Review Pub Admin Mang

An Open Access Journal
• ISSN: 2315-7844

ARABIAN GROUP OF JOURNALS

Review of Public Administration and Management

ROPAM

Research Article | Homepage: www.arabianjbmr.com | AGJ

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) AND TERRORIST ORGANIZATIONS

Adeyemi Adewumi Ayomide
Prof. David Oladimeji Alao
Babcock University, Ilishan, Nigeria.
Email: adewumiadeyemia@gmail.com
Email: Alaoda@babcock.edu.ng

ABSTRACT

The advent of Information and Communication Technology at the end of the 20th Century has brought about a lot of transformation globally. Its consistent stream of development has resulted in the inventions that have not only filled the world with high technological gadgets, but have also eased communication and the transfer of information globally. Although, most ICT users use it to better their lives, it has also constantly been linked to performing terrible acts by some people and organizations such as terrorists to advance their cause.. This informed this paper to examine the various ways through which the terrorist organizations (Boko Haram and ISIS) make use of ICT to achieve their goals and the implication on global security. It is a descriptive paper that relied on secondary data sources. it found that terrorists use ICT majorly for fund raising, Networking, propaganda, recruitment and psychological warfare with grave consequences on global security. It concluded that terrorism remains a monster that threatens the stability of all nations and terrorist organizations continue to take advantage of ICT to sustain their existence. It is recommended that nation states, International Organizations and ICT service providers reach an agreement that will enhance an information sharing relationship amongst them, as this will enable the government to be able to handle terrorist threats to ICT usage more effectively.

1. INTRODUCTION

Information and Communications Technology (ICT) has become an important component of life. It has provided enormous amount of information and enabled relatively cheap and instant communication across the world. To a large extent, it has made life easier by solving communications problems and its continuous growth over the years has had great impact on our society, making a lot of lives and activities to depend heavily on its usage. Although ICT users use it to ensure improvement in socio-economic life, it has also constantly been linked as a tool for performing terrible acts by some people and organizations some of which include terrorist groups. Terrorist groups make use of ICT to advance their dangerous objectives because of its ease of manipulation and its easy accessibility with little or no restrictions as rightly observed by Oremus, (2011). The continuous development of ICT have also shifted the concept of national security. The transition into the ICT age has been accompanied with a series threats to the national and international security. Today, nations face the danger not only of physical attack but also having their information infrastructures destroyed, altered or incapacitated by the new genre of offensive technologies. A case in mind is the September 11, 2001 attack on the United States in which it has been widely reported that the terrorists made use of ICT tools to plan and carry out the attack (Oremus, 2011). The irony is that the ICT tools used were common tools like mobile phones, e-mails, and the internet. These destructive usage of ICT by the terrorist organizations informed this study to examine the various ways it has been using the technology and the challenges it poses on global security. The paper is descriptive and relied largely on secondary data sources such as relevant textbooks, journals, Internet sources and documentary evidences. The data sources and contents were critically interrogated to minimize possible subjectivity since some dealt with social issues and personal opinion.

2. CONCEPTUAL REVIEW

2.1 ICT

According to a United Nations report (1999), ICT cover Internet service provision, telecommunications equipment and services, information technology equipment and services, media and broadcasting, libraries and documentation centers,

commercial information providers, network-based information services and other related information and communication activities. Pelgrum and Law (2003) traced the origin of the popularity of ICT to the end of the 1980s when the term 'computers' was replaced by 'IT' (Information Technology) signifying a shift of focus from computing technology to the capacity to store and retrieve information. This was followed by the introduction of the term 'ICT' (information and communication technology) around 1992, when e-mail started to become available to the general public (Pelgrum& Law, 2003). According to Sulaiman (2010), the two major components of ICT include computers and the Internet.

There is no doubt that globalization itself was fueled by new developments in ICT. Advances in ICT, knowledge and information sharing have transformed globalization process making the world a "global village" (Dalgish, 2006). This connectedness between ICT and globalization is therefore viewed as a pillar for the strengthening of globalization activities (Ogunsola, 2005). The understanding of the role of ICT in the interaction of world societies is very important to understanding the complex structures, institutions and processes of globalization (Mabiza, 2016). This cannot but inform non-state actors like terrorists to key in to the benefits derivable from ICT in the planning, recruitment of foot soldiers and launching of coordinated attacks particularly by Boko Haram and Islamic State.

2.2 Terrorism

Terrorism is complex term, meaning different things to different category of people. The difficulty associated with is a function of whether one is an agent or victim of terrorism. Hoffman (1998:3) therefore notes that If one identifies with the victim of the violence, for example, then the act is terrorism. If, however, one identifies with the perpetrator, the violent act is regarded in a more sympathetic, if not positive. Kegley, (1990:13) notes that it is a value laden subject that is difficult to give precise definition. Sick in Kegley, 1990:52) therefore adds that "The cliché that 'one man's terrorist is another man's freedom fighter' is no less true for being trite" In their work, Schmid and Jongman, 1988 dissected hundreds of definitions of terrorism and came up with common elements. They discovered five elements with more than 40 per cent frequency of which 83.5% associated the term with violence or force. 65% views it as political violence while 51% identified elements of fear or terror. Threat recorded 47% and psychological effects and anticipated reactions received 41.5%. Crenshaw in Sick, (1990:53) sees terrorism as "The deliberate and systematic use or threat of violence to coerce changes in political behavior. It involves symbolic acts of violence, intended to communicate a political message to watching audiences". The Department of State and the Central Intelligence Agency use Title 22 of the U.S. Code—Section 2656f (d) defines it as "Premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience".

Pillar (2001:13-14) came up with some basic elements of terrorism which are prominent in governmental cycles and these are that their actions are premeditated, politically motivated, don't obey rules of military engagement, the targets are noncombatants while perpetrators are either sub-national groups or clandestine agents. It has also been observed that terrorist acts are by nature symbolic and not instrumental and this explains why the victims of the attack are largely not the intended targets. However, a critical analysis of the operational strategies of Boko Haram and Islamic State reveal that some of the basic elements have undergone transformation. Terrorists now freely attack combatant forces without restriction, there are state sponsored terrorist groups while they attempt to control territories. This transformation could to a large extent be linked with the advent of ICT that has made information gather, communication, fund raising and coordinated attack relatively easy.

3. THEORETICAL FRAME WORK

Proponents of this theory of framing include Ervin Goffman in his 1974 book titled Frame analysis: an essay on the organization of experience. Other proponents include; Fairhurst (1996), Scheufuele and Tewksbury (1999). This theory states that the way an issue is presented influences the way the issue is viewed and accepted and finally the decisions they take and the choices people make concerning that particular issue. It could also be said to mean that, the way information is presented can have an influence on how it is interpreted or understood by the audience (Scheufele& Tewksbury, 2007). One of the core assumptions of framing is that the way in which the news is brought, the frame in which the news is presented, is also influence the choice made by the presenter. Thus a frame refers to the way information is organized and presented and the way audiences interpret what they are provided. Frame influence the perception of the information to the audience and not only tells them what to think about, but also how to think about it. This theory is relevant to this study because it best captures terrorists growing interest in social media. Terrorism has now shifted from physical casualties to psychological casualties. Terrorist are more concerned about their popularity and how they are viewed by the growing online international community than how many people they kill or harm. So they construct messages that disseminate information about their activities and exaggerate those messages so it leaves a lasting impression on their numerous audiences.

4. WAYS THROUGH WHICH TERRORIST ORGANIZATIONS MAKE USE OF ICT

Makatiani, (2016:8) observes that the use of E- services is expanding in globally while it offers a wide range of services ranging from online shopping, filling tax returns, cashless policy introduction and the use of Bank Verification Number (BVN). According to Clement (2020), about 4.57 billion people are connected to the Internet as at April 2020 and the terrorists inclusive. Goodman (2008) in effect observes that strategies often used by terrorists are internet enabled through which they

raise fund, exchange communication, promote their ideologies, transfer money and engage in propaganda. Of importance is the use to collect and send operational information, booking and ordering supplies among others. This might have informed, Margaret Thatcher cited in Muller et al.,2003 saying that, "publicity is the oxygen of terrorism." Hoffman (2006) observed that without the use of ICT to capture and transport these terrorists acts, their impact is arguably wasted, remaining narrowly confined to the immediate victims of the attack, rather than reaching the wider 'target audience' for whom the terrorists' violence is actually aimed." Similarly, Brigitte Nacos agrees with Hoffman that, "without massive news coverage, the terrorist act would resemble the proverbial tree falling in the forest: if no one learned of an incident, it would be as if it had not occurred" (Nacos, 2000).

The specific ways are presented below:

4.1 Psychological warfare

Terrorism has often been conceptualized as a form of psychological warfare with the main aim to instill fear in the heart of its audiences. Clearly, terrorist groups have decided to wage this warfare through the use of ICT. The internet is one of the various ICT tools that have been adopted to achieve this. The Internet, which is an uncensored medium that carries stories, pictures, threats, or messages regardless of their validity or potential impact is especially suited to allow even anyone or any group to send messages and exaggerate its importance and the threat it poses (Weimann, 2014).This term is used to denote any action which is practiced mainly by emotional methods with the aim of evoking a planned psychological reaction in other people (szunyogh, 1955). Clearly, terrorist groups have decided to wage this warfare through the use of ICT. The Internet is an Information Technology that is being used to spread misinformation, deliver threats intended to generate fear and helplessness, and to share horrific images; an example is the brutal murder of the American journalist Daniel Pearl by his captors, a videotape of which was replayed on several terrorist websites (Montclos, 2014). Boko Haram's social media propaganda reportedly often focuses on anti-state grievances, as well as on displaying the group's weapons and tactics (RAND, 2017). The group's early propaganda strategy centred on Yusuf's recorded and open air lectures (Olawale, 2013). ISIS runs an active online propaganda campaign: a 2015 report found that the group releases a total of 38 new items per day, ranging from videos and documentaries to audio clips and online pamphlets (Winter, 2015). The group's online propaganda content is often extremely violent, with beheadings and killings posted openly to mainstream media sites including Twitter, Facebook and YouTube (Koerner, 2016). However, in recent years the group has also distributed online propaganda glamorising life in the Caliphate in order to attract foreign fighters and skilled workers to the group (al-Britani, 2015). ISIS also uses narrowcasting, creating varied content that caters to niche audiences, which portrays public works projects and acts of benevolence in order to draw popular support from Muslims worldwide (Koerner, 2016).

4.2 Fund raising

Like many other political organizations, terrorist groups use the Internet to raise funds. Since the 9/11 terrorist attack, terrorist groups have increasingly relied on the Internet for finance related activities. Fundraising is the process of soliciting and gathering contributions by requesting donations, often in the form of money. Some of the ways through which terrorist groups raise funds online includes: donations, auctioneering and drug trafficking. Popular terrorist organization websites often have links such as "What You Can Do" or "How Can I Help". Terrorist websites publish requests for funds by appealing to sympathetic users to make generous donations and contribute to the funding of their various attacks. Visitors to such websites are monitored and researched. Repeat visitors or individuals spending extended periods on the websites are contacted (Piper, 2008). Most of these individuals are guided to secret chat rooms or instructed to download specific software that enables users to communicate on the Internet without being monitored (Nordeste, 2006).

Popular terrorist organization websites often have links such as "What You Can Do" or "How Can I Help". Terrorist websites publish requests for funds by appealing to sympathetic users to make generous donations and contribute to the funding of their various attacks. Visitors to such websites are monitored and researched. Repeat visitors or individuals spending extended periods on the websites are contacted (Piper, 2008). Most of these individuals are guided to secret chat rooms or instructed to download specific software that enables users to communicate on the Internet without being monitored (Nordeste, 2006). Drug trafficking is considered a large income source for terrorist groups. Fake Internet drugs are trafficked, containing harmful ingredients such as arsenic, boric acid, leaded road paint, polish, talcum powder, chalk and brick dust. In an elaborate scheme, Americans were tricked in believing they are buying Viagra, but instead they received fake drugs. The money paid for these drugs is used to fund Middle Eastern terrorism (Whelpton, 2009).

ISIS has manipulated ICT when it encouraged donations and conducted a marketing campaign in a manner that is consistent with industry standards established by major crowd funding companies. Crowd funding is a method of drawing donations from a large group of people through a combination of technology and marketing. Leading crowd funding platforms have used statistical analysis to optimize online crowd funding campaigns through the encouragement of perks or donation tiers. (Indiegogo, 2014). This terrorist organisation has through the use of ICT extorted funds from Politicians and citizens and have threatened them with harm to themselves or their families if money was not paid

(Pate, 2015). Nigerian citizens have received text messages, emails, social media and phone calls demanding money with the threat of harm to the individuals and their family if they did not pay the amount being asked (Obi, 2014).

4.3 Recruitment

Information and Communication's Technology has be used not only to solicit donations from sympathizers but also to recruit and mobilize supporters to play a more active role in support of terrorist activities or causes. The New York Times, 2015, reported a case of a young woman in the United States who had been communicating with ISIS recruiters' online (New York Times, 2015; pp. 5). The woman claimed that the recruiters connected with her through social media and explained how they (ISIS) gradually indoctrinated her to believe that the western media had exaggerated ISIS atrocities (New York Times, 2015). Sara Khan, a director at the anti-extremist group Inspire, found that terrorist groups recruit on 'common social media sites'. She further gave an instance of a Twenty-year-old Aqsa Mahmood, who travelled to Syria to become a "jihadi bride" in 2013 and has since thought to have been promoting terrorism via ICT. "The sad reality is that these terrorist organizations make use of thousands of extremist websites - all claiming to speak in the name of religion" (New York Times, 2015). ISIS is said to favor online recruitment methods over offline (physical) recruitment activities (Awan, 2017). Twitter has been the main platform for ISIS's recruitment efforts (Awan, 2017). Berger (2015) also noted that recruiters have also used other instruments of ICT, including Kik, WhatsApp, Facebook, Telegram and Ask.fm to recruit followers. ISIS has used Twitter to radicalise students in certain cases, by first sharing information with them relating to job opportunities, before shifting the conversation in order to influence the youth to join ISIL (RAND, 2017). It has also been suggested that different social media platforms are used in different countries to recruit individuals, citing the example of Sudan where Twitter and Facebook are reportedly the primary tools for recruiting followers' online (RAND, 2017).

5. EFFECT OF CONTINUOUS USAGE OF ICT BY TERRORIST ORGANIZATIONS ON GLOBAL SECURITY

The prolific use of ICT by terrorist organizations has greatly enhanced their ability to disseminate information. The world has been confronting a surge in terrorist propaganda and training available via the Internet and social media. Due to online recruitment, indoctrination, and instruction, terrorist organizations are no longer dependent on finding ways to get terrorist operatives into other countries to recruit and carry out acts of terrorism. Terrorists in ungoverned spaces (both physical and virtual) readily disseminate propaganda and training materials to attract easily influenced individuals around the world to their cause. They motivate these individuals to act at home or encourage them to travel. This is a significant transformation from the terrorist threat our nation faced a decade ago (Wray, 2019)

The hybrid communication structure of extremist terrorist groups as facilitated by ICT has the tendency to promote threat to international security and world peace. This is because of the user-friendly platform which makes it easy for sharing information like propaganda with the intension to cause fear and psychological war to be distributed online. This finding agrees with the views of Goodman, Kirk and Kirk (2014) that there are many characteristics of the Internet, or cyberspace as they refer to it, that creates an environment conducive to the promotion of the ideas and ideals of terrorist organizations. These include anonymity, confidentiality, accessibility, low costs, intelligent interfaces, ease of use and the "force multiplier". ICT provides users with an uncensored and essentially anonymous forum, which they can use as a means of conducting research, gathering intelligence and creating communication networks. Moreover, studies on terrorist communication have revealed a concern for the protection of anonymity, for example many posts on terrorist websites inform "users" of ways in which they can avoid spyware and surveillance. Furthermore, the free availability of encryption programs has also provided terrorist organizations with the ability to communicate with one another via secure conduits without "detection." In addition, it is also extremely difficult to effectively track terrorist communications when they are utilizing emails, as account information is usually anonymous, or the email messages are encrypted.

Also, the paper agree with the findings of Cronin (2016) that the increased availability of and access to ICT, specifically the Internet, has made it much easier for terrorist organizations to communicate, plan and coordinate attacks. Thus, ICT has essentially aided terrorists in their aims and could be said to have facilitated international terrorism. Furthermore, the mere existence and evolution of cyberspace has created a new type of terrorism that could possibly be used in conjunction with traditional terrorist attacks. It is however important to note that technology has not encouraged international terrorism, but that it has only aided/facilitated it. It is argued that globalization has also allowed terrorist organizations to move and reach across international borders in the same way that business and commerce do. In addition, terrorist organizations often make use of the same channels as business and commerce.

6. CONCLUSION AND RECOMMENDATIONS

The study concludes that the introduction of ICT and the usage has both positive and negative consequences with attendant implication on global security because it has become an accepted medium of communication globally that has been convenient for terrorist organization to promote their ideologies, plan and coordinate their attacks. The paper recommends that though ICT has come to stay, the governments should seek for advance technology to counter the propaganda of the terrorist. Also, the paper advocates to stronger international collaboration to checkmate the unlawful use of ICT and through

Interpol, culprits should be made to face stiffer penalty. Terrorism flourish when there are societal discontentment, the paper advocates inclusive governance to minimize societal strife and disaffection.

REFERENCES

Awan, I. (2017). Cyber-Extremism: ISIS and the Power of Social Media. Social Science and Public Policy 54 (2): retrieved from; https://link.springer.com/article/10.1007/s12115-017-0114-0

Berger, J. (2014). How ISIS games twitter .retrieved from, www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media- strategy/372856/.

Berger, J.M. (2014). Following the money men. retrieved from http://news.intelwire.com/2014/06/following-money-men.html,

Clement, J. (2020). How many people use the internet? *Worldwide digital population as of April 2020.* Retrieved from https://www.statista.com/statistics/617136/digital-population-World wide/. Accessed June 21,2020

Crenshaw, "Causes of Terrorism," p. 94; and Feliks Gross,Violence in Politics: Terror and PoliticalAssassination in Eastern Europe and Russia, Studies in the Social Sciences 13 (The Hague:Mouton, 1972), p. 90.

Cunningham, Jr. W G (2003) "Terrorism Definitions and Typologies" in Terrorism: Concepts, Causes, and Conflict Resolution. [Online] Available: http://terrorism.about.com/od/causes/a/causes_terror.htm. (June 28, 2012).

Dalgish, C (2006). From globalization to the 'global village' Pages 115-121 |https://doi.org/10.1080/14781150600687833

Gerges, F.A. (2005). The far enemy, why Jihad went global. New York: Cambridge University Press.

Goodman, J. (2008). Terrorism in the West 2008 : A Guide to Terrorism Events and Landmark Cases. https://www.bookdepository.com/publishers/Foundation-for-Defense-of-Democracies

Hoffman, B. (2006). Inside terrorism (revised and expanded edition). Columbia University Press: Frank Cass

Hoffman, Bruce. (1993). Holy Terror: The Implications of Terrorism Motivated By Religious Imperative. RAND Paper P-7834, Santa Monica, CA: RAND.

Indiegogo, P. (2014). Creating your campaign. Retrieved from https://go.indiegogo.com/playbook/life-cycle-phase/creating-campaign

Kegley, Charles W., Jr. (ed.). (1990). International Terrorism: Characteristics, Causes, Controls, New York: St. Martin's Press

Koerner, B. (2016). 'Why ISIS is winning the social media war.' Retrieved from; https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat

Mabiza, Junior & Edoun, Emmanuel & Ezeanyika, Samuel. (2016). The impact of information and communication technology (ict) on globalisation.

Montclos (2014). Nigeria's Interminable Insurgency? Addressing the Boko Haram Crisis. chatham house

Nordeste, B. &Carment, D. (2006), " Trends in terrorism series: A framework for understanding terrorist use of the internet ", ITAC, vol. 2006-2, pp. 1-21.

Ogunsola, L. & Aboyade, W.. (2005). Information and Communication Technology in Nigeria: Revolution or Evolution. Journal of Social Sciences. 11. 10.1080/09718923.2005.11892487.

Olawale, I. (2013). Radicalisation and Violent Extremism in West Africa: Implications for African and International Security. Conflict, Security and Development; 13 (2). Retrieved from; http://www.tandfonline.com/doi/abs/10.1080/14678802.2013.796209

O'Sullivan,A. & Steven M. (2003). Economics: Principles in action. upper saddle river. p. 453. Pearson prentice hall; New Jersey.

Pelgrum, W. J. & Law, N. (2003).ICT in education around the world: trends, problems and prospects.retrieved fromwww.worldcatlibraries.org/wcpa/ow/02d077080fcf3210a19afeb4da09e526.html.

Pillar, P (2001) Terrorism and United States foreign policy; brookings institution press, Washington DC

Piper, P. (2008), Nets of terror: Terrorist activity on the internet; vol.16, issue 10.

Schmid, A., and A. J. Jongman. (1988). Political terrorism. Amsterdam: North-Holland Publishing.

Sulaiman, S. (2010). The state of ICT in Nigeria and its economic implicationshttp://www.scnbd. com/doc/31835015/ The-State-of-ICT-in-Niqeria Retrieval Date 10/04/2020

Szunyogh, B. (1955). Psychological warfare; an introduction to ideological propaganda and the techniques of psychological welfare. United States: William-Frederick Press

U.S. Dept. of State (DoS). (2001). U.S. Statement to OSCE on Addressing the Causes of Terrorism. Statement delivered by Amb. David T. Johnson to the OSCE Permanent Council, Vienna, Austria, November 1, 2001, www.usinfo.state.gov.

Weimann, G. (2004). United States institute of peace: How modern terrorism uses the internet. Retrieved from www.usip.org.

Whelpton, J. (2009), Psychology of cyber terrorism in cyber-terrorism; Ekwinox, South Africa

Winter, C. (2015). Documenting the Virtual "Caliphate". Retrieved from; http://www.quilliaminternational.com/wp-content/uploads/2015/10/FINAL-documenting-thevirtual-caliphate.pdf

Wray, C. (2019). Global terrorism: Threats to the homeland. FBI security statement. Retrieved from https://www.fbi.gov/news/testimony/global-terrorism-threats-to-the-homeland-103019