The Centre for the Study of Terrorism and Political Violence
Journal of Terrorism Research

Articles

Sub Saharan African Terrorist Groups' use of the Internet

by Stewart Bertram and Keith Ellison

Introduction

Recent actions by French military forces in Niger and the global prominence of terrorist groups such as Al Shabaab and Boko Haram, have highlighted the growing counter terrorist focus on the countries of Sub Saharan Africa. Additionally in a post Bin Laden world and with the immanent withdrawal of coalition combat troops from Afghanistan, there is the possibility of Africa as a continent becoming the new front in the Global War on Terror (*Mben* et al., 2013). However, it is a mistake to assume that Africa's story is uniformly one of violence and death. Vibrant cultures and a rugged entrepreneurial spirit have combined with a robust Internet backbone, to create the embryonic emergence of high tech hotspots across Africa. With rising IT literacy levels, more and more Africans are becoming connected to the information super highway on a daily basis (Graham, 2010). A tiny minority of these Africans are terrorists.

Sites such as Al Shabaab's Twitter feed have been highly graphic in their content and both blatant in their promotion of terrorism as a legitimate practise, and notable in how easily accessible they are for the common Internet user. Indeed as of the date of this study the phrase "Al Shabaab Twitter Feed" is one of the suggested searches in the Google search engine when the name Al Shabaab is entered, showing how well trodden in digital terms the path to the Al Shabaab Twitter Site has become.

While the presence of Sub Saharan African terrorist groups on the Internet is obvious, there are many questions that examine the issue on a more granular level that remain unanswered. *Are the terrorist website publishers of Sub Saharan Africa actually resident in Africa? What is the preferred web-publishing technology for terrorist web publishers in Sub Saharan Africa? What is the geographic distribution of terrorist groups publishing in Sub Saharan Africa? Who are the target audience for the terrorist publishers of Sub Saharan Africa?* These are all questions that remain unanswered regarding Sub Saharan African terrorists relationship to the Internet.

The core objectives of this study were threefold. Firstly and most immediately, the research seeks to quantify the web presence of terrorist groups active in Sub Saharan African. Secondly, the study seeks to explore the relationship between web technology availability and adoption by terrorist groups, and if one factor precipitated another i.e. do terrorist groups merely follow the technological trends that surround them or do they use web technologies in a unique way? Thirdly, the study seeks to advance the methodology of terrorist netnography (as defined by Kozinets, 2009) by explicitly differentiating between web publishing technologies and deliberately confining the projects scope to purely Surface Web [1] sites within the Sub Saharan geographic region.

Sub Saharan Africa represents a unique opportunity for terrorist informatics researchers as the Continent is in a unique position of experiencing recent full connection (2012) to the fibre optic backbone of the Internet, with the contiguous perceived rise of terrorism on the Continent (Perry, 2011, Morocco on the Move, 2013, Sapa-AFP, 2012, Lyman in Harbeson et al. 2013, Pan, 2003). The combination of both these factors presents an opportunity to study the relationship between terrorism and the Internet free from the overwhelming volumes of data associated with Western countries.

Literature

The base line concepts surrounding the use of the Internet by terrorists, is a relationship that has been well explored within the context of previous research. Early works such as Weimann (2006) and a United Nations 2012 study, clearly illustrating the appeal of the Internet to terrorist groups. Additionally the enthusiastic adoption of Web technology by prominent individuals within Al Qaeda such as the late Anwar al-Awlaki, and the role that cyber facilitated networking and indoctrination has played within terrorist plots such as the cases of the Toronto 18 (Wilner, 2010) and Roshonara Choudhry (Carter, 2013), has kept terrorist use of the Internet high on the counter terrorist agendas of many Western countries for the past decade.

Possibly one of the most beneficial features of the research carried out on terrorist use of the Internet thus far, is the firm distinction between terrorists using the Internet in a non-technical manner to spread publicity, as opposed to the primarily theoretical idea of true cyber terrorists using the Internet to perpetrate physical acts of death and destruction (Conway, 2003 and Rid, 2013).

Despite the often-banal content of many terrorist websites (Holbrook *et al*., 2013) the very presence of a terrorist group on the Surface Web has consistently provoked strong reactions from the public (Sheobat, 2013) and policy makers. With the assumed radicalization and recruitment power of terrorist web sites (Lappin, 2010, Awan, 2007 and Weiner quoted in FoxNews, 2010) many politicians have been critical of Internet service providers lethargy in response to terrorist use of social media [2] platforms (Kendzior, 2013). Following in the wake of cases such as Anders Behring Breivik (Wroe, 2011), negative perception surrounding terrorist use of the Internet has grown to such an extent that the issue is starting to shape the very form that web technology takes, with services such as YouTube offering functionality that allows users to explicit label content as inappropriate due to the materials promotion of terrorism (Kanalley, 2010).

Although, to date, there have been no specific studies investigating Sub Sahara African terrorist groups use of the Internet, Somalia's' Al Shabaabs' use of the social media platform Twitter, has drawn large amounts of analysis from both media and policy circle (Pearlman, 2012). Academic studies such as (Kahn et al., 2004) have shown how common and easily accessible terrorist web content such as the Al Shabaab site has become, and just as the Internet tangentially touches many people's lives so, increasingly; many studies of terrorist issues tangentially touch on terrorist use of the Internet. For example, *Stroud's* (2013) study of Anders Breivik's relation to music, references Breivik's use of Massive Multi Player Online Role Playing Games (Deep Web [3] Internet technology) and the role these technologies played as a self gifted 'reward' to Breivik before he committed the attacks he has since become famous for.

There is also a growing body of work that examines terrorist, dissident and criminal use of the Internet as the core focus of the work. Studies such as Cheong *et al.* (2011) examined how the micro blogging site Twitter could be used by security services in the event of a terrorist attack and a growing number of works address social media's role in civil unrest (Khondker, 2011 & Ghonim, 2012). Within the field of criminology a number of significant studies have explicitly segregated malicious activities within the Dark Web [4] (Christin, 2012) from Surface Web [5] activity (Décary-Hétu *et al.*, 2011) however, to date, the majority of research that has examined cyber terrorism has exclusively examined Dark Web terrorist activity (The

University of Arizona Dark Web Portal being the most prominent). What currently lacks in the literature is a more granular examination of both how various web technology platforms are being used by terrorists and how terrorist web content published to the Surface Web, deep and Dark Webs are connected from the perspective of the user experience.

Currently types of web technology vary vastly, from the ever-evolving catalogue of social media technology that has increasingly come to dominate the web publishing market since 2000, to the more static Hyper Text Mark-up Based (HTML [6]) sites that has been used since the inception of the Internet. Terrorist groups use both HTML sites as well as the full range of social media platforms. However, there have been few studies that have explored how the same group may use different technologies for different purposes.

The importance of making this distinction between technologies is highlighted by both Sagemans' (quoted in Weiman 2006, 118) conclusion that over 60% of terrorists are recruited via network of friends and family and the observation that once a terrorist group has become established the robustness and flexibility of a network form of organization often becomes pivotal in the groups success or failure (Arquilla *et al.*, 2001 & Ronfeldt *et al.*, 1991). Given that social networking technology is similar to the flexibility, redundancy and ease of use of the network form of organization that is so integral to the majority of terrorist groups, it is surprising that more academic work has not explicitly sought to disambiguate terrorist use of social networking technology from more static forms of Internet technology within the scope of the research.

Method

Geographic Scope

The scope of the research was decided by data held within the Global Terrorism Database (GTD) (START, 2012) on terrorist groups active within Sub Saharan African. The decision was made to use the GTD in this way, as this data source provided an authoritative list of the most active and visible terrorist groups in Sub Saharan African and also provided a widely accepted definition of what was considered a terrorist act and by implication a terrorist group (for more background on the GTD consult Bowie *et al* in Schmid, 2013, pp. 295-298).

Currently in regard to the Sub Saharan African region the GTD contains 6401 terrorist events that occurred between 1970 and 2010 that have been attributed to 349 separate terrorist groups spread across 45 of the 47 of the countries in the Sub Saharan region. Of the original 349 terrorist groups listed in the GTD 104 had to be discounted, leaving 245 whose web presence the research team went forward to investigate. Terrorist groups were removed from the original 349 GTD list due to one of two reasons. Firstly, some group descriptions were too generic to yield meaningful results i.e. *"Anti Government Rebels," "Islamist Extremist," "Tribal group," "Coup Plotters Against the Government"* etc. and secondly, there were a number of examples of former terrorist groups becoming legitimate political parties within a country i.e. the African National Congress (the authors are not contesting that groups that fit into this category did not and do not continue to perpetrate terrorist activities merely, that due to their legitimised status and typically sizable web presence, any results drawn from these groups within the context of this study would be meaningless). While groups that had fully transitioned to political parties were removed, groups that were still engaged in political violence with only a marginal mainstream political presence were left in the study group.

Internet Scope

This initial list of countries and terrorist groups provided the foundation for the research team to begin conducting searches with a specific country's Top Level Domains (TLD [7]). Of the 45 Sub Saharan African countries included in the research after the GTD had been mined, 26 of these countries had a Google search engine specifically optimized for that TLD e.g. Mali's specific Google search engine is http://www.google.ci/. If the country did not have a Google specific TLD then Google.com was used as the default search engine. As search engine results can be highly specific according to TLD, the reasoning behind the studies search strategy was that by using regional search engine results in conjunction with the larger Google.com search engine the chances of finding a web site specific to a terrorist search was increased.

The Internet Scope of the research was not only defined by TLD selection but by the strata of cyber space that the research team searched for terrorist web content within i.e. Surface, Deep or Dark Web. The study confined itself to examining Surface and Deep Web sites that were listed on Google with the investigative team never entering the Dark Web. The decision was made not to examine the Dark Web within this study due to the difficulties in searching the Dark Web space in the systematic way used for the Surface and Deep Web searching and the challenges of linking Dark Web sites to specific geographic domains [8].

The date range for the studies data collection phase ran from June 1 2013 to July 30 2013. The research team acknowledges that due to the distribution of the collection of web sites meta data across a date range, there was some inherent disparity between the user generated features of the collected sites, that could have generated errors within later interpretation of the data set e.g. Facebook Site X would have 300 *likes* on June 1, while Facebook Site Y would have 301 *likes* on July 30. In this case Y would appear to be the more liked site however, in the intervening period between X and Y's data collection, X could have gained more likes and hence be more popular than Y. The research team acknowledges this as a shortcoming in the date collection method and as an area for improvement in future studies.

During the search phase of the research, only web sites that could be directly attributed to the terrorist group were included with the collected data set, as such news websites and social media websites merely commentating on a groups activities were not counted within the study. Direct affiliation of a website to a group was based on the qualitative judgement of the research team and features such as declared overt support of a terrorist group, explicit use of a terrorist groups iconography in banner and headlines and tangible evidence of terrorist activities such as images and videos showing terrorist actions. One aspect of the data set that may lead to confusion for those seeking to replicate the results of this study is the exclusion of a large number Facebook sites that are apparently the home pages of terrorist groups. Pages such as https://www.facebook.com/pages/Janjaweed/114753351875498 are examples of pages automatically generated by Facebook to attract new users, as opposed to original user generated content; as such they have been discarded from the data set.

As an exhaustive search of the Internet for every web site linked to the terrorist groups examined within this study was not possible, the research team made the decision to only view the first page of Google results returned. Search Engine Optimization research shows that over 90% of Internet users do not go beyond the first page of Google results (Toddjensen, 2011), as such the research team reasoned that by only examining the first page of Google results they were accurately modelling the behaviour of the average Internet user looking for information on terrorist groups in Sub Saharan Africa. Efforts were made to adapt Internet searching to the main languages spoken with the country being examined however, due to the large number of spoken languages in the Sub Saharan Africa region and the limitations the research team, searches within each country were only uniformly carried out in English, French and Arabic where applicable.

The specific mechanics of the Google search employed the use of speech marks to enclose terrorist group names [9] with the addition of the terms *Facebook* and *Twitter*. Typically the combination of these searching strategies returned any terrorist themed website that had been published to the Internet within that region. As with the teams focus only on the first page of Google results the team felt that the limited use of search syntax accurately represented the skills of the average Internet user. The variance of these three-search terms consistently yielded different results within which terrorist web content would typically be listed if it existed. The research team acknowledge that although this method was not completely rigorous, it was a consistent and impartial method of conducting Internet searching.

Coding of collected websites

Once a website linked to terrorist group was identified a number of features were recorded and some simple coding added. Features that were recorded about each websites included number of *likes [10]* (for Facebook pages), number of followers and following [11] (for Twitter pages), number of views (Youtube) and WhoIs [12] data for standard HTML pages. Additionally the date of creation was recorded for all websites.

The most important methodological distinction that the study sought to make was to separate social media based websites from more static web platforms (coded as HTML within the data set).

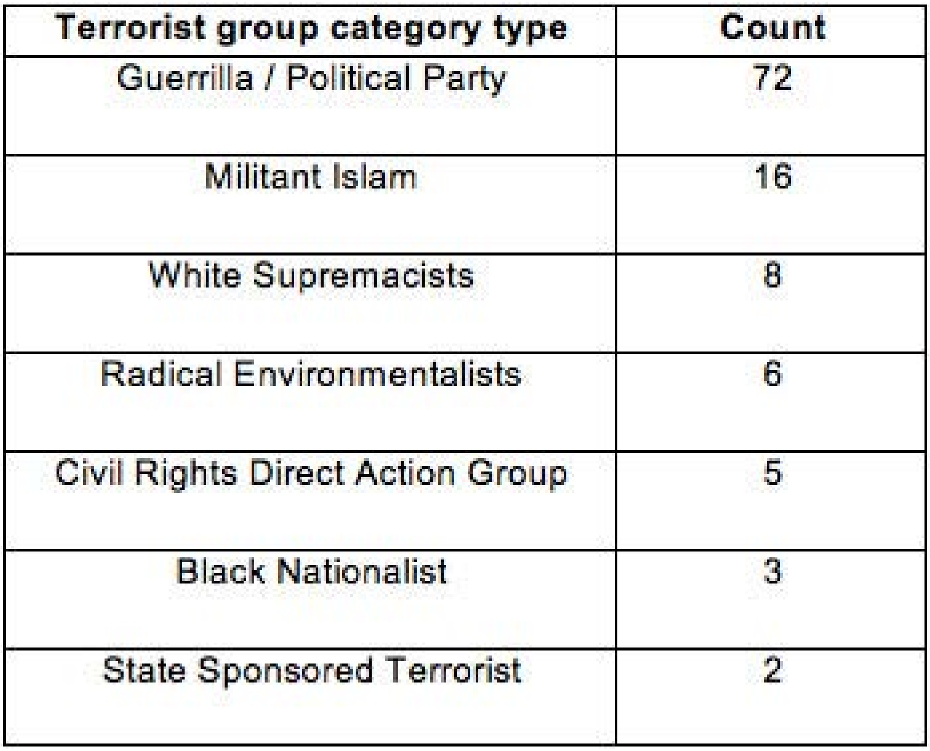
To conclude the methodology section of this paper, this study should be viewed a primarily qualitative study [13], using standard social science coding methodologies. The software used as part of the study included The Onion Router (TOR) anonymised web browser, Microsoft Excel, Batchgeo for mapping and Google Refine that was used for data cleaning and basic text mining purposes.

Although the technological approach of the study was simple, the study did attempt to adopt a more sophisticated approach to the subject matter by translating a cultural interpretive approach (Geertz in Martin *et al.*, 1994) into a cyber-medium. Pervading the methodology of the study is the researchers attempt to accurately adopt the behaviour of an average Internet user in one of the countries of Sub Saharan Africa. As with the majority of world Internet users it is assumed that most Africans favour Google over other search engines (Sterling, 2013), do not use advanced search syntax (Bray, 2003), do not stray beyond the first page of search results (iProspect, 2006) and are not aware of (or have little interest in) accessing the Dark Web (based on the inverse of Tor Metrics Portal: Users, 2013).

Results – base line stats

Once the survey phase had finished, key features of the researches data set included

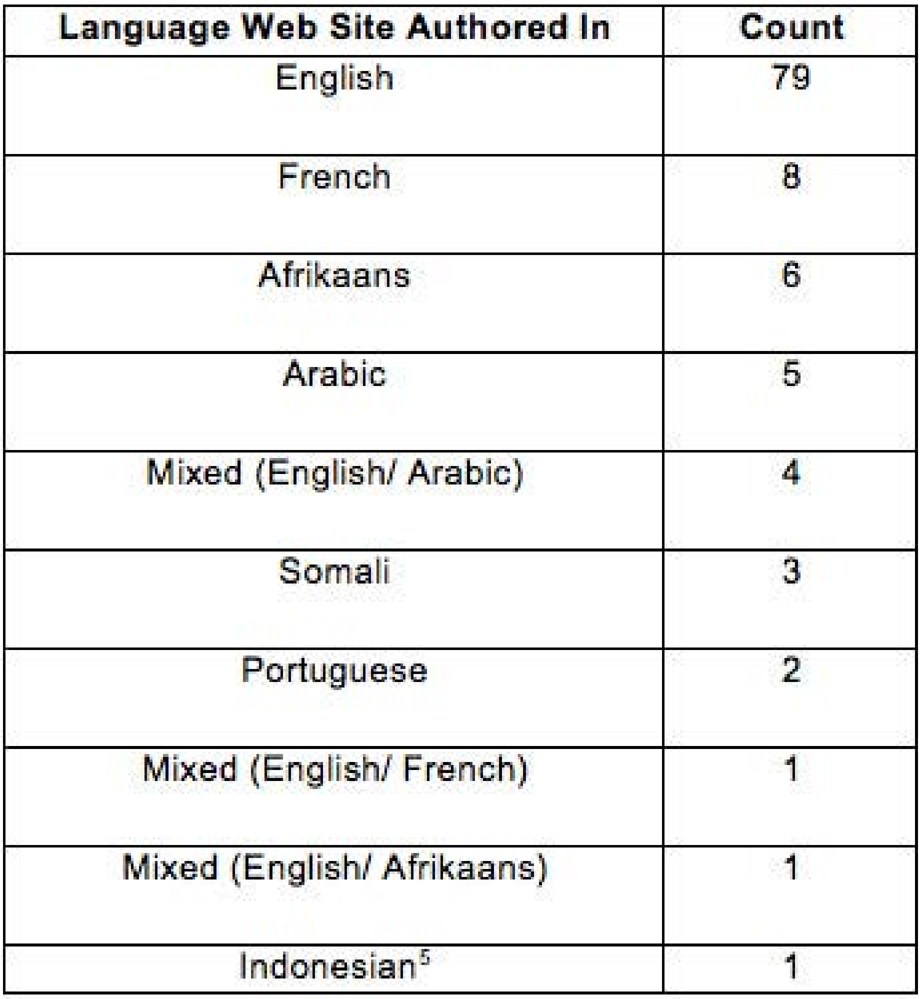
- The research team found 112 websites that were linked to Sub Saharan African terrorist groups.
- Of the 45 Sub Saharan African countries surveyed 18 had evidence of terrorist web sites accessible from their TLD.
- Of the 245 terrorist groups surveyed, 57 had a web presence of some kind
- Of the 57 terrorist groups with a web presence the Ogaden National Liberation Front [14] active in Somalia and Ethiopia, had the greatest number of attributable web sites with 10 distinct sites in total.
- Breaking the 112 discovered websites down by the terrorist group category type showed the following (Figure 1).



Terrorist group category type	Count
Guerrilla / Political Party	72
Militant Islam	16
White Supremacists	8
Radical Environmentalists	6
Civil Rights Direct Action Group	5
Black Nationalist	3
State Sponsored Terrorist	2

Figure 1: Terrorist category group type mapped to website count

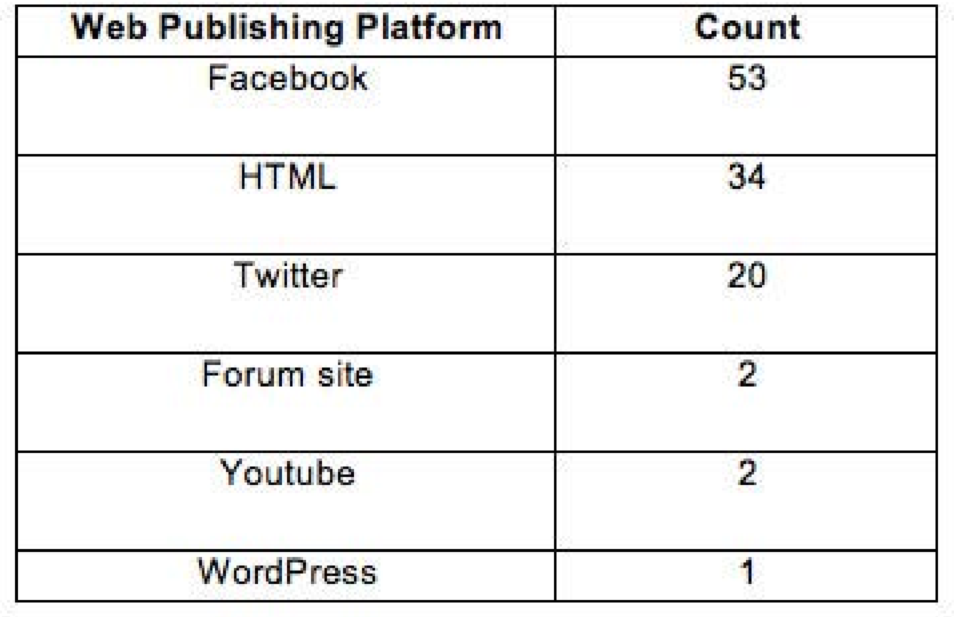
- The earliest active social media site was the Ogaden National Liberation Front Youtube site (https://www.youtube.com/watch?v=nPJLy7EGuQk), which was created in 2008.
- The earliest active HTML site was the National Union for the Total Independence of Angola (http://www.unitaangola.com/PT/PrincipNouvP0.awp), which was created in 1995.
- Linguistic division of the web content was as follows.



Language Web Site Authored In	Count
English	79
French	8
Afrikaans	6
Arabic	5
Mixed (English/ Arabic)	4
Somali	3
Portuguese	2
Mixed (English/ French)	1
Mixed (English/ Afrikaans)	1
Indonesian[5]	1

Figure 2: Count of web site publishing language

- Six different types of web publishing technology were seen within the data set, with a full brake down as follows



Web Publishing Platform	Count
Facebook	53
HTML	34
Twitter	20
Forum site	2
Youtube	2
WordPress	1

Figure 3: Count of web publishing platforms

- The Facebook page with the most *likes* was Boko Harams' site (https://www.facebook.com/NigerianTerrorismNewsArena) with 6817 likes (as at 5 August 2013)
- The most active twitter feed was the Mujahideen Youth Movement (https://twitter.com/AMEF3) with 5056 Tweets (as at 5 August 2013)
- The Twitter account with the most followers was the Al-Qa`ida in the Lands of the Islamic Maghreb (AQLIM) site (https://twitter.com/Andalus_Media) with 9929 followers (as at 5 August 2013)
- The Twitter account following the most other Twitter accounts was the Oromo Liberation Front site (https://twitter.com/marsaabo) which followed 284 other Twitter accounts (as at 5 August 2013)
- South Africa and Nigeria were the Sub Saharan African countries with the highest number of terrorist web sites associated with them, with 19 individual sites attributable to each. Somalia closely followed in second place with 18 web sites associated with it.
- No data was available for the user traffic that any of the 112 sites received due to the fact that this data is either proprietary or simple unavailable

Results - qualitative analysis of the data set

One significant initial observation was that in almost all cases, where a search on a terrorist group returned a web site linked to terrorism, within the first page of Google results, and invariable higher on the page than the terrorist website, were pages from Wikipedia, GTD and the wider Start website [15] explicitly describing the group as a terrorist organization. While this result is predictable given that the original list of terrorist groups used in the study was sourced from the GTD, the observation does highlight the fact that it is unlikely that a user could stumble into a terrorist website without being aware of the groups' status as a prescribed organization.

Examining the data in more detail revealed a clear trend in the geographic distribution of terrorist web sites across the Sub Saharan African region. Shown below in figure 4, is a visualization of the distribution of terrorist website in the region (distribution in this case is not based on the location of the server hosting the site but on the physical location of the terrorist group related to the web site)

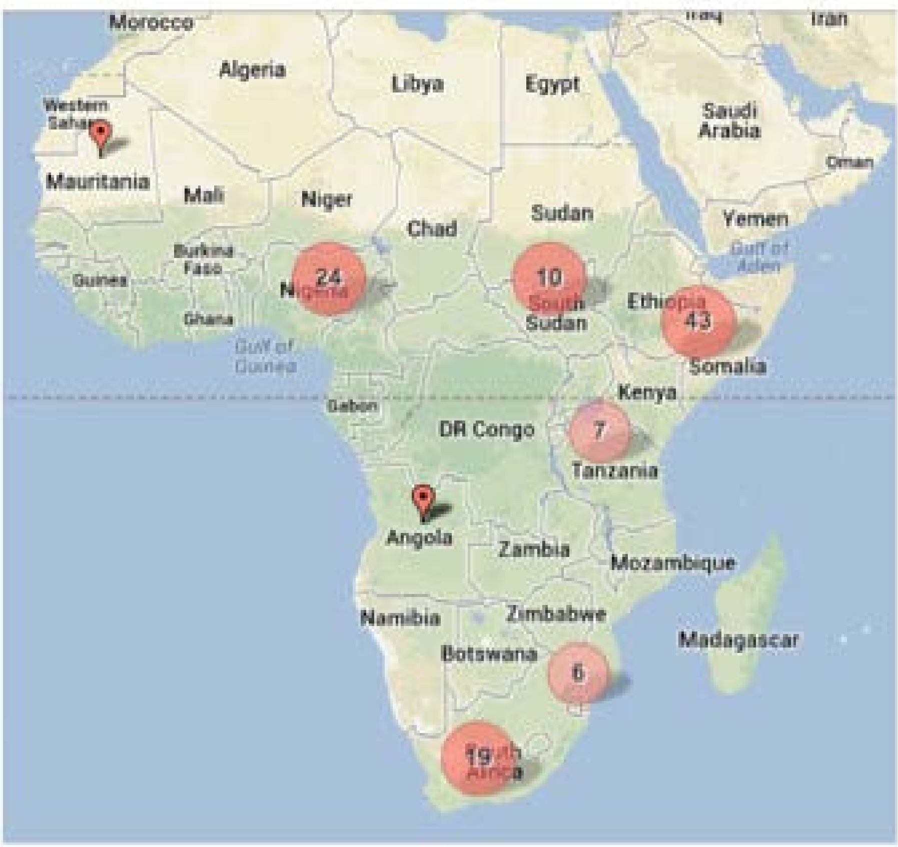


Figure 4: Regional geographic clustering of terrorist groups with an identified web presence

The obvious trend shown by Figure 4 is that there are clear concentrations of terrorist web publishing activity in the Eastern, Western and Southern regions of the African continent. The nexus of activity in South Africa is possibly to be expected, due to the long established Internet connectivity and high IT literacy rates in the country, however, the clustering of activity in Eastern Africa is more intriguing. The 43 sites that are spread over Ethiopia, Eritrea, Sudan and Somalia is an unexpectedly high figure given the very low Internet penetration rate within East Africa (Sudan has the highest with 19% Internet penetration of the population in 2012 (Internet World Stats) and the fact the East Africa was the last part of Africa to be connected to the Internet. Examining the linguistic break down of the 43 web sites associated with East Africa, this shows that 33 are written exclusively in English with 5 others written partly in English with the reminder written in either Arabic (2) or Somali (3). The favouring of English over the indigenous languages of the region is unusual, as although English is widely spoken in Sudan and Eritrea; other languages such as Arabic and Somali have a far higher population base within this region, therefore one would have assumed the terrorist groups would seek to publish in the first language of their host countries if their intention was to focus on indigenous population as their target audience.

Combining the linguistic analysis of the East African cluster of terrorist websites with the additional observation of the dominance of the English language within the wider data set (70 of 112 web sites were published in English), the obvious question arises concerning who the intended target audience is of the websites collected within the study? As the majority of terrorist groups within the survey are publishing in English (with the notable exception of Far Right groups active in South Africa, who would appear to exclusively publish in Afrikaans) it is a tentative conclusion of this study that the target audience for the majority of terrorist groups of Africa is predominantly Western Anglophones as opposed to groups indigenous to Africa. This conclusion is supported by the findings of other studies that have observed groups such as Al Shabaab using the Internet in its attempts to actively attract Western recruits to African based conflicts (Jihadist Forum Monitor, 2010)

Notable in their divergence from the African norm regarding the intended target audience, are the web sites associated with terrorists published in South Africa. The sites of both South African Right-wing White and radical Black African groups would appear to be addressing their own regionally based constituency rather than seeking to engage the English-speaking West. It would appear that in contrast to other Sub Saharan African sites, whose objective would seem to be to attract support from the West to African causes, the intention of South African group's use of the Internet is to increase social cohesion within the group. The authors of Radical Black African sites such as *The Inkatha Freedom Party* and *AZAP[16]*, have created a number of open and closed sub groups for supporters to network in what would appear to be an attempt to promote greater inter-party unity.

In contrast to the assessed 'outward from African' facing nature of the majority of terrorist websites examined within this survey, the collection phase of the research discovered a number of websites that opposed terrorism who appeared to focus on African nationals as the target audience. Sites such as *One-million-somalis-against-Al-Shabaab* (https://www.facebook.com/pages/One-million-somalis-against-Al-Shabaab/109814322403744) and *If You hate Al Shabaab Join Us* (https://www.facebook.com/5Somaliwayn), communicate a powerful message of opposition to the ideals of terrorist groups, due to the social proof of the tangibility nature of those posting vehement messages of opposition. In all cases these 'counter-terror' websites had received vastly more *likes* than their pro terrorist counterparts. This use of social media by the same diaspora, to both promote and denounce terrorism mirrors Mogadans (2005) staircase of terrorist engagement, within which although many thousands of people may feel a common grievance, those that turn to violent terrorism as a solution make up only a tiny minority of a wider population.

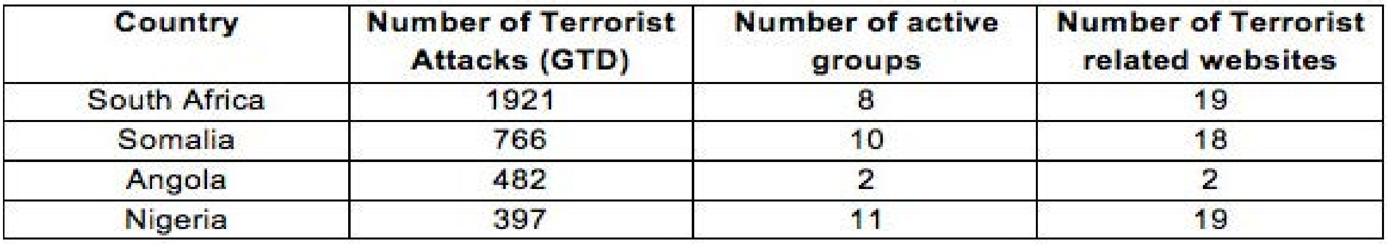
The example of the tangible power of a counter terrorist narrative coming from African nationals, highlight the influence that authentic author attribution can have for either a pro or counter terrorist message. One of the main challenges of the research was dividing web sites that were authored by individuals closely associated with terrorist groups and those authored by publishers who were merely commentating in a supportive manner about terrorist activity, with few tangible relations to the terrorist group. The research team assumed that the former category was more important within the wider context of terrorist use of social media than the latter however, research quickly showed that this division would appear to be arbitrary to many consumers of terrorist social media.

One of the most active generic social media platforms in Nigeria is the forum site *nairaland.com* and it was within this web site that researchers found a discussion on Boko Harams' use of Facebook (http://www.nairaland.com/1297912/boko-haram-leader-shekau-opens-facebook). The Facebook site being discussed on *nairaland.com* is purported to be the work of Abubakar Ibn Muhammad Shekau the current leader of Boko Haram.

Despite the fact that a number of postings on the Shekau Facebook page had been made from the Northern Nigerian town of Maiduguri, the current geographic center of gravity for Boko Haram, the research team assessed that the page was not the work of the real Shekau, due to the banality of the postings and the excessive use of stock photography of Shekau. The mostly negative discussion on *nairaland* about the Shekau Facebook site (which as of the date of this paper has filled five pages) clearly shows that a terrorist web site need not be authentic to be provocative. The Shekau Facebook example highlights the growing importance of social media within Nigerian life and the potential influence that social media driven web content can have on a target audience.

One trend that was not present in the data set was any evidence of terrorist groups making any attempts to transition from the passive use of the Internet to the more destructive use of cyber space outlined by Conway (2005). Indeed of the 112 websites examined in the study only one website (http://anonymousnigeria.blogspot.ca/2012/01/peoples-liberation-front-press-release.html) showed an overlap between a conventional terrorist group and computer hacker collective, in this case the People's Liberation Front of Niger and a Nigerian offshoot of the Anonymous collective, a group only tangentially linked to true cyber terrorism under the most broad of definitions. While there were three examples within the data set of terrorist web sites distributing malware, it is incorrect to assume that the author of the malware was the same as the designer of the web site. Most commonly this type of malware is develop by a third party and embedded on a target website due to the websites lax security, rather than any link with the ideology of the web site. As such, based upon the data collected and examined within the study, the research team concluded that there was no firm evidence of a shift towards true cyber terrorism from any of the groups examined within this study in the Sub Saharan African region. Instead it would appear that the objective behind the creation of the web sites examined within this study was to spread the ideology and goals of the specific terrorist group to a wider audience.

Results – quantitative analysis of the data set



Country	Number of Terrorist Attacks (GTD)	Number of active groups	Number of Terrorist related websites
South Africa	1921	8	19
Somalia	766	10	18
Angola	482	2	2
Nigeria	397	11	19

Figure 5: Country, mapped to number of terrorist attacks, groups and websites

The above table shows that while there is no relation between number of active groups and number of terrorist attacks or associated websites, there is a suggestion of a relationship between the number of terrorist attacks within a country and the number of terrorist related websites within that territory. Although there is only enough data to suggest a trend, the data does imply the presence in Sub Saharan African of the symbiotic links between terrorism and media production that has been previously observed in other parts of the world (Biernatzki, 2002).

Examining the data a step further it was obvious from the base line statistics that the overwhelming majority of the studies web sites (72 of 112), were linked to quasi legitimate guerrilla groups engaged in nationalist / separatist causes. These groups were relatively evenly geographically distributed across Sub Saharan Africa. In contrast, the Militant Islamic groups with a web presence (16 of 112) were concentrated into East Africa

(Ethiopia, Somalia and Kenya) and West Africa (Nigeria and Niger).

Examining in more detail, some of the data points specific to Islamic Extremist web sites reveals more insight into this subgroup of and the unique way they are using the Internet. Shown below in Figure 6, is a scatter plot showing the number of webs sites created each year, but with the web sites for Islamic extremist groups broken out and represented separately.

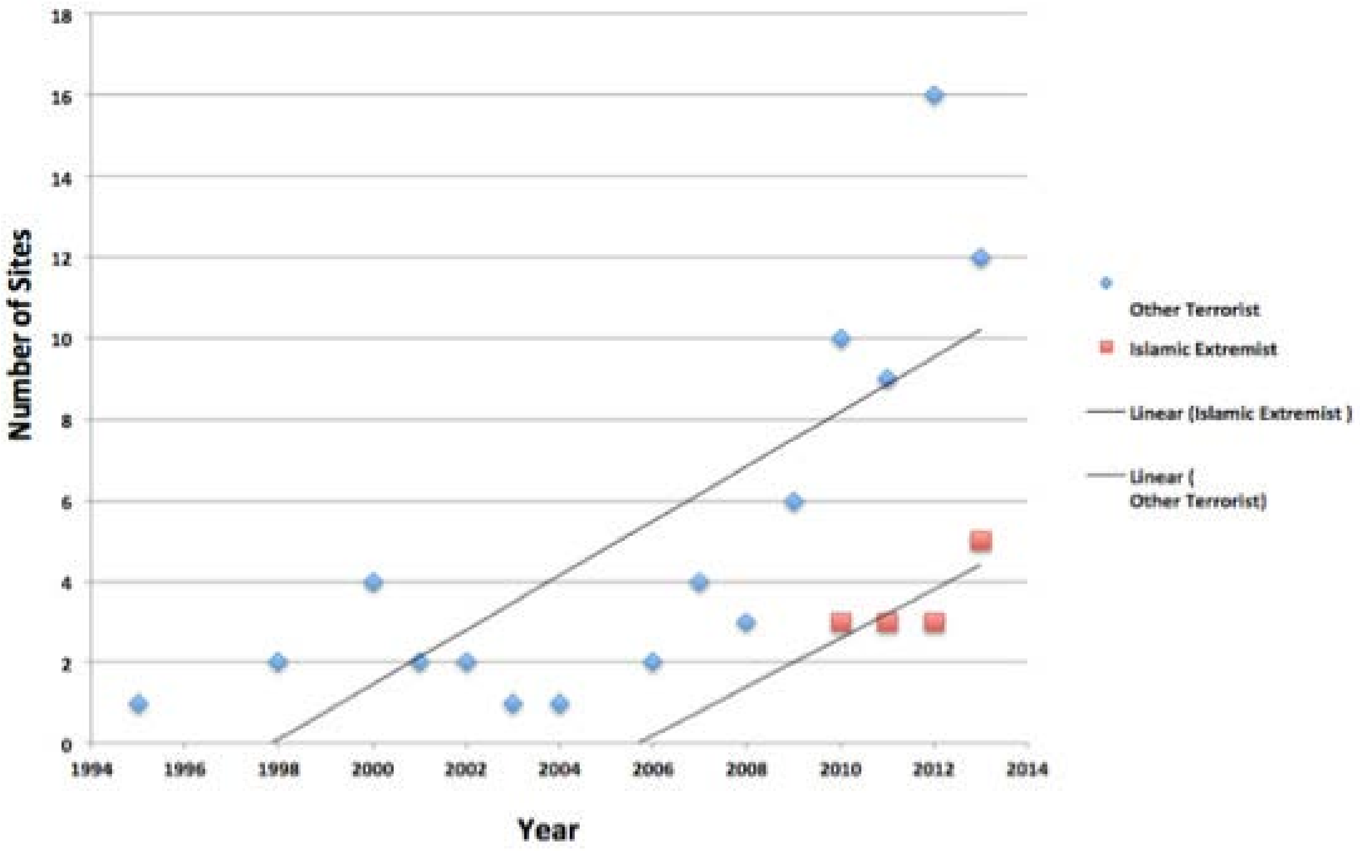


Figure 6: Count of terrorist web site mapped against creation date (red squares represent Islamic Extremist sites; blue diamond's represent all other terrorist category types)

Figure 6 shows that web sites associated with Militant Islamic groups a relatively recent (2009) addition to the collection of Sub Saharan Africa's terrorist web sites. Additionally Figure 6 also shows the start of a trend in the increase in the number of web sites associated with Islamic extremist groups, a trend that is following almost exactly the rising trend in terrorist web site publishing in the Sub Saharan African region.

Another unique point concerning Militant Islamic websites that is not represented in Figure 6, is that all the web sites associated with Militant Islamic groups were published exclusively via social media technology, with no examples of an Islamic Extremists website published in HTML (of all the terrorist actor categories within this study, Islamic extremists are the only group exclusively publishing to the Internet using social media).

Looking at social media adoption across all Sub Saharan African terrorist groups, revealed a strong trend within the data of the rapid adoption levels that social networking technology has enjoyed within the terrorist user group of this region. Shown below in Figure 7 is a graph showing the creation date for both HTML and social media sites mapped against year and number of sites created.

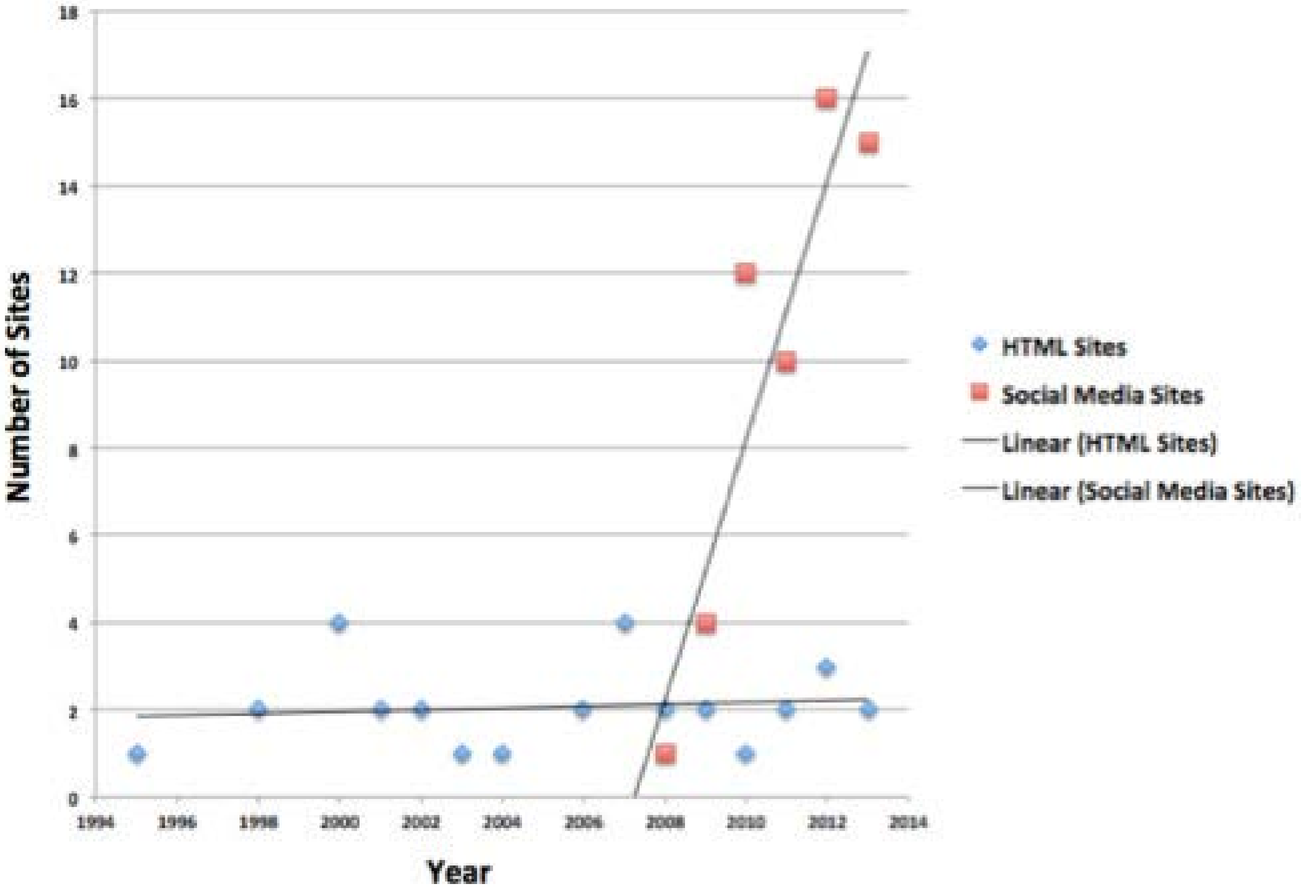


Figure 7: Number of HTML and Social Media sites created from 1994 to 2013

Within Figure 7 the trend lines are almost superfluous, with the creation rate for HTML sites only rising slightly since 1994, but the creation rate for social media sites rapidly rising in 2008. With such a strong trend in relation to social media adoption evident within the data, it is apparent that the overall rise in terrorist web site publication that started in 2007 (shown earlier in Figure 6) was facilitated largely by the arrival of social media technology.

While the authors of this paper are in no way insinuating that social media creates terrorism, the data quantitatively demonstrates what many have suspected for some time: that social media technology is playing a major role in facilitating the spread of terrorist messaging onto the Internet.

Accounting for the appeal of social media platforms to terrorists, are the technological properties inherent to platforms such as Facebook and Twitter. Social media requires no programming skills to publish rich multimedia content, reaches a global audience separated from the vagaries of Search Engine Optimisation and completely free to the user. Additionally the inbuilt security settings of social media fulfil the unique user requirements of terrorist groups in that, social media platforms are resistant to Denial of Services attacks due to their highly robust technical infrastructure. In effect when any terrorist uses social media they sit behind a digital battlement that protects their sites from hacking attacks that regularly knock HTML websites offline. Additionally the defences of social media technology are not only technical, but legal also. With groups such as Al Qaeda finding their HTML sites increasingly being taken offline (Awan *et al.*, 2009), the legal protection that is afforded a group by default when they use a service from a social media giant like Twitter is considerable. The example of Anwar al-Awlakis' YouTube videos, highlights the legal umbrella that social media membership affords, with the body of al-Awlakis' videos only being taken down after a direct request to YouTube from US Congress (The Guardian, 2010).

Based on the data represented in Figure 7 it is a fair assessment to make that social media will continue to be the dominant web publishing technology for terrorist publishers in Sub Saharan African for the foreseeable future.

In 2013 Facebook users reached over 1 billion users globally and while terrorist groups may have been caught in the huge tide of social media adoption, analysis of the studies data set shows that the way terrorist use social media could be markedly different from the average user. Aside from the content of the posts, one difference from an average user, inherent to almost all the terrorist Twitter feeds examined within the study was the ratio of Following to Followers. Quantitative studies by social media statisticians (Boris, 2010) shows that the average ratio between Following to Followers is approximately a one-to-one ratio however, of the 20 Twitter sites found in the study only 6 site came close to the standard one-to-one ration with a further 6 sites having no followers at all with the remaining sites showing very low Following to Followers ratios.

The Movement for the Emancipation of the Niger Delta (MEND) (https://twitter.com/mendnigerdelta) and the Al-Shabaab (https://twitter.com/HSMPRESS1) Twitter feeds typify the use of the social media platform by the terrorists within this study; following few or no other account and very few or no re-Tweets of others messages or hash tags. In the Twitter sphere, were success of an account is typically based on levels of engagement, the use of the service in this way is unusual and turns the platform from a tool for discourse and debate into merely a platform for broadcast. With one of the core concepts of Twitter being that new traffic is attracted to an account by the levels of engagement of that account, it is obvious that low engagement terrorist social media sites such as the MEND feed, rely on other mechanism such as traditional media to attract new traffic to their feed.

When the likes and follower counts of the studies 73 Facebook and Twitter accounts are added together a combined figure of 88623 is derived. Given that within both Facebook and Titter's functionality an account can only like or follow another account once, the figure of 88623 is an reasonable accurate representation [17] of the number of individual who have engaged with one of the terrorist accounts. This figure is in itself a surprising indicator of how widely social media technology allows terrorists to distribute their message, free from the constraint of having to attract the attention of the mainstream media. Given the fact that large scale use of Facebook and Twitter are relatively recent additions to the terrorists array of web publishing mediums (figure 7) and the fact that of the remaining 47 sites (user numbers unavailable) have been online since at least 1995 it is possible that the 112 sites examined within this study have reached an audience of hundreds of thousands.

One theory that is consistently prevalent within media and policy thinking in regard to terrorist use of the Internet, is that Surface Web sites such as the ones being examined by this study act as a gateway into more extreme Internet forums within the Deep and the Dark Web (Noveau, 2010, Lappin, 2010). With this theory in mind the research team examined the content of a number of the most active and extreme web sites, in and effort to find any links onto yet more extreme material on other Internet platforms or within deeper layers of the web.

Downloading all Tweets from the two main Al Shabaab Twitter Feeds (https://twitter.com/hsmpress123, https://twitter.com/HSMPRESS1) on the 1 August 2013 collectively yielded 506 separate Tweets. When the text was searched for links to other websites 6 links to .info websites were fond, 1 to a .net site, 65 to various .com sites and 173 links to other Twitter feeds (using the hash tag (#) internal URL posting method used in

Twitter). Significantly, there was no link to Al Shabaabs far more radical forum *alqimmah.info [18]* within any of the 506 tweets and the websites and Twitter accounts that the Al Shabaab Twitter sites did point to were predominantly open source news agencies and far less radical in content than the seed Al Shabaab Twitter feed.

Based on these observations it becomes difficult to see how a would be terrorist convert would move from terrorist Surface Web sites, to more extreme Deep and Dark Web material. Possible accounting for this lack of explicit links to extremist media is the notion that the introduction to more extreme web sites such as *alqimmah.info* is done within private messaging, making the transit mechanism from Surface Web to Deep Web less visible.

The final quantitative point that the can be drawn from the data set is the registered location (WhoIs) data of the HTML websites (social media sites do not have WhoIs records). Of the 34 HTML sites only 12 were deliberately using registration obfuscation services were no registration details could be seen. Of the remaining web sites 11 were hosted in the USA, 4 in Great Britain and South Africa (respectively) and 1 in Australia and Switzerland (respectively). Aside from South African Far Right groups, it would appear that terrorist web site publishers in Sub Saharan Africa prefer to host their sites outside of the African continent. Given that reliable Web Hosting [19] services have been available out of South Africa since at least the late 1990s, the registration of terrorist HTML sites outside of Africa suggests that the authors of the sites are not resident in Africa [20] and highlights the international nature of the African terrorism.

One of the main unanswered questions left open by this study is how tangibly linked the authors of the studies' web sites are to the terrorist groups core operatives conducting the 'bomb and bullet' (Hoffman, 1998) activities of the groups. Based on this studies data alone it is almost impossible to discern this relationship with any degree of certainty. It would appear that all the content of the 112 web sites examined within the study could have been collected from the open source media and re-published by enthusiastic supports with little or no connection to the terrorist organization other than an ideological alignment. There was one notable exception to this trend and that was the Twitter account of Boko Haram (https://twitter.com/BOKOHARAM2012).

Although purely anecdotal it would appear that the Boko Haram Twitter account had a far closer connection to core terrorist operatives than any of the other sites examined within this study. A particularly compelling aspect of the Boko Haram site that would support this assertion was the photographs that were posted to the account. While there were a number of graphic images of conflict and death the vast majority of images posted to the account showed Boko Haram members engaging in community work such as aid distribution and community conflict resolution. The content of the Boko Haram site reflected a sophisticated understating of classic insurgency techniques such as an attempt to supplant the traditional rule of government and social work that would curry favour for Boko Haram within the target population (it is notable that the Boko Haram site examined by this study is in fact the third iteration of the site after Twitter suspended the first two accounts (Guardian, 2013)). Although the second iteration of the Boko Haram Twitter account fell outside of the collection date range of this study, the account is particularly significant in that it was suspended when is displayed graphic images of a dead French Special Forces solider (Gordts, 2013). This incident supported that theory that the account's author had an intimate connection to Boko Haram operatives due to the fact that the multiple images displayed on the account were obviously from a primary source [21] and predated open source news reporting by at least 12 hours.

Conclusion

The most significant conclusion of this study is the observation of the strong adoption trend by terrorist web publishers of social media technologies such as Facebook and Twitter. The trend was so strong that the study concludes that this adoption of social media technology (within the terrorist web publishing diaspora) has been the main factor in facilitating the overall rise of the terrorist web presence in Sub Saharan Africa.

While social media undoubtedly gives a voice to terrorists, this study has shown that the technology also gives voice to the 'every man' citizen that would oppose the use of violence to achieve political objectives. The examples of emotive, first person narratives with high *like* counts that the studies researchers observed, manifestly demonstrates that terrorist often do not represent the views of the wider countries population. With an almost consensus perception within academic and professional circles that terrorist use of the Internet is uniformly a negative phenomenon, this study challenges this perception and raises the possibility that discourse facilitated via social media has the potential to counter terrorism more effectively than more conventional forms of counter terrorist messaging.

The results of the WhoIs record searches and the fact that that the majority of the Sub Saharan African terrorist web sites are hosted outside of Africa, combined with the heavy Anglophone trend of the websites content, highlight the increasingly international nature of terrorism in Africa (Shinn, 2010).

Terrorist web site publishing in the study region consistently bucked the local Internet usage trends, both in terms of choice of language the sites was published in typically English (79 of the 112) and the greater than expected density of publishing activity for a minority interest group within a developing Internet region. Both of these factors are clear indicators that the use of the Internet is becoming an integral and most likely pre planned, part of many Sub Saharan African terrorist groups media engagement strategy. The issue of how successful terrorist web sites are at achieving an organization's objectives remains a matter of debate (Jenkins, 2011). This study found no evidence of a direct link between a terrorist's web presence and any tangible material benefits that groups may derive from Internet publicity [22].

In regard to the methodological goals of the study the research team concluded that the study highlighted the need to develop frameworks to compare the Meta data associated with different social media technology platforms. As one example of the issues that a lack of a unified framework creates, Facebook has the ability to *like* a page were as Twitter does not, conversely Twitter accounts have a follower and following count, a function that Facebook lacks. Using this example, is a Facebook like the same as a reciprocated following relationship in Twitter? Different social media platforms have different types of functionality, that dually create different data points, without a robust framework a meaningful comparison of the increasingly technologically mixed medium that terrorist web content inhabits will become a challenge.

The importance of this area of terrorist study has become particularly germane in light of the recent attack by al-Shabaab on the Westgate shopping centre in Nairobi, during which terrorist used social media during the attack to give updates of their actions to the public as they carried out their actions. While social media has been seen to be used to support terrorist operation in real time in the past (the Mumbai attacks by Lashkar-e-Taiba in 2008 (Kilcullen, 2013) the al-Shabaab Westgate incident is an example of the real time, direct to target audience propaganda that social media facilitates. Cast within this light the question of how closely a terrorist web site publisher is connected to a groups core operational personnel becomes particularly relevant as this knowledge could be used in the future to preeminent incident such as the Westgate attack.

Clearly automation software if configured correctly, would facilitate a full enumeration of Sub Saharan African terrorist groups presence on the Internet. One particularly intriguing possibility is that the trend regarding the adoption of social media technology by Islamic Extremist groups may be continued on a global scale. Illustrating this theory is the observation that the Afghanistan based Taliban's Twitter feed (https://twitter.com/alemarahweb) was created in 2011, around the same time that the Boko Haram and Al Shabbab Twitter sites were created. Whether the author of the Taliban's Tweeter feed drew inspiration from the media exposure of the al-Shabab Twitter feed, or if two separate authors merely arrived at the same conclusion at the same time remains opaque. This and other many other fundamental questions remain about terrorist's relationship to the Internet and only further research will examine theories such as these to the depth that they require.

About the authors

The authors wish to thank James Ball for his assistance with content analysis

Stewart K. Bertram *holds an MSc in Computing and an MLitt in Terrorism Studies from the University of St. Andrews. His research interests include the development of frameworks for applying open source intelligence to national security issues, use of the Internet by terrorist and other malicious actors and how networks of power and control are manifested within highly technologically enabled groups. Professionally, Stewart currently works as a freelance Intelligence and Cyber Security consultant working with a number of small and medium sized business on various issues. Previous to his current role, Stewart managed an Intelligence team looking at issues associated with the cyber black market and before this Stewart served five years in British Military Intelligence. Contact: berts231@hotmail.co.uk*

Keith Ellison *was born in1953 in Liverpool, England and served in The British Army Intelligence Corps as a Senior Non Commissioned Officer, "Operator, Intelligence and Security" for over 12 years, stationed in the UK, Northern Island, Hong Kong and Germany. During this period Keith worked on Counter Terrorism issues in Northern Ireland; served as military liaison with Special Branch; ran a combat intelligence section in West Germany, and a Security Intelligence Section in West Berlin. After leaving the Army, Keith worked as an Executive Officer/computer programmer for the Ministry Of Defence before joining the Foreign Commonwealth Office, working there for 17 years in several different areas affecting British Government foreign policy. Educationally Keith obtained a German Civil Service Interpretership while with the Army and a NEBSS Diploma in Supervisory Management and Certificate in Security Management. Additionally Keith holds a Certificate for Management of Industrial Security accredited by the Institute of Industrial Manager's. Contact: keithellison@hotmail.com*

Notes

[1] Surface Web – defined as a layer of the Internet that is easily accessible via mainstream search engines such as Google. Sites on the Surface Web can be either HTML or social media based however, all have the common feature that they have been designed so that they can be easily found by an Internet user with basic skill levels

[2] Social Media – characterized by highly malleable, user created content. Web services such as Twitter, Facebook and Youtube are all examples of social media web sites.

[3] Deep Web – defined as a layer of the Internet that is not listed (indexed) within a Google search due to

technological incompatibility. Deep Web sites are not deliberately hidden by the creators rather their inner content is opaque to most main stream search engines i.e. a Google search for "Barack Obama Twitter," will return a link to Obamas' Twitter account (Surface Web), but will not list the content of any of the posting (Deep Web) within the account in the search results.

[4] Dark Web – a layer of the Internet that is deliberately hidden and is not accessible by any search engine. Accessing a Dark Web site requires specific technology and explicit knowledge regarding the location of the site the user wishes to visit. Dark Web content is typically illegal in nature.

[5] Surface Web – defined as a layer of the Internet that is easily accessible via mainstream search engines such as Google. Sites on the Surface Web can be either HTML or social media based however, all have the common feature that they have been designed so that they can be easily found by an Internet user with basic skill levels.

[6] Hypertext Mark-up Language (HTML) – a basic programming language used to code a web page. The term is used within the scope of this study to describe a web site that has no functionally to allow users to interact or otherwise edit the content.

[7] Top Level Domain (TLD) – shown as the suffix after a web address i.e. www.XYZ*.co.uk*, TLDs provide regional and thematic specific division of the Internet. TLDs are not necessarily hosted in their target geography they merely suggested a thematic relation to a geographic region.

[8] The Dark Web does not use an indexing system in the same way that the Surface Web does, with the affect that the space cannot be searched in the same way as the Surface Web. Within the Dark Web a user has to know the exact address of the web site they wish to visit, thus making the search method used within this study ineffective within this space.

[9] Encapsulating text within speech marks signals to the Google search engine that the search term is a phrase and typically returns a more accurate result than a search that does not use speech marks

[10] A like is a function of Facebook and other social media platforms that gives users the option to demonstrate a favorable opinion towards another user. One Facebook user can like either a posting or whole profile of another user. Likes are displayed as a number (how many people have liked page or resource) next to a 'thumbs up' sign on the user profile page.

[11] A following relationship on the Twitter social media platform is created when one account holder (A) decides to actively follow (button click action) another (B) and hence A joins B's 'follower list' and B is displayed on A's 'following list.' Following is different from a like on Facebook as a follower does not by default support the view of the account that is being followed for example, the official CIA Twitter account could be observed following the Boko Haram Twitter site before the later was taken offline. Although a reciprocated following / follower relationship is considered a sign of mutual admiration, within the context if this study the follower count is considered a rough metric of how widely observed the Twitter profile is within the wider Twitter user community.

[12] WhoIs data is derived from the registration details that are provide when an individual registers a website with a domain registrar. This data can be recovered by a specialist web search termed a WhoIs search. There is little data validity checking on the part of the most domain providers. Social media platforms such as Twitter and Facebook do not have WhoIs data it is only more static HTML websites that have WhoIs records

[13] Although quantitative methods are used on the studies data set the research team felt that due to the

subjective nature of the data collection phase, overall, that study should be considered qualitative in nature

[14] The Ogaden National Liberation Front (ONLF) is a rebel group founded in 1984, fighting to make the Ogaden region (approximately 400 000 kilometers) of Ethiopia an independent state.

[15] http://www.start.umd.edu/

[16] Both the Inkatha Freedom Party and AZAPO are legitimate prolitical parties in South African however, the sites collected within this study were seen to be the work of the most extreme elements of these groups

[17] It is possible to fake like and follower counts by a single user creating numerous accounts and then liking or following the target account. This practice is common within marketing campaigns hence the caveat placed around the figure of 88623 individual users within the context of this study

[18] Active 3 August 2013

[19] Web Hosting – once any web site is created it must be placed on a web server connected to the Internet backbone, from were Internet users can access it. Site hosting can be in one physical location or hosted across multiple distributed locations (so called Cloud hosting)

[20] WhoIs searches on the HTML web sites revealed the identities of a number of individuals based outside of Africa, investigation into these individual revealed no obvious links to terrorist groupings

[21] The posing of the body and equipment, combined with the multiple photographic angles was almost forensically detailed in nature

[22] To be explicit this study is not challenging the idea that there may be a link between factors such as terrorist web presence and recruitment, merely that there was no indication of these factors within the studies data.

References

Arquilla, J. Ronfeldt, D. (2001). *Networks and Netwars*

Awan, A. Al-Lami, M. (2009). AL-QA'IDA'S VIRTUAL CRISIS. *Royal United Service Institute Journal* FEBRUARY 2009 VOL. 154 NO. 1 pp. 56–64

Awan, A. (2007). Virtual Jihadist media. Fuction, legitimacy and radicalizing efficiency. *European Journal of Cultural Studies*. Vol 10(3) 391-410

Bowie, G. Neil and Schmid, P. Alexander. (2013).The Routledge Handbook of Terrorism Research. London: Routledge

pp. 295-298

Bray, T. (2003). On Search: The Users. Retrieved 7, December 2013 from http://www.tbray.org/ongoing/When/200x/2003/06/17/SearchUsers

Biernatzki, W. (2002). Terrorism and Mass Media. *Communication Research Trends*. Volume 21 (2002) No. 1

Boris. (2010). Twitter Statistics:82% of Twitter users have less than 350 followers. *TNW The Next Web*. Retrieved 27, August 2013, from http://thenextweb.com/socialmedia/2010/09/30/twitter-statistics-82-of-twitter-users-have-less-than-350-followers/

Carter, J. (2013). Case Study: Roshonara Choudhry, The Radicalization Process of Roshonara Choudhry. *The Risky Shift.com* Retrieved 27, August 2013, from http://theriskyshift.com/2013/01/case-study-roshonara-choudhry/

Conway, Maura (2003) Hackers as terrorists? Why it doesn't compute. *Computer Fraud and Security*. pp. 10-13. ISSN 1361-3723

Cheong, M. Lee, V. C. (2011)**.** A microblogging-based approach to terrorism informatics: Exploration and chronicling civilian sentiment and response to terrorism events via Twitter. *Journal of Information Systems Frontiers*. Volume 13 Issue 1, March 2011 Pages 45-5**9**

Christin, N. (2012). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. Carnegie Mellon INI/CyLab. Retrieved 27, August 2013, from http://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab- 12-018.pdf

Conway, M. (2005). Terrorist Web Sites: Their Contents, Functioning, and Effectiveness. *Terrorism and the Media*. New York: Palgrave

Décary-Hétu, D., Morselli, C. (2011). Gang Presence in Social Network Sites. *International Journal of Cyber Criminology* 5(1)

Fox News. (2010). *Al-Awlaki's YouTube Videos Targeted by Rep. Weiner*. Retrieved 27, August 2013, from http://www.foxnews.com/politics/2010/10/25/rep-weiner-calls-youtube-al-awlakis-videos/

Gordts, E. (2013). Dead French Soldier Photo: Tweet By Al Shabaab Allegedly Shows Troop Killed In Somalia. *Huffington Post*. Retrieved 27, August 2013, from http://www.huffingtonpost.com/2013/01/14/dead-french-soldier-photo-tweet-al-shabaab_n_2474141.html#slide=1984930

Guardian. (2013). *Al-Shabaab Twitter account shut down for second time*. Retrieved 27, August 2013, from http://www.theguardian.com/world/2013/sep/06/al-shabaab-twitter-shut-down

Graham, M. (2010). Development and Broadband Internet Access in East Africa. *Oxford Internet Institute*. Retrieved 27, August 2013, http://www.oii.ox.ac.uk/research/projects/?id=59

Ghonim, W. (2012). *Revolution 2.0*. London: Fourth Estate

Geertz, C. (1994). Thick Description: Towards an Interpretive Theory of Culture. In Martin, M. McIntyre, L. *Readings in the Philosophy of Social Science*. London: A Bradford Book

Jenkins, B, M. (2013). Is Al Qaeda's Internet Strategy Working? RAND. Before the Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence United States House of Representatives

Pan, E. (2003). AFRICA: Terror Havens.Council on Foreign Relations. Retrieved 27, August 2013,from http://www.cfr.org/world/africa-terror-havens/p7716

Hoffman, B. (1998). *Inside Terrorism*. Columbia University Press

Holbrook, D., Ramsay, G., Taylor. (2013). "Terroristic Content": Towards a Grading Scale. *Terrorism and Political Violence Volume 25, Issue 2*

Internet World Stats. Retrieved 27, August 2013, http://www.internetworldstats.com/stats1.htm

iProspect. (2006). Search Engine User Behaviour Study. Retrieved 7, December 2013, from http://district4.extension.ifas.ufl.edu/Tech/TechPubs/WhitePaper_2006_SearchEngineUserBehavior.pdf

Jihadist Forum Monitor. (2010). *Al-Shabab (Mym) in Somalia Video Urges Muslims From Around The World to Travel to Somalia For Jihad - Calls on Muslims in Sweden to Kill Lars Viks*. Retrieved 27, August 2013, from

http://www.bukisa.com/articles/402298_al-shabab-mym-in-somalia-video-urges-muslims-from-around-the-world-to-travel-to-somalia-for-jihad-calls-on-muslims-in-sweden-to-kill-lars-viks

Kendzior, S. (2013). Twitter's dangerous lack of transparency on terrorism. *Aljazeera Online* Retrieved 27, August 2013, from http://www.aljazeera.com/indepth/opinion/2013/02/201321015712442895.html

Kanalley, C. (2010). YouTube Gives Users Ability To Flag Content That Promotes Terrorism. *Huffington post* Retrieved 27, August 2013, from http://www.huffingtonpost.com/2010/12/13/youtube-terrorism-flag_n_796128.html

Khan, R. Kellner, D. (2004). New media and internet activism: from the 'Battle of Seattle' to blogging. *New Media & Society Vol6(1):87–95 DOI: 10.1177/1461444804039908*

Khondker, H. H. (2011). Role of the New Media in the Arab Spring. *Globalizations* Volume 8, Issue 5

Kozinets, R. V. (2009). Netnography: Doing Ethnographic Research Online. 2009. London: SAGE Publications Ltd.

Kilcullen, D. (2013). Our of the Mountains, the coming age of the urban Guerrilla. C. London: Hurst & Co. (Publishers) Ltd.

Lyman, P.N. (2013). The War on Terrorism in Africa. In Harbeson, J., Rothchild, D. *Africa in World Politics: Engaging A Changing Global Order.* London: Westview Press

Lappin, Y. (2010). *Virtual Caliphate: Exposing the Islamist State on the Internet*. Washington DC: Potomac Books Inc

Moghaddam, F. M. (2005). The Staircase to Terrorism A Psychological Exploration. *American Psychologist* Vol. 60, No. 2, 161–169

Morocco on the Move. (2013). IS TERRORISM ON THE RISE IN MIDEAST, NORTH AFRICA? – ARAB SPRING NOW. RETRIEVED 27, AUGUST 2013, FROM HTTP://MOROCCOONTHEMOVE.WORDPRESS.COM/2013/06/02/IS-TERRORISM-ON-THE-RISE-IN-MIDEAST-NORTH-AFRICA-ARAB-SPRING-NOW/

Mben, P.H., Puh, J. (2013). 'Gates of Hell': Mali Conflict Opens New Front in War on Terror. *Spiegel Online* Retrieved 27, August 2013, from http://www.spiegel.de/international/world/mali-offensive-opens-new-front-in-the-fight-against-terror-a-878750.html

National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2012). Global Terrorism Database [Data file]. Retrieved 27, August 2013, from http://www.start.umd.edu/gtd

Nouveau, T. (2010). Al Qaeda recruits terrorists on Facebook. *TGD*. Retrieved 27, August 2013, from http://www.tgdaily.com/security-features/52990-al-qaeda-recruits-terrorists-on-facebook

Pearlman, L. (2012). Tweeting to Win: Al-Shabaab's Strategic Use of Microblogging. *The Yale Review of International Studies*. Retrieved 27, August 2013, from http://yris.yira.org/essays/837

Perry, A. (2011). Threat Level Rising: How African Terrorist Groups Inspired by al-Qaeda Are Gaining Strength. *Time Magazine* Retrieved 27, August 2013, from http://www.time.com/time/magazine/article/0,9171,2101780,00.html

Rid, T. (2013). *Cyber War Will Not Take Place*. London: Hurst

Ronfeldt, D. Arquilla, J. Fuller, G. Fuller, M. (1999). *The Zapatista "Social Netwar" in Mexico*. New York: RAND Corporation *The Future of Terror, Crime, and Militancy*. New York: RAND Corporation

Shinn, D. (2010). AL-SHABAAB TRIES TO TAKE CONTROL IN SOMALIA. Foreign Police Institute. Retrieved 7, December 2013 from http://www.fpri.org/enotes/201011.shinn.somalia.html#note10

Sterling, G (2013). October Search Market Share: Bing Continues To Grow At Yahoo's Expense. Retrieved 7, December 2013 from http://searchengineland.com/search-market-share-bing-continues-to-grow-at-yahoos-expense-176896

Sapa-AFP. (2013). Islamic terrorism on the rise in Africa. *Times Live* Retrieved 27, August 2013, from http://www.timeslive.co.za/africa/2012/07/06/islamic-terrorism-on-the-rise-in-africa

Sheobat, W. (2013). *The Boston Bombings: Inside the Shocking Web of Terror Training*. Retrieved 20, September 2013, from http://shoebat.com/2013/05/02/the-boston-bombings-inside-the-shocking-web-of-terror-training/

Stroud, J. (2013). The Importance of Music to Anders Behring Breivik. *Journal of Terrorism Research*, Volume 4, Issue 1 (2013)

Tor Metrics Portal: Users. Retrieved 7, December 2013, from https://metrics.torproject.org/users.html

The University of Arizona Dark Web Portal. Retrieved 27, August 2013, from http://ai.arizona.edu/research/terror/

toddjensen. (2011). 2ND Page Ranking: Youre the #1 Loser. *Gravitate Online*. Retrieved 27, August 2013, from http://www.gravitateonline.com/google-search/2nd-place-1st-place-loser-seriously

The Guardian. (2010). *YouTube removes Awlaki hate videos*. Retrieved 27, August 2013, from

http://www.theguardian.com/technology/2010/nov/03/youtube-removes-awlaki-videos

United Nations. (2012). *The use of the Internet for terrorist purposes*. Retrieved 27, August 2013, from http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

Wilner, A. (2010). From Rehabilitation to Recruitment: Canadian Prison Radicalization and Islamist Terrorism. Presented to the Canadian Political Science Association annual conference; Concordia University (Montreal, Canada), June 1-4, 2010

Wroe, D. (2013). Anders Behring Breivik's scary internet world. *Global Post* Retrieved 27, August 2013, from

http://www.globalpost.com/dispatch/news/regions/europe/110727/anders-behring-breivik-anti-islam-blogosphere

Weimann, G. (2004). www.terror.net : How Modern Terrorism Uses the Internet. *United States Institute of Peace*. Retrieved 27, August 2013, from http://www.usip.org/publications/wwwterrornet-how-modern-terrorism-uses-the-internet

Weimann, G. (2006). *Terror on the Internet: The New Arena, The New Challenges*. Washington DC: United States Institute of Peace Press