (BVN) program strengthens the security of banking transactions and improves national financial intelligence collection. This government initiative improves detection of laundered money and shares information on emerging risks. Unique BVNs in Nigeria make it easier for banks to manage depositors' identities regardless of the number of accounts they have. The program has reduced the practice of depositors using multiple identities to launder funds through various banks and accounts. With the BVN, banks can track irregularities within accounts. The area of focus extends to identifying and targeting financial collection/aggregation/accounting points among criminal and terrorist organizations. BVNs allow law enforcement agencies to focus on the recipient of the funds, rather than just the source.

Cyber security program

The federal government of Nigeria has championed a national cyber security program that encompasses the Cyber Security Policy and Strategy and the Cyber Crime Law. The Cyber Crime law provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cyber crime in Nigeria. This law ensures the protection of critical national information infrastructure, and promotes cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights. It mandates that service providers retain all traffic data and subscriber information with regard to an individual's constitutional right to privacy and take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved.

Computer emergency response team

The Nigeria Computer Emergency Response Team was established to monitor and respond to security incidents within the nation's cyberspace — both proactively and reactively. The proactive service protects and secures Nigerian cyberspace in anticipation of attacks, problems or events. The services include technology watch, intrusion detection services, vulnerability assessment and penetration testing. The reactive services are designed to respond to requests for support against any threats or attacks on information systems in Nigeria's cyberspace. This includes incident analysis, on-site incident response, incident response coordination, incident response support, forensic evidence collection and forensic analysis.

Strategic online narratives

The strategic online narrative is a statement of identity, cause and intent, behind which the Nigerian government, the people and the Armed Forces are uniting in the fight against terrorism. It is propagated consistently to Boko Haram members, the general populace and security forces. The counternarrative for Boko Haram members, which is consistently disseminated, promotes a moderate form of Islam. It suggests that the Holy Prophet never killed innocent children or kidnapped women to propagate the Islamic cause. It further enjoins them to be true Muslims and surrender or submit to the authorities, who will embrace and treat them well. The narrative for security forces strengthens their morale and reminds the troops that the cause they are fighting is just.

Social media crisis communication centers

Crisis communication centers can monitor social media activities. The center involves civil society, the press, social media enthusiasts/activists, young people and nongovernmental organizations that share ideas and provide information to counter violent extremist ideology.

Detecting and preventing online terrorist activity

Nigerian security agencies have acquired modern technology to help collect information on terrorism. This technology enables the lawful interception of electronic communication when there are reasonable grounds to suspect that the content is required for the purposes of a criminal investigation or proceedings.

Public education and warning alerts

The government urges Nigerians to be vigilant and volunteer information to authorities to enable security agencies to prevent Boko Haram attacks. Similarly, tips for spotting a terrorist and forwarding information that can lead to an arrest are circulated online. Social media platforms are littered with sponsored dramatic sketches, as well as the use of comedy, musical clips, jingles, testimonies from surrendered and deradicalized Boko Haram members, and documentaries. Additionally, leaflets and factual press releases are distributed in Boko Haram controlled areas and at civil-military cooperation activities, at the operational and tactical levels, in the areas of health care and infrastructure.

SOCIAL MEDIA CHALLENGES

Changing tactics

It has proven difficult over time to distinguish between sympathizers, supporters and actual terrorists. The identification of those contributing money, either intentionally or unwittingly, is a serious challenge for security authorities. It is difficult to obtain evidence associated with the use of terrorist funds when money is transferred via the Internet. Social networks could be used to show relationships, but finding proof is still difficult.

Privacy versus security

Sometimes it is beneficial for government to block a citizen's access to websites or servers used by terrorists. However, when considering the right of freedom on the Internet, it becomes difficult to implement such policies.

Denying access to known terrorists

YouTube, Twitter and Facebook are some of the social media platforms often used by terrorists like Boko Haram for propaganda. When a known terrorist leader like Abubakar Shekau posts a propaganda video on social media, it is always difficult to get the cooperation of the owners or the administrators of such platforms to deny the terrorists the use of their platforms/servers, even when the user is a known terrorist.

CONCLUSION

Boko Haram terrorists in Nigeria, like other terrorist organizations, have continually tried to exploit social media for recruitment, propaganda, fundraising and communication. The Nigerian government is mindful of the risk inherent in cyberspace. Therefore, for its citizens to continue to benefit from the full potential of the information and communications technology revolution, it must take cyber risks seriously. It is against this backdrop that the government is determined to confront threats, uphold and support the openness of cyberspace, as well as balance security with respect for privacy and fundamental rights.

The government of Nigeria is constantly embarking on new initiatives to counter terrorists' use of social media through comprehensive national cyber security programs, the use of financial intelligence to track funds and the establishment of a communications center to counter terrorist ideology and radicalization. Other initiatives include Internet surveillance, censorship, cyber operations, as well as mass education and public awareness.

Several challenges still exist, and efforts are ongoing to overcome them. These challenges include the ability to identify funds transferred through social media and why the money is being transferred. Another challenge is striking a balance between citizens' freedom on the Internet and national security. Lastly, the difficulty in getting owners and managers of social media platforms to deny access to known terrorists is also a challenge. □