GSDRC Applied Knowledge Services
Governance · Social Development · Humanitarian · Conflict

www.gsdrc.org
helpdesk@gsdrc.org

Helpdesk Research Report

The role of online/social media in countering violent extremism in East Africa

William Robert Avis

17.06.2016

Question

What is the role for online/social media for countering violent extremism in East Africa?

Contents

1. Overview

Countering violent extremism (CVE) is a broad umbrella phrase that covers a wide array of possible approaches to dealing with radicalisation to extremist violence. There is growing recognition amongst academics and policy makers that de-radicalisation and countering violent extremism programmes can be a more effective way of tackling extremism than purely militaristic approaches.

Given the multiplicity of drivers of radicalisation, the issue of how to counter violent extremism is complex. Online CVE programmes are routinely divided into positive and negative measures. Positive CVE strategies produce counter-content that seeks to challenge extremist narratives and propaganda, while negative CVE strategies are designed to block, filter, take-down or censor extremist content:

- Countering the use of the internet to facilitate terrorist attacks by **remotely altering information** on computer systems **or disrupting the flow of data** between computer systems
- Countering the use of the internet as an **information source for terrorist activities**

- Countering the use of the Internet as a means for **disseminating content** relevant to the advancement of terrorist purposes
- Countering the use of the Internet as a **means for supporting communities and networks** dedicated either to pursuing or supporting acts of terrorism

Online and social media are useful in the dissemination of counter narratives in multiple languages, and to reach a broad, geographically diverse audience. There is a three-pillared strategy for the implementation of online counter-narratives:

- **The message**, which requires the creation of multi-layered and attractive counter-messages to terrorist group ideology that are tailored to individual groups. Linking to existing narratives, appealing to emotional connections and the sensitive use of humour can be successful content ideas.
- **The messengers**, who must appear to have some sort of legitimacy or credibility with the target group. Former radicalised individuals, government leaders, civil society and religious leaders are all appropriate messengers depending on the target audiences.
- **The media**, which requires careful publication and dissemination of the counter-narrative message.

The evidence base for the use of online/social media in countering violent extremism in East Africa is limited with few empirical studies that explore the impact of either online/social media campaigns or counter narratives. Despite this limited evidence base, various organisations are seeking to utilise online/social media to counter violent extremism. Beyond traditional platforms such as radio, these organisations have found that strategies should include using social media and peer-to-peer communication such as WhatsApp where appropriate, particularly when targeting youth vulnerable to radicalisation. This report includes brief regional examples from Uganda and Kenya, and other case studies from CVE initiatives in the UK and elsewhere using online/social media.

2. Countering violent extremism

There is growing recognition amongst academics and policy makers that de-radicalisation and counter-violent extremism programmes can be a more effective way of tackling extremism than purely militaristic approaches (ElSai'd & Harrigan, 2012; IPI, 2010). While de-radicalisation refers to policies and approaches that aim to de-radicalise groups and individuals, with the aim of re-integrating them into society and preventing further violence (El-Sai'd, 2012), counter-radicalisation/extremism is a term used to describe approaches that intend to prevent the emergence or rise of violent radicalisation in society.

There is an expanding body of literature that explores the theory and implementation of strategies to tackle radicalisation and extremism. Much of this tends to focus on de-radicalisation efforts in Europe and America (RAN, 2016; UNODC, 2012); but there is also emerging literature on programmes in Asia and Africa (Feddes & Gallucci, 2015). Most interventions tend to be country-based approaches, driven by national or local government.

According to the Radical Awareness Network (RAN, 2016), the processes of radicalisation leading to violent extremism have evolved. The variety of ideologies that provide inspiration for extremist groups is growing and includes religious-inspired extremism, left wing, anarchist and right wing ideologies as well as nationalist and separatist ideologies. Extremists are no longer acting only as part of organised, hierarchical organisations but also within smaller cells and sometimes as lone wolves (Weimann, 2012). All forms of extremism have become more globalised, exploiting the opportunities of a more interconnected world. Consequently, terrorist or violent extremist actions are harder to detect and predict, making traditional law enforcement techniques alone insufficient to deal with these trends, particularly in relation to tackling the root causes of the problem. RAN (2016) calls for a broader approach, aimed at earlier intervention and prevention through engaging a wide spectrum of society actors.

Given the multiplicity of drivers of radicalisation, the issue of how to counter violent extremism is complex. In a review of national strategies to target radicalisation, the United Nations Counter-Terrorism Implementation Task Force (UN-CTITF, 2008) identified nine types of national programmes: prison programmes; education; promoting inter-cultural dialogue; tackling economic and social inequalities; global programmes to counter radicalisation; internet policies; legislation reforms; developing and disseminating information; and training and qualifying agencies involved in implementing counter radicalisation policies (UN-CTITF, 2008).

Approaches to countering radicalisation and violent extremism involve both a range of policy interventions and also a variety of stakeholders. According to White and McEvoy (2013) a partnership approach involving law enforcement, intelligence agencies, other statutory organisations, and community-based non-governmental organisations with grassroots credibility is more likely to result in effective CVE. The principles of meaningful partnership must include mutual respect, acknowledgment of respective strengths, skills and expertise between agencies and community-based organisations, and a willingness, in appropriate circumstances, to take calculated risks to ensure that those with the required local knowledge and technical capacity are able to approach hard-to reach groups (White & McEvoy, 2013).

There is little research on what works and does not work in relation to de-radicalisation and counter radicalisation efforts, in part because results are hard to measure (Schmid, 2013). It is difficult to attribute the absence of a terrorist attack, for example, to a particular initiative (Schmid, 2013). De- and counter-radicalisation initiatives can be broadly categorised as follows:

- Promoting integration: Some countries have sought to devise interconnected integration and security measures in order to counter radicalisation and terrorism (Zimmermann and Rosenau, 2009). Bigo et al. (2014) argue that counter-terrorism concerns should not underpin community cohesion programmes and should not aim particularly at Muslim communities in order to prevent alienation of such communities.
- Community outreach: The primary focus of many counter-radicalisation efforts is strengthening and empowering the communities from which radicals and terrorists might emerge (Schmid 2013). Key challenges are deciding which partners to approach for collaboration and which initiatives should target (Schmid, 2014). Framing outreach more holistically, rather than directing it at specific communities as terrorist threats, can be effective. Ranstorp & Hyllengren (2013) emphasise that women should be seen as influential advocates of anti-extremist measures.
- Counter-narratives: The aim is to expose the shortcomings of radicals' and extremists' narratives and to counter their ideas (Schmid, 2013; Parent & Ellis, 2013).

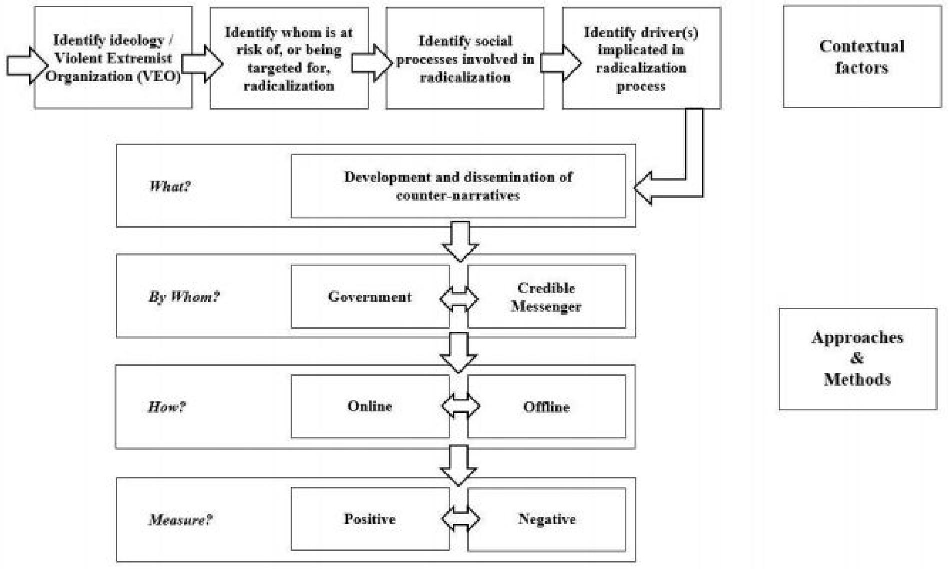
The role for online/social media in countering violent extremism

It is widely acknowledged that in recent years, the use of the Internet by violent extremists as a means of spreading propaganda, raising funds, recruiting members, and communicating with activists has expanded exponentially (UN-CTITF, 2008). Violent extremists have also used the Internet as a virtual training camp, establishing various forms of online, private, and person to person or group communication to exchange experience and knowledge (Weimann, 2012; UNODC, 2012).

There is concern that a variety of state and non-state actors are deploying strategies (recruitment, radicalisation, propaganda) which threaten international stability, social cohesion, and human rights (Ferguson, 2016). There are numerous examples of how advocates of violent extremism (IS, Al-Shabaab, AQIM etc.) are developing media and communication strategies to promote violent extremism (Jones, 2013; Liang, 2015). These organisations are especially adept at their use of social media.

The question of how to limit terrorist use of the Internet has been discussed for some time (UN-CTITF, 2008). Much of the debate has centred on questions of whether governments should intervene through censorship, monitoring and counter-propaganda programmes, or allow the free flow of traffic on the Internet to support democratic values such as freedom of expression (Fidler, 2015). Online CVE programmes are routinely divided into positive and negative measures. In general terms, positive CVE strategies are those that seek to challenge extremist narratives and propaganda by producing counter-content, negative strategies are designed to “block, filter, take-down or censor content (Davies et al, 2016).

Figure 1 CVE Programme Structure



Identify ideology / Violent Extremist Organization (VEO)
Identify whom is at risk of, or being targeted for, radicalization
Identify social processes involved in radicalization
Identify driver(s) implicated in radicalization process
Contextual factors
What?
Development and dissemination of counter-narratives
By Whom?
Government
Credible Messenger
How?
Online
Offline
Measure?
Positive
Negative
Approaches & Methods

Source: Davis et al (2016: 62)

The internet can be used in a variety of ways to counter violent extremism (UN, 2009). While packaged as positive measures, many CVE initiatives have a significant potential to threaten the human rights to equality and freedom from discrimination, the right to privacy, and the freedoms of expression, association, and religion or belief.

Countering use of the Internet to perform terrorist attacks by remotely altering information on computer systems or disrupting the flow of data between computer systems

It is agreed by academics and policy makers that the most important contribution to the fight against terrorist cyber-attacks is the development and expansion of cyber-crime laws (Jarvis et al, 2015; UN, 2009). The Council of Europe Convention on Cyber-crime has achieved wide acceptance as a model for international cyber-crime legislation (UN, 2009). The International Telecommunications Union is building on its work, developing a cyber-law 'toolkit'. A number of other organisations, such as the Gulf Cooperation Council, are working at the regional level to promote uniform cyber-crime laws.

More relevant to a possible terrorist cyber-attack are attempts to build capabilities for protection of infrastructure and incident response at the regional and international levels. One recent example is IMPACT, the International Multilateral Partnership Against Cyber Threats hosted in Malaysia (ITU-IMPACT, 2012). This initiative aims to perform a number of functions, providing a worldwide forum for government and industry; an international incident response capability; cyber-security training, and security testing and certification.

Countering use of the Internet as an information source for terrorist activities

The issue of terrorist access to useful but legitimate content is difficult to resolve (UN, 2009). There are instances in which providers have been required to remove or reduce resolution of images of potentially at-risk sites. However, these would not cover major civilian areas. Given terrorists' tendency to attack civilians and soft targets, such measures are likely to be limited as a counter-terrorist tool.

Countering use of the Internet as a means for disseminating content relevant to the advancement of terrorist purposes

Given the difficulty of agreeing a single definition for terrorism-related content, the issue of countering the dissemination of such material on the Internet tends to be addressed at a political level through a number of laws and approaches (UN, 2009). Depending on the jurisdiction, some items of content that may be related to terrorism may already be illegal without recourse to terrorism laws (UN, 2009). This could include, for example, videos featuring graphic depictions of terrorist violence, or material expressing racist views of particular ethnic or religious groups.

By contrast, official material attributable to terrorist groups could be largely inoffensive. This is the case with many official websites, particularly ethno-nationalist groups (Weimann, 2012). There may nonetheless be an objection to such content on the grounds that it fulfils a part of a terrorist group's wider strategic agenda and thereby adds value to its acts of violence.

It may be considered necessary to create new legislation dealing with certain categories of content that may be particularly relevant because of their availability via the Internet. The most obvious example of this is provided by the Council of Europe Convention on the Prevention of Terrorism, which contains provisions against 'public provocation to commit a terrorist offence' and the dissemination of material relating to terrorist training (UN, 2009). The European Union New Framework Agreement on Countering Terrorism has partially adopted this approach (Ryan, 2007). The potential limitations that such a broad law might place on a fundamental human right to freedom of expression are cause for concern (Fidler, 2015).

If content is illegal in one country, but is hosted in another, then removing it may be difficult, though not impossible. It may be, for example, that a company with international operations chooses to conform to the laws of another State regarding content, rather than forego business in that country. However, this is not a consistently effective approach. An alternative is to filter for illegal content at the local level. Although this has a number of disadvantages; depending on how heavily the State wants to filter, it may be expensive and may also reduce the speed and performance of the Internet nation-wide (UN, 2009).

Countering use of the Internet as a means for supporting communities and networks dedicated either to pursuing or supporting acts of terrorism

It is possible to disrupt virtual communities in a number of ways. Since many online communities are based around a virtual setting such as a website or bulletin board, removing this site may be one way to disrupt the community (UNODC, 2012). Moreover, since radical online communities are likely to be relatively easy to infiltrate as they are established, creating alternative, trusted forums may be a difficult process (UN, 2009).

At present, Internet communities that offer ideological support for terrorism do still exist on publicly accessible forums. However, the more serious examples of online networking support for terrorism have taken steps to preserve a measure of secrecy. For example, using password-protected forums. Such forums serve to preserve a veil of privacy over the activities of the community. However, they are not very secure, as the anonymity of the Internet means that they are inherently vulnerable to infiltration, particularly when the forum is first set up (UN, 2009).

3. The role of online/social media in providing counter-narratives

The range of uses of the Internet to counter violent extremism mentioned above suggests that there is no single, integrated approach possible to address the issue of use of the Internet for violent extremist purposes. Developing coherent and coordinated international responses to is therefore particularly challenging given national sensitivities regarding jurisdiction, issues around freedom of expression and allocation of responsibility for monitoring and censoring online information.

Various experts note that the Internet is rarely the sole instrument of radicalisation and is not considered a cause of radicalisation (Bigo et al., 2014; Schmid, 2013; Conversi, 2012). It has, however, played an important role in the dissemination of radical messages; the creation of a virtual ideological community; the raising of funds; the communication between radicals and members of terrorist organisations; and the radicalisation of vulnerable individuals (Schmid, 2013; Parent & Ellis, 2011). There has been a rise in radical groups and individuals using social media sites, such as Facebook (Osman, 2010; cited in Parent & Ellis, 2011). If individuals become absorbed in webs of information, their susceptibility to recruitment increases (CSIS, cited in Whine, 2009).

Whilst efforts in reducing accessibility to terrorist content are important, they alone will not prove an effective enough deterrent. It has become increasingly apparent that preventing and tackling radicalisation leading to terrorism and violent extremism is not only a security issue, but is also about addressing public opinion and countering and challenging extremist ideologies (RAN, 2016).

Strategic communications that provide counter-narratives to terrorist propaganda is one means of countering violent extremism. Online and social media are particularly useful in the dissemination of counter narratives in multiple languages, to reach a broad, geographically diverse audience. The Center for Strategic Counterterrorism Communications, based in the United States, offers an example of a recently launched inter-agency initiative which is aimed at reducing radicalisation and extremist violence. It identifies extremist propaganda on the Internet in a timely manner, responding swiftly with targeted counter-narratives via a wide range of communications technologies, including digital tools (UNODC, 2012).

Counter narratives explored

The term 'alternative narratives' and counter narratives are often used interchangeably to refer to on- and offline communication activities which directly or indirectly challenge extremist propaganda in different types of fora such as, for example, face-to-face, using testimonials, blogs and chatrooms, social media websites etc. (RAN, 2016; Thompson, 2010; Ashour, 2011).

With the Internet playing a role in radicalisation, it has become an increasingly important security issue to devise strategies to counter online narratives. Thompson (2011) argues that the intelligence and national security communities need to become more involved in social media themselves in order to better understand its potential as a medium for radicalisation. Ashour (2010) outlines a three-pillared strategy for the implementation of online counter-narratives:

- The message, which requires the creation of multi-layered and attractive counter-messages to terrorist group ideology that are tailored to individual groups.
- The messengers, who must appear to have some sort of legitimacy or credibility with the target group. Ashour (2010) identifies former radicalised individuals as a resource for delivering counter-narrative messages.
- The media, which requires careful publication and dissemination of the counter-narrative message.

One of the most important lessons of alternative/counter narratives is that different audiences hold different types of opinions and ideologies. This broad spectrum must be identified and these audiences must be specifically targeted if alternative narratives are to be effective. This can vary from the micro-level focusing on disengagement of individuals to a more broad societal approach at the macro-level (RAN, 2016).

Counter narrative messengers

RAN (2016) comments that credibility and trust worthiness of the individual, group or institution delivering the message or narrative is as important as the message itself. Different messengers should be utilised for the different types of alternative narratives. Five types of messengers for the different layers in alternative narratives have been distinguished by (RAN, 2016: 239):

- Government leaders, communication and policy advisors are most suited to deal with the political counter narrative.
- Key members of civil society, representation groups (including victims) and journalists are deemed credible to counter moral narratives. Families, social workers and peers can also play a role in this respect.
- Religious leaders, institutions and communities. Mullahs, imams and Muslims in general are best equipped to engage in this type of religious counter narrative.

- Former violent extremists may in some cases be appropriate messengers for deploying the social alternative narrative to promote the message that there is nothing heroic about violent extremism.
- Victims are considered to be credible messengers as their testimonials can divert (potential) radicals from becoming violent extremist.

Further to this, successful online alternative narratives often have an effective branding campaign, including the use of music, polished production and compelling stories, in common with their target content (RAN, 2016: 241).

- Linking to existing narratives: It can be effective to link to narratives that are already popular as it takes the counter-narrative directly to the target audience. This may be through posting an "in response to" video on YouTube linking to the extremist content, or through reaching an extremist group through the music they like.
- Emotions are important: Narratives need to appeal to human emotion as evidence alone can be refuted and countered.
- Humour entertains: Humour can be a disarming way to share the counter-narrative, especially from credible sources. However given the subject matter it should be used carefully and in a sensitive manner.

By themselves, alternative narratives may not interrupt the radicalisation process or may not de-radicalise individuals, but they can deconstruct extremist messages for individuals at risk. Online alternative narratives should go hand in hand with offline counter-measures, for example, educating young people at school about the consequences of violent extremism. The Internet and social media might place seeds of doubt. However ties between people (bridging and bonding) that open the possibility for a change of mind can be persuasive.

Evaluating alternative/counter narratives is notoriously difficult. RAN (2016) call for some measurable targets to be established from the outset. Viewer analytics, level of engagement and impressions will be available on many online platforms and social media websites.

The role for online/social media in countering violent extremism in East Africa

The evidence base for the use of online/social media in countering violent extremism in East Africa is limited with few empirical studies that explore the impact of either online/social media campaigns or counter narratives. Despite this limited evidence base, various organisations are seeking to utilise online/social media to counter violent extremism. The Global Center on Cooperative Security (2015) note that media practitioners, civil society organisations, and policymakers could be supported in the development of regional and sub-regional strategic communication plans which create common approaches to communicating about and engaging violent extremist groups, and developing shared counter narratives drawing on local and regional resources.

The Intergovernmental Authority on Development (IGAD) Security Sector Program (SSP), in partnership with the Global Center on Cooperative Security, is actively convening discussions on the following topics:

- Drivers and enablers of violent extremism, current national and regional P/CVE initiatives
- Strategies, and best practices, role of government agencies and civil society actors engaged in P/CVE

- Early warning indicators and early response mechanisms for violent extremism
- National and regional P/CVE priorities and opportunities for engagement
- Areas for collaboration and coordination on regional P/CVE programming

The outcome of these discussions will inform the establishment and development of the Horn and Eastern African Counter Violent Extremism Center of Excellence and Counter-Messaging Hub in Djibouti. Agreement was reached on the importance of effective counter messaging campaigns to delegitimise the ideas of violent extremists. IGAD (2016) identified the essential role of madrassas and imams in countering violent extremist messages, while at the same time acknowledging that radicalisation to violence may also take place in skewed religious environments. It also highlighted lack of organisation and oversight of madrassas, and their control and/or influence by independent and often external entities as a key problem. As such, the empowerment and strengthening of local Muslim communities has been suggested, so they can lead the debate and set the frameworks for discussion rather than being subject to external control and guidance.

IGAD (2016) note that strategies should go beyond traditional platforms (like radio) to include social media and peer-to-peer communication, such as WhatsApp, where appropriate, particularly when targeting youth vulnerable to radicalisation. Examples of projects that utilise social media to a lesser or greater extent includes:

Kenya Community Support Centre (KECOSCE)

This project aims at empowering communities to prevent and contest radicalisation on the Coast of Kenya. It carries out research, documentation and youth capacity building to increase resilience to counter violent extremism, create community organisations, and to provide continuous space for community dialogue with public institutions, local authority officials, politicians and development actors to deal with grievances (Hassan, 2014).

KECOSCE uses multimedia such as billboards, LED screens, radio commercials and social media to reach wider communities and create awareness of the negative impact of radicalisation and violent extremism.

Uganda Muslim Youth Development Forum (UMYDF)

UMYDF advocates zero tolerance for extremist narratives. It urges imams, Muslim leaders and Muslims to focus on religious literacy, and engages Imams in social media. This initiative works in partnership with security actors and other faiths, organising Masjids as centres of development, and establishing the Muslim Leadership Institute to provide the most at risk youth, skills in leadership (Hassan, 2014).

4. Case study programmes

While the internet is an important tool in modern radicalisation, few de- and counter-radicalisation programmes have included an online component (Hinds, 2013). In broad policy terms, three approaches can be adopted: a hard strategy of zero tolerance; a softer strategy of encouraging internet users to directly challenge extremist narratives and report offensive or illegal material; and an intelligence-led strategy of monitoring, which leads to targeting, investigation, disruption and arrest. Most countries adopt a mixed approach, using a combination of all three depending on the nature of the content, the identity of its creators or hosts, and the tools at their disposal. RAN (2016) has identified a number of best practice examples of programmes that tackle extremism (in a variety of forms) that involve a social media component.

Web constables

Web constables are police officers who work on social media. They participate in discussions across different social media networks (Facebook, Twitter, etc.). Web constables are available for question and answer sessions, passing on information and making complaints about other people or the police. They try to solve cyberbullying cases where they take place (e.g. gaming sites or forums). Their main focus is dealing with vulnerable youth. They do background checks based on police databases and gather social media information that can be passed on to local police departments, who then collect information that cannot be found on social media (domestic violence, school issues, possibility of acquiring a gun etc.). This information is used to plan how to help those identified as being at risk. Web constables are also active in countering (predominantly right wing) youth radicalisation.

Evidence and evaluation

Web constables measure the number of reported cases, which are rising year on year. They are also involved in outreach activities, giving lessons to students and parents to make people aware of the initiative.

Identity, Belonging and Extremism (IBE)

This media content-based project is delivered in schools, tailored to local needs and created in consultation with students. IBE seeks to engage students on issues relating to the online world with an offline engagement medium. Its themes are generic but crucial to understanding radicalisation and extremism, and it targets both mind-set and behaviour. The programme is based on the premise that the majority of extremist narratives offer three simple modes of engagement and understanding: a sense of Identity; a sense of belonging; and a sense of loyalty/duty. IBE discusses racism, Islamism, islamophobia, stereotypes and social media to tackle these narratives.

The project targets the visual, emotional and social reality of an individual, and offers an alternative that is based on individual reasoning and ‘group think’ behaviour. The programme seeks to engender critical thought into the process of how actions affect the person.

Evidence and evaluation

The IBE project has been part of a RAN evaluation and the UK Home Office has recognised it as best practice for its user driven focus and engagement. Over 500 students have been engaged across Years 9, 10 & 11 (13-16 age range).

HOPE Not Hate (HNH)

The programme uses counter narratives to challenge extremism (for instance the #wearethemany hashtag). The programme provides accurate, research-based analysis of extremist groups in order to empower communities to challenge hatred/violent extremism when it presents itself and undermine the credibility of extremist campaigns. This includes tackling myths and inaccuracies through blogging, newspapers, leaflets, meetings, videos, education, speeches, T-shirts etc. HNH provides a platform and support for vulnerable individuals to speak out against extremists in communities. As well as a bi-monthly publication, HNH has three separate blogs and roving news links that provide up-to-date information and intelligence on extremists.

HNH also has a large social media presence where they interact with the public, providing them with information, resources and positive news and stories to highlight empowering good practice from others. HNH also works extensively with people inside hate/extremist organisations and also ex-extremists to provide a non-sensationalist view of extremist groups and individuals. HNH publishes four research documents per year, separate to the magazine and website.

Evidence and evaluation

HNH's campaigning and education is widely credited with the defeat of the far-right British National Party in the 2010 elections.

Against Violent Extremism (AVE)

This network aims to provide a platform for former violent extremists and survivors of violence to connect with each other to share ideas, collaborate, and identify relevant and related partners, projects and resources that can help amplify their initiatives and bring them to a wider audience. It has three primary functions: to connect credible messengers to one another so they can learn best practices and share ideas; to match credible messengers to private sector resources, skills and support; and, in the aftermath of an extremist attack, it can act as a positive outlet for members of the public wishing to 'do something' as they can register their skills and interests in order to get involved with AVE projects working to counter extremism.

It looks at all forms of violent extremism (from far right and far left to AQ-linked and inspired groups, and gangs). Individuals can join the network on the central AVE website (and also on Facebook, Twitter and Google +). AVE advocates for the role which former extremists and survivors of violent extremism have to play in pushing back against extremist narratives. In addition to the above, AVE also actively seeks to facilitate longer term project partnerships, from education programmes using members narratives to prison intervention programmes.

Evidence and evaluation

AVE is atypical in that it functions as a network. As such, AVE's performance can largely be measured by the growth of the network and partnerships facilitated. To date, AVE has a growing membership of over 2139 connections (306 formers, 164 survivors, and 69 projects inclusive). In addition to its quantitative successes, AVE has also facilitated partnerships offline leading to the establishment of numerous sub-projects.

Al-Sakina

Al-Sakina is an independent, non-governmental organisation with financial support from the Ministry of Islamic Affairs (Saudi Arabia). It was initiated to engage in online dialogue as a way to combat online radicalisation. The Sakinah Campaign promotes a one-on-one engagement strategy designed to counter the appeal of violent extremist ideologies online. Volunteers include religious scholars, psychologists and psychiatrists, sociologists and academics. The programme is divided into different sections. The Scientific Section - made up of academic and religious scholars and psychologists - directly engages users in dialogue. Though the scheme works with those seeking answers to Islamic questions, it also engages directly with those who have expressed solidarity with extremist narratives. Transcripts of conversations are often published online to extend the programmes reach. Additionally, the Sakinah Campaign houses a Psycho-Social Section, which explores the social and social-psychological dynamics of violent extremist groups, and the Monitoring Section, which provides research and analysis into online extremist content. Finally, the Publishing Section is responsible for the formulation and dissemination of religious texts and educational materials. The programme also contains a Design Section, Service-Site Section, Public-Relations Section and Supervision and Planning Section.

The Al-Sakina process involves appointed groups of academics and intellectuals visiting websites popular with Islamic radicals and challenging extreme interpretations of Islam (Hearne & Laiq, 2010). To target younger audiences, the organisation uses social media and produces video materials in English and Arabic (ISD, 2013).

5. References

Ashour, O. (2010). Online de-radicalisation? Countering violent extremist narratives: Message, messenger and media strategy. *Perspectives on Terrorism* 4 (6): 15-19. http://terrorismanalysts.com/pt/index.php/pot/article/view/128/html

Bigo, D., Bonelli, L., Guittet, E.P. & Ragazzi, F. (2014). *Preventing and countering youth radicalisation in the EU*. Brussels: EU. http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/509977/IPOL-LIBE_ET(2014)509977_EN.pdf

Borum, W. (2011). Radicalization into Violent Extremism I: A Review of social science theories. *Journal of Strategic Security* 4 (4): 7 – 36. http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1139&context=jss

Conversi, D. (2012). Irresponsible radicalisation: diasporas, globalisation and long-distance nationalism in the digital age. *Journal of Ethnic and Migration Studies* 38 (9): 1357-1379. DOI: 10.1080/1369183X.2012.698204.http://www.tandfonline.com/doi/pdf/10.1080/1369183X.2012.698204

Davies, G. et al. (2016) Toward a framework understanding of online programs for countering violent extremism. *Journal for Deradicalization* Spring 2016 no. 6: 51 – 86. http://journals.sfu.ca/jd/index.php/jd/article/view/43/38

El-Sai'd, H., & Harrigan, J. (2012). *De-radicalising violent extremists: Counter-radicalisation and de-radicalisation programmes and their impact in Muslim majority states*. Abingdon: Routledge

El-Sai'd, H. (2012). *De-radicalising Islamists: Programmes and their impact in Muslim majority states.* London: The International Centre for the Study of Radicalisation and Political Violence. http://icsr.info/wp-content/uploads/2012/10/1328200569ElSaidDeradicalisation1.pdf

Feddes, A. and Gallucci, M. (2015). A literature review on methodology used in evaluating effects of preventive and de-radicalisation interventions. *Journal for Deradicalization* Winter 2015 no. 5: 1-27. http://journals.sfu.ca/jd/index.php/jd/article/view/33

Ferguson, K. (2016). *Countering violent extremism through media and communication strategies A review of the evidence.* Cambridge, UK: Partnership for Conflict, Crime and Security Research. http://www.paccsresearch.org.uk/wp-content/uploads/2016/03/Countering-Violent-Extremism-Through-Media-and-Communication-Strategies-.pdf

Fidler, D. (2015). *Countering Islamic State exploitation of the internet*. Cyber Brief. New York: Council on Foreign Relations Press. http://www.cfr.org/cybersecurity/countering-islamic-state-exploitation-internet/p36644

GCCP. (2015). Countering violent extremism and promoting community resilience in the Greater Horn of Africa: An action agenda. New York: Global Center on Cooperative Security. http://www.globalcenter.org/wp-content/uploads/2015/05/HoA_Action_Agenda_Low_Res.pdf

Hassan, N. (2014). The role of CSOs in Countering Violent Extremism (CVE) - A case of actors in East African Region. UMYDF Working Paper Series 1: 2014. Kampala: Uganda Muslim Youth Development Forum. http://umydf.org/downloads/Role%20of%20CSOs.pdf

Hearne, E., & Laiq, N. (2010). A new approach? Deradicalization programs and counterterrorism. Vienna: International Peace Institute. https://www.ipinst.org/2010/07/a-new-approach-deradicalization-programs-and-counterterrorism

Hinds, R. (2013) Islamic Radicalisation in North and West Africa: Drivers and approaches to tackle radicalisation (GSDRC Rapid Literature Review). Birmingham, UK: GSDRC, University of Birmingham. http://www.gsdrc.org/docs/open/islamicradicalisationnwafrica.pdf

IGAD. (2016). Strengthening regional capacities to prevent and counter violent extremism in the Greater Horn of Africa. Djibouti: IGAD. http://www.globalcenter.org/wp-content/uploads/2016/04/17-19Feb_HoA-CVE-Stakeholders-Meeting-Outcome-Document_FINAL.pdf

ISD. (2013). *Case study report: Al-Sakina, Saudi Arabia*. London: Institute for Strategic Dialogue. https://www.counterextremism.org/resources/details/id/414/al-sakina

ITU-IMPACT. (2012). International Multilateral Partnership Against Cyber Threats (IMPACT). Geneva/Cyberjaya: International Telecommunications Union/IMPACT. http://www.itu.int/ITU-D/cyb/publications/2012/IMPACT/IMPACT-en.pdf

Jarvis, L. Nouri, L. & Whiting, A. (2015). Terrorism, violence and conflict in the digital age. In: *Researching Terrorism, Peace and Conflict Studies: Interaction, Synthesis and Opposition* (eds. Tellidis, I. and Toros, H.). Abingdon: Routledge.

Jones, S. (2013). *The Terrorist Threat from Al-Shabaab.* Testimony. Santa Monica: RAND. http://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT400/RAND_CT400.pdf

Liang, C. (2015). *Cyber Jihad: Understanding and countering Islamic State propaganda.* GCSP Policy Paper. Geneva: Geneva Centre for Security Policy.

http://www.gcsp.ch/News-Knowledge/Publications/Cyber-Jihad-Understanding-and-Countering-Islamic-State-Propaganda

Parent, R. B. & Ellis, J. O. (2011). *Countering radicalization of diaspora communities in Canada.* Vancouver: Metropolis British Columbia, Centre of Excellence for Research on Immigration and Diversity. http://mbc.metropolis.net/assets/uploads/files/wp/2011/WP11-12.pdf

RAN. (2016). *Preventing radicalisation to terrorism and violent extremism.* Amsterdam: Radicalisation Awareness Network. http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation_awareness_network/ran-best-practices/docs/ran_collection-approaches_and_practices_en.pdf

Ranstorp, M. & Hyllengren, P. (2013). *Prevention of violent extremism in third countries: Measures to prevent individuals joining armed extremist groups in conflict zones. Executive summary*. Stockholm: Center for Asymmetric Threat Studies (CATS), Swedish National Defence College. http://www.diva-portal.org/smash/get/diva2:688158/FULLTEXT01.pdf

Ryan, J. (2007). *Countering militant Islamist radicalisation on the Internet.* Dublin: The Institute of International and European Affairs. http://www.iiea.com/publications/countering-militant-islamist-radicalisation-on-the-internet

Schmid, A. P. (2014). *Violent and non-violent extremism: two sides of the same coin?.* The Hague: The International Centre for Counter-Terrorism (ICCT). http://www.trackingterrorism.org/sites/default/files/chatter/ICCT-Schmid-Violent-Non-ViolentExtremism-May-2014_0.pdf

Schmid, A. P. (2013). *Radicalisation, de-radicalisation, counter-radicalisation: A conceptual discussion and literature review.* The Hague: International Centre for Counter-Terrorism (ICCT). http://www.icct.nl/download/file/ICCT-Schmid-Radicalisation-De-Radicalisation-CounterRadicalisation-March-2013.pdf

Thompson, R. L. (2011). Radicalisation and the use of social media. *Journal of Strategic Security* 4 (4), 167-190. http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1146&context=jss

UN. (2009). Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes New York: United Nations. http://www.un.org/en/terrorism/ctitf/pdfs/wg6-internet_rev1.pdf

UN-CTITF. (2008). First report of the working group on radicalisation and extremism that lead to terrorism: Inventory of state programmes. New York: United Nations. Retrieved from: https://data.unhcr.org/syrianrefugees/download.php?id=10129

UNODC. (2012). *The use of the Internet for terrorist purposes*. Vienna: United Nations Office on Drugs and Crime. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

Weimann, G. (2012). Lone wolves in cyberspace. *Journal of Terrorism Research* 3 (2). http://jtr.st-andrews.ac.uk/articles/10.15664/jtr.405/

Whine, M. (2009). The radicalisation of diasporas and terrorism. In: *The radicalisation of diasporas and terrorism (eds.* D. Zimmermann and W. Rosenau): 17-40. Zurich: Center for Security Studies. http://www.css.ethz.ch/publications/pdfs/ZB-80.pdf

White, S. and McEvoy, K. (2013). *Countering violent extremism: Community engagement programmes in Europe*. Dohya: Qatar International Academy for Security Studies (QIASS). http://soufangroup.com/wp-content/uploads/2013/12/QIASS-CVE-Paper-Phase-II-Paper-I.pdf

Zimmerman, D. & Rosenau, W. (2009). Introduction. In: *The radicalisation of diasporas and terrorism (eds.* D. Zimmermann and W. Rosenau): 9-16. Zurich: Center for Security Studies. http://www.css.ethz.ch/publications/pdfs/ZB-80.pdf

Suggested citation

Avis, W. (2016). *The role of online/social media in countering violent extremism in East Africa* (GSDRC Helpdesk Research Report 1,380). Birmingham, UK: GSDRC, University of Birmingham.

About this report

This report is based on four days of desk-based research. It was prepared for the UK Government's Department for International Development, The views expressed in this report are those of the author, and do not necessarily reflect the opinions of GSDRC, its partner agencies or DFID.

The GSDRC Research Helpdesk provides rapid syntheses of key literature and of expert thinking in response to specific questions on governance, social development, humanitarian and conflict issues. Its concise reports draw on a selection of the best recent literature available and on input from international experts. Each GSDRC Helpdesk Research Report is peer-reviewed by a member of the GSDRC team. Search over 400 reports at www.gsdrc.org/go/research-helpdesk. Contact: helpdesk@gsdrc.org.