

AL SHABAAB ON TWITTER, THE USE OF INTERNET BY JIHADIST ORGANIZATIONS

By Michele AVINO¹

Introduction

At the beginning of February Somalia's Al-Qaeda linked Al-Shabaab insurgents have returned to Twitter with a new account, after they were suspended because using twitter to post a photographs of a French they had killed.

"For what it's worth, shooting the messenger and suppressing the truth by silencing your opponents isn't quite the way to win the war of ideas," this is what we have read on the new account re-open on the 3rd of February. The new account @HSMPRESS1 has attracted over 1000 followers in two days.

The previous account was suspended on 24th of January (an extremely active account), after posting photographs of a French soldier, and after threatening to execute Kenyan hostages. Twitter didn't comment on the account deletion, but social-media experts reasoned that Al-Shabaab had violated Twitter's terms of service, which prohibit direct threats of violence. As a general background Al-Shabaab came to prominence in 2005, when the Islamic Courts Union (ICU) took over southern Somalia. At that time a young group broke away from the "Islamic Union" and established a new organization, which they named "Al-Shabaab Al-Mujahideen". On September 2008, the leaders of Al-Shabaab declared the establishment of the "Islamic Emirate of Somalia" in the south of the country. On January 2010, Al-Shabaab expressed its support for "Al-Qaeda in the Arabian Peninsula".

In April 2010, the Jihadist propaganda center "Da'awat Al-Haqq Lil-Dirasat Wal- Buhuth", which is under the auspices of Al-Shabaab, published a booklet titled "A Real, Living Model of the State Envisioned by Al-Qaeda" on various Web forums.

Al-Shabaab pursue its media strategy with strong presence on twitter given that like other Al Qaeda affiliates group it has recognised the importance to provide timely and continuous narrative to their followers.

¹ Michele AVINO is Islamic affairs analyst and is a specialist on issues relating to the fundamentalism, radicalisation and related terrorism. He is expert analyst on radicalization process leading to the homegrown terrorism and counter terrorism strategy. In his analysis he explore the beliefs, narratives and ideologies that lead to violent radicalism underpinned by an abusive interpretation of Islam, with a view to understanding of the causes and remedies for violent radicalization. He follows methods, such as internet, through which Islamist militants in Europe mobilise their supporters and find new recruits. He is expert analyst on the radicalization in prisons as well as prevention and response strategy.

They currently use internet to justify their actions, to provide update on the group's progress and to distribute material dedicated for western muslim followers. In this particular case the engagement of Al-Shabaab with western muslims occurs with the production of English language material.

The English output of Al-Shabaab on twitter has multiple aims such as to convey ideology to potential western recruits and to provide the followers with a trusted alternative media source.

It is worth to note that Al Shabaab start to tweet on 7th of December 2011 entirely in Arabic language, the account has the title of HSM Press Office and has some 20000 followers.

It has to be noted that when Twitter suspended the Al Shabaab account, many jihadi groups created new accounts on Twitter and Facebook pages.

Problem Analysis

These recent events have demonstrate the ability of jiahdists to continually mature their methods while attempting to demonstrate that their appeal is worldwide. Online Jihadism has to be considered a crucial, binding and organising factor in a substantial part of attack plots against the West and Western citizens remaining an important factor in national and international threat assessments.

These data provide evidence that jihadists are systematically moving from conventional web forums to Twitter.

Terrorists group are increasingly using internet as an instrument for propaganda, radicalisation and recruitment.

Why now Twitter? It offers a real time communication tool which allow to spread information on event recently occurred. This platform allow followers to be part of the jihad in real time creating some sort of excitement to the members of the Somali diaspora and English speaking Muslims.

Twitter provides a more public platform than a password-protected forum, but one critical utility of forums for jihadist is the ability to have relatively private conversations.

Twitter does, however, provide a means for jihadist organizations and individuals to provide information when breaking news occurs. Jihadist are likely to turn to Twitter for rapid response and to live-tweet extended violent events.

By its nature internet confirmed to be the ideal place for activity by terrorist organizations, it offers advantages as easy access, anonymity, huge audience, fast information sharing, lack regulation of control.

The Internet also allows terrorists to convey their messages to international and distant audiences with whom it would otherwise be difficult to communicate. The Internet provides a means for terrorist groups to feed the mass media with information and videos that explain their mission and vision. Thereby, the group's message can reach a greater audience and more easily influence the public agenda.

The Internet allows jihadist people to get in touch with like-minded people faster, to exchange ideological ideas more swiftly and to validate their own ideology.

The terrorists organizations are able to be active on the network without geographical limitations.

In addition to launching their own websites, terrorists can harness the interactive capabilities of chatrooms, instant messenger, blogs, video sharing websites, and self-determined online communities and social networks.

So far, all active terrorist groups have established at least one form of presence on the Internet and most of them are using all formats of up-to-date online platforms like e-mail, chatrooms, e-groups, forums, and resources like You-Tube, Facebook, Twitter, and Google Earth.

It not surprising anymore that Jihadist message boards and chatrooms have been known to have "experts" directly answer questions about how to mix poisons for chemical attacks, how

to ambush soldiers, how to carry out suicide attacks and how to cyber attack computer systems.

In 2012 the General Intelligence and Security Service (AIVD) of The Netherlands (AIVD) estimates that approximately 25,000 jihadists originating from over 100 countries belong to this jihadist group of core Internet forums. Most of them operate on the so-called invisible Web, a part of the World Wide Web that has not (yet) been indexed and cannot be found by readily accessible search engines. The core forums hidden inside this invisible Web are constructed and maintained by fanatical jihadists.

It is important to become better informed on the use of internet by terrorists and monitor their activities. In this view we have to consider that in a recent years the security expert have focused mainly on the threat of cyberterrorism paying less attention to the more routine use of internet by terrorist organizations.

There is a consolidated situation where a social network account (Twitter or Facebook) affiliated or run by a terrorist organization go offline for a while and then later a new account emerges like a cat and mouse game.

Twitter is widely considered a leader among social networks in its commitment to free speech, but there is a perception that the platform lack of clear policies when it comes to dealing with extremist or terrorist organizations.

The interactive possibilities characterises jihadi cyberspace and allow jihadists worldwide to find each other quickly, to meet in 'public' virtual places, like on social media, on Internet forums and in chat rooms.

One of the most attracting aspect of the forums is that all members can take part in group discussions addressing a wide variety of themes. These interactive group discussions lay the foundation for the radical discourse that paves the way for legitimised violence against the enemies of 'true' Islam.

These Internet forums offer in particular for Western jihadists a unique possibility to get in touch with likeminded individuals in jihadist conflict zones, such as Afghanistan and Yemen. They may be inspired by such contacts and supported in their efforts to participate in Jihad, or they may be deployed to carry out attacks in the West countries.

The Western jihadists participating in these forum play also an important role in the redistribution of jihadist propaganda to the visible surface Web such as Facebook and YouTube filling the gap between core forums and the surface Web.

This ideology basically contends that Islam must be protected against actors who are considered a threat to Islam, including the West.

Online Jihadism is characterised by a number of processes: the process of radicalisation and Jihadisation and the network formation.

Radicalisation is mainly a group process that can take place partly or, in some cases, entirely online. The process of jihadisation takes place at the extreme end of the radicalisation spectrum, i.e. radicalised individuals who are ultimately prepared to engage in violent Jihad, both verbally and physically.

Individuals who have radicalised on Internet and who play an active role in jihadist cyberspace usually form networks. Such networks mostly develop online and can represent a serious threat. These virtual jihadist networks are often more internationally oriented and much larger than physical jihadist networks.

Jihadist social network and web forum also act as a virtual marketplace where jihadist supply and demand meet and which focuses on violent Jihad. This is where experienced jihadists and respected ideologists get in touch with young enthusiastic providing them with reply to their personal comments. Their background and the fact that the Internet does not stop at national borders generate an international threat.

Another consideration to be made is the fact that the worldwide growth of the number of Internet users has led to a globalisation of virtual Jihad. This is also causing a growing

number of people from a different geographic countries to be touched and inspired by jihadist ideas.

In this view Jihadist organisations such as Al-Qaeda merely play an inspiring role and a central guiding role in this development.

Secondly, the social network and web forum usage is growing fastest in jihadist hotspots, such as Afghanistan, Pakistan, Somalia and Yemen. It has been noted that a growing number of experienced jihadists from these countries are coming online, driving and enriching the dynamics of online Jihadism.

The professionalisation of virtual Jihad is allowing a growing number of jihadist actor groups to mask their identity, their location and the content of their communications. It also generates an abundance of high-quality jihadist propaganda that is increasingly capable of radicalising individuals around the globe.

Western jihadist and new group of jihadist consumers from Islamic countries increasingly make direct contact with these experienced jihadists. As a result, more and more of these new recruited people are enabled to travel to said hotspots in order to take part in jihadist activities. They can pose a threat to Western interests in the region or to the West itself if they return.

Under sociological point of view we can observe that rapidly rising Internet usage, high levels of youth unemployment, and the continuing lack of real political change and sufficient peaceable outlets for legitimate political dissent are factors that together create a situation in which Jihadist websites which offer radical, utopian solutions to complex socio-economic and political challenges.

Recent years have witnessed a corresponding “re- Islamization” (return to the fold) of diasporic Muslim youth in particular. Many young Muslims seem to be searching for “a more authentic form of Islam” than the one their parents practice.

For many young devout Muslims living in the West, the preferred course of action is to become involved in non violent campaigns designed to combat Islamophobia and American intervention in Iraq. However, other young Muslims are apparently receptive to many of the extreme ideas and tactics popularized by the Jihadist movement on line.

In recent years, and due to a growing awareness in the West of the importance and popularity of jihadist Web forums, attempts to close them down have become increasingly prevalent.

How dealing effectively with the threat

Which types of measures governments and intelligence service agencies can adopt to counter terrorists’ use of the Internet? Removing content from the web taking down of websites; filtering – restricting users’ access and controlling the exchange of information; and hiding – manipulating search by manipulating search results or deleting recommended links or suggestions for websites and videos that are known to promote terrorism or hate speech. – on line censorship.

Even though it may be possible to remove, filter or hide content that is available from relatively static Web sites, such efforts will be largely ineffective when it comes to chat rooms, instant messaging, virtual worlds and networking sites.

Between late March and early April 2012, most of the major jihadi forums were shut down for a period ranging from three to 16 days. It is not clear why the forums went dark in such a coordinated manner, but the outage provided an opportunity to assess how jihadi forum use evolves when specific forums are no longer available.

When more prominent jihadi forums go down, activity increases on smaller forums, which suggests that the overall jihadi communications enterprise is durable in the long term.

The most immediate way to confront violent extremist online propaganda is to go to the virtual places where extremist messages are being purveyed and engage actual and potential violent extremists in dialogue and discussion.

Rather than removing violent extremist content or trying to undercut the demand for it, the aim is to take full advantage of violent extremists' and terrorists' presences in cyberspace and make maximum use of the information they are sharing with others.

In particular, exploiting these social network and web forum to gather intelligence and/or evidence can be the most effective way of dealing with online radicalization.

Government should pursue this approach more systematically and should consequently increase the training offered to members of intelligence agencies so they can be conscious of the increasingly virtual nature of the threat and can use online resources to gather information about radicalization process. Trying to understand the conversations that happen online and who is involved may be just as important as more complex human intelligence activity aimed to spying on a terrorist group's leadership or interpreting their official announcements and statements.

Technological innovations saw internet penetration increase from 16 million to 2.2 billion from 1995–2011, bringing about huge advancements in speed and accessibility, as well as the systems and virtual architecture that construct and sustain cyberspace. Internet penetration is not limited to particular demographics or social movements and we should not be surprised, therefore, that terrorist groups, are utilising cyberspace to reach audiences, self publicise, release propaganda, rally support, raise funds, and mobilise activists.

The presence of jihadist organizations on line developed in parallel with the technological developments in web communications, and as a consequence of the global nature of jihadist organizations and their need to reach potential audiences worldwide.

The most recent Web 2.0 innovations and creation of social media platforms (blogging, Facebook, YouTube, and Twitter) have flattened control over the production of online jihadi media.

A wide range of individuals jihadi, organizations, and Web forums have established Twitter feeds to promote their activities. This trend is likely to continue, but Twitter is unlikely to supplant the forum architecture because it cannot replace the sense of authenticity and exclusivity created by the forums.

Jihadist on line resources constitute the backbone of the soldiers of jihad, many of them are experts in ICT and computer programming, have good command of foreign languages, and are familiar with aspects of network security and freely share what they know.

Twitter, Facebook and other jihadist Web forums are essential source to better understand the dynamics of jihadist movements. They represent an authentic and unique source of information to understand the jihadist dialogue, jihadist religious-legal debate, and feelings of participants regarding the progress of Global Jihad.

An increasing number of jihadist producers turn their virtual Jihad dreams into violent action or active participation. More and more jihadist consumers acquire the knowledge, expertise and connections they need to act on their violent intentions after being deeply immersed in jihadist cyberspace.

Jihadist groups are no longer confined to specific regional boundaries. Now jihadist networks can recruit members located in any part of the globe. A person in Europe can literally take a terrorist training course within the privacy of their bedroom.

Modern jihadism can be seen as also increasingly de-territorialised, yet united around common ideologies. As online engagement and interaction has increased, in line with ICT innovations, isolated jihadist are able to congregate, interact, and socialise in cyberspace in ways they are unable to offline.

When considering how to combat Islamist terrorist activities on the Internet, people often think first of legal remedies.

Intelligence and law enforcement authorities are in a difficult position in the fight to contain online radicalisation. There's a lack of uniform legislation across jurisdictions, and limited capacity to cope with the volume of websites disseminating jihadi propaganda. And the internet operates extraterritorially. Its anonymity reduces the ability of law enforcement

authorities to remove undesirable content and to investigate and prosecute those responsible for websites and their contents.

When approaching on line jihadi-threats we have to consider some basic factual finding:

- A jihadist web initiative can be assembled by almost anybody, anywhere.
- The nature of the web-domain permits an extremely rapid diffusion of them.

In other words, the jihadist on line threat it is not confined in space and time and the counter measures are extremely challenging.

As a result of the available network technology and the multitude of Internet-based services, these challenges range from preventing the availability of instructions on how to commit terrorist acts to monitoring the use of encryption technology in terrorist communications.

It is very difficult to close down all the web site and social network that disseminates jihadist material.

The democratic character of the net makes the jihad web based initiatives a potential channel for venting criticism and dissension within the jihadi community.

Therefore, counter measures may require the development of unconventional concepts and taking a different approach compared to traditional counter terrorism doctrines.

The relationship between what an individual jihadist does on a forum and what kind of real terrorist activism they may be involved in is by and large unknown.

Individuals may clearly express their interest in perpetrating an act of terrorism in a public forum discussion, but for many reasons they may not reveal or indicate their intentions, capabilities, associations, and so on.

Because not all jihadist suspects follow a single radicalization roadmap on their way to become terrorist, the intelligence service also faces the task of discerning exactly when radicalized individuals become real threats.

The development and strengthening of affective ties with like-minded individuals may play a prominent role in the formation of terrorist groups.

Counter measures must be proactive in particular, to counter these capabilities in terrorist web presences, it can be suggested to learn more about the psychographic profiles of the targets and the messages that affect them.

Much of what Jihadists do online involves passive observation of discussions, and so many of those discussions involve links directing the observer to other sites or to data in other formats (i.e. files to be downloaded), that any investigation of Jihadist activity online needs to follow the links out of the forums.

A possible action point could be to collect examples of extremist messages on the Internet and identify the strengths and weaknesses of both their content and delivery through analysis and user reactions so as to be able to undermine strengths and exploit weaknesses in constructing and delivering counter-narratives. Analyze themes and discussion threads on extremist websites.

It become also very important identify the types/groups of users who access extremist messages so as to be able to reach them through the same portals with counter-narratives that play to their specific concerns and cultural influences.

External Sites need to be assessed and, where appropriate, monitored and investigated, likewise, files available for download need to be collected and analyzed.

In this view people with analytical, linguistic and technical skills are essential. They will need adequate training and the support of experts.

It is important to draw up a plan that sets out clearly the objectives for countering the operational aspects of terrorists' internet use, as well as countermeasures against online radicalisation.

There is also a need for enhanced cooperation between the public and private sectors; as most of the technical infrastructure upon which jihadist groups are planning, financing and

supporting their activities is owned wholly or in part by private entities, there is a strong need for leveraging existing expertise within the private sector and for increased information-sharing among stakeholders. In this regard we can agree that greater progress could be made against terrorist use of the Internet, and cyber-security issues in general, with closer cooperation between the public and private sectors.

We can certainly expect that online Jihadism will continue to play an important role in national and international assessments in the short and medium term. It is expected that in years to come online Jihadism will be a crucial, binding and organising factor in a substantial part of attack plots against the West and Western citizens and against their interests abroad.

Copyright© ESISC 2013