JOURNAL FOR DERADICALIZATION

Summer 2016
Nr. 7
ISSN: 2363-9849

Terrorism, the Internet and the Social Media Advantage: Exploring how terrorist organizations exploit aspects of the internet, social media and how these same platforms could be used to counter-violent extremism.

By: Luke Bertram[1]

Abstract

The deeply engrained nature of social media in modern life have provided ease of access to information and speed of use within almost every aspect of a person's life. These same benefit are also available to terrorists and their organizations. The same technology that allows for a globalized world to interact without regard for distance or physical location is also utilized, exploited and adapted to by terrorist organizations to conduct operations, reach candidates and ensure organizational longevity.

This article takes the position of observer of these advancements with the end goal of informing counter-violent extremism strategists of the advances that terrorist groups have already made in digital technology; and where the priority of intervention strategies should be aimed. Further, this is intended to guide policy makers to embrace and utilize digital technologies as a mechanism to carry counter-radicalization and counter-violent extremism interventions through the same digital potential and reach the same audiences as terrorist organizations. What appears strongly apparent is that social media will not abate from its intrinsic position graphed into daily life. This means that counter-terrorism, counter-radicalization and counter-violent extremism strategies must take up the same technology in order to effectively discredit and nullify extremist groups – a digital problem needs a digital solution.

Key Words

Digital technology and terrorism; Counter-Terrorism; Digital Media; Terrorist Groups Digital Potential; Digital Existence.

[1] Fellow, German Institute on Radicalization and De-Radicalization Studies (GIRDS)

Introduction & Focus

How have terrorist organizations benefited from social media advances? The short answer is that social media has delivered advantages across many varied operational spheres and hence, have come to be a greatly beneficial modern asset to terrorist organizations.

Social media activities of terrorist organizations can broadly be grouped into two categories. These categories are not mutually exclusive to each other and as will be discovered, there is often crossover between the aim and activity of these two categories.

The first category could be termed as the communication benefit, which encompasses recruitment through reaching out to potential radicals, creating group forums, collaborating with terrorist associates, administering digital training environments, coordinating organizational activity and propagating terrorist organization material (Thomas, 2003; Mishra, 2003; Rogan, 2006; Conway, 2005; Aly, 2016; Klausen, 2015; Conway, 2016). Furthermore, the social media revolution has provided a level of secrecy and clandestine communication, avoiding detection through easily delivered, yet effective encryption protocols that are provided by services such as Whatsapp and some Apple.inc platforms (McMillan, 2016). This article will explore social media as a prominent strategic aspect of terrorist organizations modus operandi that has become intrinsic to recruitment, operational planning and engaging between radicals and organizations beyond intervention (Thomas, 2003; Mishra, 2003; Rogan, 2006, Conway, 2005; Aly, 2016; Klausen, 2015; Conway, 2016).

The second category of activity could be termed as operational digital action, which includes digital activities of terrorist organizations that are intended to spread terror. These operational digital actions may include cyber-based sabotage of infrastructure, or propagating fear of attack through threat (Thomas, 2003; Grob-Fitzgibbon, 2004). Furthermore, operational digital actions also take in activity that exploit open and restricted source data holdings in order to obtain intelligence assets, support operational financing, operation planning and coordinating activities (Denning, 2001; Thomas, 2003; West, 2014).

Social Media in Terrorism & Extremism Communication

From research, it appears overwhelmingly likely that the greatest benefit to terrorist organizations of social media has been the evolution of communication capability, and this is where this discussion shall begin. Mishra (2003) describes terrorism as being symbolic communication that consists of four distinct pieces of a communication formula, all of which

are needed to achieve the goal of spreading terror. The first piece is the transmitter of the information, this is the terrorist who appears on a video or records a propaganda speech and distributes the terrorist groups message, perhaps the most traditionally recognised example of this might be a propaganda video (Mishra, 2003). The second piece of this communication formula is the message, or the meaning behind the transmission, which will be designed to serve the communication goals of a particular group (Mishra, 2003). This may include video of attacks, twisted ideological teachings or a group's founding principles (Mishra, 2003). Thirdly, the communication formula must reach an audience - there would be little point to conducting attacks that are not publicised, as this would extensively limit the achieved goal of propagating terror amongst a target audience (Mishra, 2003; Grob-Fitzgibbon, 2004; Soo Hoo, Goodman & Greenberg, 2008; Aly, 2016). This is consistent with the assertion of Grob-Fitzgibbon (2004) that the end-gaol of a terrorist group is not actually to target specific individuals or societal sectors, instead to spread fear of attack amongst a wider group or communities. Furthermore, as Braddock and Horgan (2015) identity, through effective utilization of social media platforms, particularly Twitter, Islamic State reaches an expansive audience of followers, potential recruits, combatant entities and opposition through social media communication. Returning to Mishra's (2003) communication formula, the fourth requirement is feedback, or the response of the audience. This response requirement also supports that the primary intent of terrorist groups is not necessarily to kill or injure one individual person, rather it is to spread fear and terror amongst a community (Grob-Fitzgibbon, 2004; Soo Hoo, Goodman & Greenberg, 2008). In considering this end-goal of terrorist groups as being to spread terror, the benefit that social media provide is extensive and undeniable. Furthermore, Soo Hoo, Goodman & Greenberg go so far as to say that:

> "The rise of indiscriminate terrorism is partly a product of the modern electronic mass media, as terrorists may commit these acts almost exclusively for the publicity that they generate" (Soo Hoo, Goodman & Greenberg, 2008. pg.137).

This clearly demonstrates the benefit that social media has provided to Jihadis, as an exceptionally effective method of reaching out to an audience (whether willing or not) in order to propagate messages or media content that meets the goal of spreading terror (Grob-Fitzgibbon, 2004, Soo Hoo, Goodman & Greenberg, 2008; Klausen, 2015). The clear benefit

of digital technologies, such as the internet, to meet this goal is the simplifying and accessibility of all aspects of communication that the internet provides, as well as providing this access at relatively low operating cost (Thomas, 2003; Koehler, 2014).

While not the only component of the digital revolution, the internet is arguably the most integrated, adaptive and expansive feature and hence the provider of greatest benefit if exploited effectively (Harrison, 2002; Conway, 2005; Mackinlay, 2009). The importance and inherent advantage of the internet to terrorist organizations lies in its purpose as a user-friendly communication device (Conway, 2005; Eriksson and Giacomello, 2006). To illustrate this advantage, Conway (2005) notes the ease at which one can seek out and find bomb-making instructions, among other illicit and dangerous material. The internet's highly advantageous purpose as an easily accessible information portal and communication channel is stated as:

> "The internet was designed to maximize simplicity of communication, not security of communication. The price for this has been the increasing opportunity from criminals or wrongdoers to exploit the vulnerabilities of the network for their own ends" (Eriksson and Giacomello, 2006, pg. 225).

This means that the internet itself, as a digital advancement, has provided a strategic benefit to terrorist organizations (Eriksson and Giacomello, 2006). This benefit is delivered through the purpose of the internet's design, being that it strives to streamline communication channels and is not overly onerous in terms of scrutiny (Eriksson and Giacomello, 2006). The benefit of the internet as a communication apparatus is clear, as simplified communication with little oversight is exceedingly beneficial to clandestine activities. The clear benefit of communication capabilities that terrorist organizations benefit from includes recruitment, propaganda dissemination, global linkage between terrorists as well as action coordination through digital communication technology (Thomas, 2003; Weimann, 2006; Rogan, 2006). These facets are defined by Weimann (2006) as computer mediated communication, who explains further that terrorist organization operations are well suited to the use of the internet in stating:

> "…it is de-centralized, it cannot be subject to control or restriction, it is not censored, and it allows access to anyone who wants it" (Weimann, 2006. pg. 25).

The above statement of Weimann (2006) is simplistic to the point that it loses some accuracy, as several examples of state-instigated internet censorship do exist (Denning, 2001). However, if this statement of Weimann (2006) is considered only as a concept, it supports the assertions of others that the internet has been so voraciously taken up as a communication mechanism by terrorist organizations, as it provides the perception of anonymity as well as safe space beyond the reach of state authorities (Weimann, 2006; Rogan, 2006; Von Behr, Reding, Edwards and Gribbon, 2013; Tehrani, Manap and Taji, 2013; Koehler, 2014).

The manner in which social media has affected terrorist organization recruiting practices is broadly that these technologies have provided the ability to digitally cross borders unseen and has shown these organizations into the home of any potential radical. Organizational recruiting can be viewed from two points, being the overcoming of distance and sovereign boundaries (Labi, 2006), as well as the greatly increased ability to distribute propaganda (Thomas, 2003; Mohamedou, 2015; Aly, Macdonald, Jarvis & Chen, 2016). Recruitment of potential terrorists and dissemination of group propaganda are interlinked activities, as it is highly likely that propaganda is a significant factor in the radicalization of a terrorist, accordingly these subjects will be discussed side by side (Pretch, 2007; The Clarion Project, 2014). Labi (2006) supports the notion that through harnessing digital communication technology advances, terrorist groups have been able to make terrorism borderless within cyber environments. This however is not the extent of benefit that social media has brought to recruitment and radicalisation. In terms of radicalisation, Aly, Macdonald et al (2016) refer to a staged progression through an online platform, which first introduces the potential jihadi to the organization's ideology, through to enrolment, progressing to methods of participating in the organization through activity and connecting the new jihadi to others within the organization. Referring specially to Al Qaeda, Aly, Macdonald et al (2016) describe a grassroots-driven recruitment strategy, in that violent extremist propaganda is made readily available via internet or social media platforms, which can be sought out by potential Jihadis, essentially relying to some extent on online self-radicalisation. Conway also notes that terrorist group's recruitment practices have benefited by information communication technology advancements in stating:

> "… it [the internet *sic*] makes information gathering easier for potential recruits by offering more information, more quickly, and in multimedia format" (Conway, 2005. pg. 12).

While dealing specifically with the social media prominence of the Al Qaeda network, Rudner (2016) refers to the inherent connectivity and extremist resource availability as being a valuable tool in the recruitment of Jihadis, which have been more successful in recruitment than conventional person to person means have been.

There are clear consistencies in theory between Conway (2005), Aly, Macdonald et al (2016) and Rudner (2016) in that these sources note that an advantage of the internet and social media has been the ease of availability, extensive volume of material and the ease at which this material can be provided. The benefit from this aspect is the ability to so readily support recruitment, however the further benefit is the creation of a substantial digital presence that may give an organization prominence and influence due perhaps to the size of one organization's digital presence, which it may otherwise not have. Meaning, an organizations virtual size and resulting influence is likely to be far greater than a non-digital terrorist organization could hope to evolve to.

This aspect of the benefit that terrorist organizations take from social media is summed up effectively by Rudner, who states

> "The Internet and social media, for their part, offer radical preachers, strategists, and enthusiasts especially advantageous capabilities for reaching out and influencing, inciting, and motivating jihadist activism at a global level" (Rudner, 2016. pg.4).

Communication between terrorist organizations, vulnerable persons and potential Jihadis is greatly benefited through the availability of these cyber environments such as forums, social media platforms, webpages, blogs, post boards and email (Denning, 2001; House of Commons, United Kingdom, 2012; Klausen, 2015, Aly, Macdonald et al, 2016). The advantage of digital technology to terrorist groups is clear, social media crosses borders and allows groups to connect associates and reach out to persons vulnerable to radicalization (Mackinlay, 2009; Torok, 2013). The ease of communication from any place on Earth to any

place on Earth is a significant strategic benefit that terrorist organizations are exploiting. As an example of this global linkage, Coker (2002) describes Al Qaeda as being an organization that is built on networks, possessing global resources that can be accessed to coordinate operations, and thus shows Al Qaeda to be a true beneficiary of globalized social media communication. This almost unfettered ability to communication with like-minded associates, reach out to those who are vulnerable to radicalization as well as making terrorist propaganda so readily accessible are clear advantages to terrorist organizations. Further, as Von Behr, Reding, et al (2013) note, the internet has provided terrorist groups and individuals with a safe environment, suited to clandestine activities as it provides a potential measure of secrecy and anonymity. Additionally, the internet provides quick access to information, like-minded community forums that is also benefited through the perception that cyber environments are beyond immediate oversight and without intervention in opposition to activities that would otherwise be encountered, had the same extremist material been sought in a physical environment (Von Behr, Reding, et al, 2013). This perception of safety within the online environment is also supported by Koehler, who states:

> "The Internet provides a perceived constraint-free space and anonymity. This provokes or motivates individuals to speak or act out more radically online as they would normally do offline" (Koehler, 2014. pg. 118).

Koehler (2014) primarily bases findings of internet use amongst extremist organizations in the context of former right-wing Neo-Nazi's of Germany. What is observed from the extreme right-wing Neo-Nazi example is that amongst the significant majority of former-extremists, the use of the internet had become part of the normal organizational operation and is used heavily in communication, disseminating propaganda and coordinating administrational responsibilities amongst group members (Koehler, 2014). The question from this example is why has the internet become such a fundamental operating tool of the extremist groups? The answer is, in addition to the obvious benefits to communication, logistical barriers, social constraints and risk of being detected while operating within a cyber-environment are perceived to be reduced or not existing within a digital realm (Von Behr, Reding et al, 2013; Koehler, 2014). The benefit that the use of the internet in the manners that these right-wing Neo-Nazi's used it is, as they perceived, that the internet provides a

clandestine environment as well as the ability to access extremist material that is only constrained by the speed of one's internet connection (Von Behr, Reding et al, 2013; Koehler, 2014). Koehler (2014) also notes a belief amongst subjects that if communicating with fellow extremists or participating in organizational activity online, they had positioned themselves outside the jurisdiction of any state law enforcement. This perception of secrecy and being beyond intervention is also beneficial to terrorist organizations, as it is likely to cause terrorists to feel that they are impervious to law enforcement intervention and perhaps become more willing to complete activities on behalf of a terrorist organization.

Khalil (2014) also provides valuable commentary of the benefit that digital technology advances have provided to terrorist organizations and notes that around 1998, Al Qaeda recognised the value of propagating a message through commercial media avenues. However, prior to the expansive availability of the internet, the ability of terrorist organizations to self-publicise was minimal and all were heavily dependent on traditional media outlets (Khalil, 2014; Klausen, 2015). However, as the internet and social media emerged, the ability of terrorist groups to self-publicise increased extensively through platforms such as Facebook and Twitter, as well as uploading material for the access of followers through platforms including forums, web-pages and video hosting websites (Torok, 2013; Khalil, 2014; Simon, Goldberg, Aharonson-Daniel, Leykin and Adini, 2014; Torres-Soriano, 2016). Denning (2001) also refers to the internet being capable of overcoming censorships and refers to the ability to access information that may be restricted from publication in commercial media. This outlines that social media and internet advancements has provided key operational advantages to terrorist organizations, in that it has removed the reliance on third party media and allows organizations to self-propagate their own material, and further have the material re-disseminated widely amongst social media networks.

Heickerö (2014) notes that the use of internet platforms has become key aspects in the recruiting strategy of extremist groups and explains that the use of the internet for recruitment is multiply-faced, as it is used to reach out to potential jihadists through social media, as well as propaganda material being made easily available online. The benefit that is displayed by Heickerö (2014) is access and availability of terrorist groups to an audience and potential recruits, as well as providing access to terrorist organizations by potential terrorists.

As has been discussed, terrorism is communication with an audience with an end goal being to create terror (Grob-Fitzgibbon, 2004, Soo Hoo, Goodman & Greenberg, 2008). As

Mohamedou (2015) notes, significant advancement in the manner in which Al Qaeda has used technology to communicate with the wider public and notes that previously terrorist organizations such as Al Qaeda used a mail service to post propaganda video tapes to news outlets. This is quite an antiquated manner for Al Qaeda to go about propagating materials to the public. Compare this outdated postal method to the current ability for terrorist groups to upload videos, pictures, letters and manuals as well as communicate with associates, and what is seen is the undeniable benefit in reaching an audience, which is a direct result of social media (Neumann, 2012; Mohamedou, 2015; Klausen, 2015). While referring particulary to Twitter and Facebook, Klausen supports this stance and states that: "Social media freed Al Qaeda from the dependency on mainstream media" (Klausen, 2015. pg.3).

Setting aside the ease of access to an audience that social media delivers for a moment, by self-distributing propaganda via platforms such as Twitter and Facebook, Al Qaeda and Islamic State have become chief media editors and no longer limited by the whim of a conventional media outlet priorities or constraints. Further, social media completely removes a content barrier between the message transmitter and receiver, essentially groups such as Al Qaeda are brought into direct communication with their audience and are unchecked, able to completely influence the nature of the transmitted message (Klausen, 2015).

In terms of content and production of media material, advances in this information technology field are also extensive and again social media supports groups in transmitting these high production quality materials out to an audience. The content that is uploaded for access or disseminated through social media are high quality media productions that take advantage of advances in digital media and production technology (Mohamedou, 2015). While referring to the production quality of Islamic State media propaganda, the United States' Department of Homeland Security Secretary, Jeh Johnson is quoted as stating: "…it's about as slick as I've ever seen in terms of advertising and promotion." (Tadjdeh, 2014. pg. 1).

The quality of propaganda materials that are produced, as well as the increased ability to disseminate materials are significant advantages for terrorist organizations that are attributable to digital technology advancement, which terrorist organizations are taking full advantage of.

Radicalization & Deployment

Related to the above points, radicalization also warrants discussion, as this aspect of terrorist organization activity that has greatly benefited from social media (Torok, 2013). In plain terms social media has bridged communication barriers and provided ready access to both potential recruits as well as easy access to propaganda. The virtual communities of terrorist organizations that function through the internet are advantageous to terrorist radicalization within numerous focuses (Stevens and Neumann, 2009). These perspectives include both online radicalization involving interaction between a potential terrorist and a party to the terrorist organization, as well as lone wolf terrorists who are self-radicalised online through exposure to non-interactive materials and have no interactive contact with a terrorist group (Von Behr, Reding et al, 2013). Social media has aided terrorist organizations in radicalizing Jihadis through the methods of recruitment within both online radicalization and online self-radicals. This has been supported by the social media aspects of access to information as well as potential Jihadis, the borderless nature of virtual communities, as well as the access to platforms from which propaganda can be disseminated (Stevens and Neumann, 2009; Koehler, 2014; Heickerö, 2014). However, the social media advantage to radicalization does not end there. While social media provides such extensive access to a virtual community, simultaneously they also limit interaction with the normative world and isolate potential radicals from circumstances outside of the cyber environment (Torok, 2013). The isolation of a potential terrorist is conducive to that person becoming radicalised at some time, as the potential recruit may seek out commonality and comradeship, which may be provided by a terrorist organization (Ali, 2013; Atran, 2015; Jones, 2015). This ability of terrorist organizations to isolate and then connect with vulnerable recruits with offerings of commonality and comradeship would be greatly reduced if social media was just not available. What this means is that social media platforms have provided a communications advantage that is being expertly exploited by terrorist organizations to radicalise potential terrorists. The radicalization of potential terrorists over great distances, as is possible through social media provides two further benefits. Firstly, social media is a means used to inspire radicals to travel to terrorist group bases, as well as cultivating what have been termed ‘home-grown terrorists’ to carry out activities within the terrorist’s home country (Neumann, 2012; Jones, 2015; Ministry of Education and Home Office, United Kingdom, n.d). The ability to deploy ‘home-grown terrorists’ is a distinct advantage to terrorist groups as it requires

minimal action and resources (other than an internet connection and a smart phone) on the part of the group, but supports the spread of terror and fear amongst an audience in an arena that perhaps had not previously been considered a conventional terrorism realm (Grob-Fitzgibbon, 2004; Dubouloz and Wilner, 2015). In fact, within the Unites States Homeland Security Project report, Neumann refers to the weight that should be given to addressing home-grown terrorism in stating:

> "Arguably, the use of the Internet to radicalize and recruit home-grown terrorists is the single-most important and dangerous innovation since the terrorist attacks of September 11, 2001" (Neumann, 2012, pg. 9).

Closely related to home-grown terrorism is the lone wolf terrorist, involving a potential terrorist becoming radicalised through isolated non-interactive exposure to terrorist material (Phillips, 2011; Von Behr, Reding, et al, 2013). Social media advantages relevant to lone wolf terrorism, to a terrorist organization are very similar to the advantage that a terrorist who is radicalised online through interaction with a terrorist organization, being that that both the lone wolf terrorist and organization led online radicalised terrorist have the potential to commit attacks in home countries far from the organizations base (McCauley, Moskalenko and Van Son, 2013; Dubouloz and Wilner, 2015). The advantage of the lone wolf terrorist to a terrorist organization, over the organizationally orientated terrorist is the very minimal effort that is required to expose a vulnerable person to extremism (Edelman, 2015). Essentially, nothing further than uploading an extensive library of terrorist propaganda is required, no ongoing coordination is required and the prospect of indiscriminate attack is likely to spread terror further than coordinated attacks that may be perceived as being more predictable (Edelman, 2015). The benefit to terrorist organizations that can be taken from both category of online-radicalised terrorists is that there is potential for terrorists to be radicalised exclusively within a cyber environment (Sageman, 2008). Furthermore, in the case of lone wolf terrorists, further than providing an accessible library of material, no further action on the part of the organization is required. In this situation, the risk weighed against potential outcome is beneficial to a terrorist organization.

Digital Existence

The cyber-environment also supports terrorist organizational continuance (Torok, 2013). Torok (2013) identifies that terrorist organizations use digital technologies to exist virtually in response to their physical existence being threatened. Arguably, the clearest example of this is the establishment of cyber training groups that have been created in the face of terrorism counter-measures that target physical training centres (Torok, 2013; West, 2014). Rogan (2006) also supports that the internet has provided terrorist organizations with a cyber-place to conduct trainings, although Rogan refers to digital terrorist training supporting conventional training techniques, rather than replacing physical training environments. The description of online training environments that is offered by Rogan (2006) involves posting training manuals and instructions for recruited terrorists. Furthermore, Al Qaeda have referred to their organizations cyber training environments as Al Qaeda University (Rogan, 2006). Ahmad al-Wathiq bi-Llah, an Al Qaeda member, is quoted as describing Al Qaeda University graduates as follows:

> "…graduates of the al-Qaida University are specialists in electronic jihad, media jihad, spiritual and financial jihad, passing through the 'faculties' of both morale and explosive package technology and exploding cars and trucks" (Rogan, 2006. pg. 27).

This means that the internet, provides terrorist organizations with a safe space beyond physical attack, where training material can at worst be removed (Torok, 2013). In this manner, the internet and social media support terrorist organization activity in communication with recruits, as well as supporting ongoing operational purposes through training. In being able to store material and exist in a cyber-space from which they cannot be permanently deleted, terrorist organizations have also realised the benefit of being able to remain operational in the cyber-environment even if the physical environment is threatened. Viewing the internet as a terrorist organization's safe space is also consistent with the assertions of former members right-wing Neo-Nazi groups, who viewed the internet as safe and anonymous (Koehler, 2014). Additional to this strategic benefit of safety beyond detection, is the ability to conceal oneself within the internet, which for logistical reasons is a far easier task than attempting to conceal the physical location of a terrorist organization's base or training camp. Through the use of readily available technology, such as virtual private

networks, encryption, or proxy servers an organization or individual can conceal or misrepresent their location and identity (Ferguson and Huston, 1998; Broadhurst, Grabosky, Alazab and Chon, 2014, Klausen, 2015). The benefit of identity and location misrepresentation capability exceeds the advantage of anonymity, as terrorist organizations or individual can actively avoid detection.

Utilising the internet as a means of training and cultivation of potential terrorists shows the benefit that terrorist organizations have taken from digital technology as being adaptable to a changing environment. In addition to providing a space for learning, teaching and collaboration, the internet also provides a decentralising capability that protects data from deletion, hence this supports the longevity of a terrorist organization (Denning, 2001; Rogan, 2006; Klausen, 2015). The beneficial advantage that decentralising an organization's propaganda library is that it can be hosted from virtually any location and copied any number of times (Denning, 2001; Rogan, 2006; Klausen, 2015). This raises a further dimension to the cyber safe space concept, in that the decentralised nature of the internet as a network protects a terrorist organizations continuing existence if at very least as an extensive digital footprint (Denning, 2001; Rogan, 2006; Neumann, 2012; Koehler, 2014; West, 2014). Klausen (2015) explains this further in noting that previously modelled 'vertical' internet control measures are ineffective when used to combat digitally nimble social media users. This can by characterizing social media as a flat horizontal environment that can be edited, republished, contributed to by multiple users from virtually any location that has an internet connection (Klausen, 2015). The dilemma in this is that adaptive entity that is a social media presence cannot easily be deleted, as it is not central and singular, in fact it can be manipulated from virtually anywhere by any number of users. Somewhat converse to this position, Berger and Morgan (2015) do note that the sustained campaign to suspend Islamic State's Twitter presence and known accounts have proved successful, without being terminally destructive to the organization. The success of the Twitter account suspension initiative can be quantified by the known number of daily tweets that are attributed to known Islamic State accounts, which fell from approximately 40,000 daily tweets at the start of the account suspension campaign to under 5,000 daily tweets (Berger and Morgan, 2015). Taking in the learning from both points of view, we arrive at the strategic thinking that efforts to target the social media presence of terrorist organizations should be continued and adapted to a changing social media landscape,

however this cannot be the stand along strategy to combat organizations that is as digitally savvy and nimble as Islamic State or Al Qaeda.

Adaptability

It has been observed that terrorist groups are not passively waiting consumers of third party developed digital advances. Broadly, the evolving nature of digital technology has been more effectively utilized by terrorist organizations than governments, which is evidenced through the ability of these organizations to take advantage of social media and realise the communication potential of the internet (Thomas, 2003; Mackinlay, 2009). Terrorist organizations have been far more effective than states in making social media platforms work for them, in part because terrorist organizations have no need for communication frameworks and ethical constraints, while state actors must work within acceptable parameters (Thomas, 2003; Mackinlay, 2009). Perhaps this ability to be adaptive could be explained as terrorist groups having access to all digital advantage without any restriction, while the innovative potential of state actors is curtailed by required regulatory compliance. The opportunity to evolve digitally and develop cyber strategies that further the interests of a terrorist organization, without consideration of laws or convention is a clear benefit that terrorist organizations have over legitimate cyber entities.

Al Qaeda in the Islamic Maghreb have been somewhat of a Twitter failure, unable to effectively gain ground in building a sustainable social media presence (Torres-Soriano, 2016). However, following failures using Twitter, Al Qaeda in the Islamic Maghreb actively pursued an alternative digital media platform in which material could be uploaded and accessed (Torres-Soriano, 2016). While this does not show the social media adaptability of this organization, it does highlight that there are various alternative platforms that terrorist organizations have access to in order to propagate their material and ideology.

The adaptive digital ability of terrorist groups can be displayed through an Islamic State example (Neumann, 2012; Anti-Defamation League, 2014). The adaptability of Islamic State is customised to a problem, being that Twitter sites associated to the organization have been suspended (Neumann, 2012; Anti-Defamation League, 2014). The digital learning of Islamic State resulted in development of a proxy smartphone application named *Dawn of Glad Tidings*, which allows Islamic State to utilize external Twitter accounts linked to the application to tweet statements, despite their own known Twitter accounts having been

suspended (Anti-Defamation League, 2014; Tadjdeh, 2014). Further, Islamic State have also displayed the ability to push-out their continuing digital presence through such methods of linking onto Twitter tweets through high jacking hashtags as well as maintaining an extensive proxy-server network from which propaganda material can be disseminated (Tadjdeh, 2014). A number of years prior to the report of the Anti-Defamation League (2014) that refers to the creation of the Islamic State Dawn of Glad Tidings application, Neumann (2012) predicted that advantages of smartphones and application development would become a new focus of extremist organizations. This shows that terrorist groups, particularly Islamic State, have become adaptive and exploitative digital users, these groups now possess the ability to use social media platforms as they desire and have the ability to circumvent interventions (Anti-Defamation League, 2014). As Schmidt (2013) also notes any strategy that aims to counter the digital presence of terrorist groups must be aimed at discrediting the propaganda, as the task of removing, blocking or deleting the platforms of propaganda is not an achievable goal. The spirit of Schmidt's (2013) position is that the digital presence of terrorist organizations is beyond deletion and there is far more value in state actors themselves utilising digital advancements to propagate counter-terrorism strategies, rather than simply attempting to curtail its pervasive nature. However, this strategy should be conducted complementarily to a sustained extremist group social media presence suppression initiative, such as the activity that is achieving some gains in suspending Islamic State Twitter accounts (Berger and Morgan, 2015). Additional to the ability to overcome attempts at digital intervention, what this ability also shows is that social media and the propagation of material also preserves the digital existence of terrorist organizations.

There is extensive evidence that digital technology as a means of achieving easy and readily available communication, has been highly advantageous to terrorist organizations. This is true in all facets of communication, including one to one exchanges, creating groups that provide commonality, training, recruitment and many platforms for reaching an audience through propaganda dissemination.

Digital Operation

To this point, this article has focused on social media and the internet broadly as a communication mechanism that served terrorist organisation priorities. Additional to this focus, operational aspects of social media use within terrorist organizations will also be

discussed. Utilizing social media and the internet to achieve operational goals involves two main approaches, being cyber-based attacks intended to directly result in casualty and terror, as well as digital activities that support the organization without the activity being intended to cause direct harm (Denning, 2001; Grob-Fitzgibbon, 2004; Rogan, 2006; West, 2014). A useful explanation of cyber-terrorism is provided by Heickero, who quotes Professor Dorothy Dennings in defining cyber-terrorism as:

> "…illegal, socially or politically determined assault or threat of assault against computers, networks and stored information" (Heickerö, 2014. pg. 554).

Although short, this description of cyber-terrorism is quite useful while examining the role of social media and the internet in terrorism organization operation. In addition to the broad summary of targets that may be vulnerable to cyber-terrorism (Heickero, 2014), it can be inferred that social media may also provide a platform for cyber-terrorism attacks that is open to terrorist organizations. The prominent benefit of operations that targeted at cyber-entities, may simply be the availability of the target (Heickero, 2014). Due to the prevalence of social media in every aspect of daily life, digitally vulnerable targets have been created and presented to terrorist organizations that possess digital operation capability to an extent that these vulnerabilities can be exploited.

Within the use of social media as a means for conducting terrorism, there is also a separation of purposes (Thomas, 2003; Rogan, 2006). Rogan (2006) groups all terrorism related activity together under the term 'Jihadism Online', however draws the distinction between coordination of activity and specific acts of cyber-terrorism that seek to cause casualties. This distinction is significant, as there is difference in intention between utilizing digital means as a coordination tool and propaganda beacon in comparison to utilising the same technologies as a mechanism for causing catastrophic harm (Rogan, 2006; Stohl, 2007). Moving forward towards digital operations, the practice of terrorist organizations cultivating digital operatives, perhaps hackers is acknowledged and the potential for a digital terrorist attack exists, however there is no known evidence that any terrorist group has successfully utilized digital technology with the goal of causing casualties (Stohl, 2007; Henschke, 2014; West, 2014). Hence, the benefit of digital technology to organizational operations may be more of a coordinating nature (Thomas, 2003). Although this digital

susceptibility to digitally capable terrorist organizations is present, The Center for the Study of Terrorism and Irregular Warfare suggests that cyber-attacks are most likely to be deployed to support conventional terrorism activity (Wilson, 2005). The disastrous potential consequences of a destructively intended cyber-terrorist attack are acknowledged, however it is considered more likely that the basis of jihadism online is exploitative rather than destructive (Rogan, 2006; West, 2014). West (2014) suggests in stronger terms that given the technical complexity and financial outlay required to conduct a catastrophic infrastructural cyber-attack, it seems unlikely that a terrorist attack of this kind would be carried out. The potential threat and resultant impact of a successful digitally-based terrorism attack should be acknowledged, however it appears far more likely that coordination of effort and communication amongst members, which is easily achieved through social media, presents a much more usable benefit to terrorist organizations (Thomas, 2003; Rudner, 2016). Thomas (2003) notes that the internet is an outstanding asset for coordination and refers to the ability of insurgent groups to coordinate activities in one target country while remaining in a separate country. The coordination benefits that social media and the internet provide to terrorist groups is extensive, as it allows communication beyond vast distances as well as providing immediate availability of communication (Thomas, 2003; Soo Hoo, Goodman & Greenburg; Rudner, 2016).

However, the benefit of a successfully conducted cyber-terrorism attacks can be quickly understood. The potential resultant chaos could potentially exceed that of a violent terrorist attack, such as a bombing, while there is a greatly reduced risk of exposure and loss of operatives (Thomas, 2003; Soo Hoo, Goodman & Greenburg). Consider the possibility of a cyber-attack that totally compromised the electrical infrastructure of a city. Within current societal settings, in which digital infrastructure is deeply embedded in government and public administration, a total loss of electricity would have potential to cripple healthcare, water supply, financial institutions, domestic living conditions and potentially could impact on every aspect of life (Rogan, 2006; Soo Hoo, Goodman & Greenburg, 2008).

Social media and digital platforms are continuing to evolve, becoming further and further intertwined into institutional infrastructures, which is provides significant benefit to industry and institution, however the open and accessible nature of these digital platforms also provides a digital attack target, as Soo Hoo, Goodman & Greenburg say: "…this new

information infrastructure has become both an asset to defend and an avenue by which other infrastructures may be attacked" (Soo Hoo, Goodman & Greenberg, 2008. pg.1).

While the potential for catastrophic impact of digital infrastructure vulnerability exists, it appears that currently this manner of cyber-attack would require a prohibitively high level of technical expertise and resourcing in order to succeed in a cyber-attack against digital infrastructure (Heickerö, 2014; West, 2014). Stohl (2007) explains the concept of widespread digital attack against a state entity as political threat, rather than being any sustained campaign. However, this is where another benefit lies, the threat and concern that may be caused by the possibility of such a crippling attack meets the end-goal of a terrorist organization, being to spread terror (Grob-Fitzgibbon, 2004; Tabansky, 2011). This is the advantage of social media within digital operations and cyber-terrorism, being that information can be distrusted to audiences efficiently within a platform that encourages interaction between audience and transmitter (Aly, 2016). Thomas (2003) explains this further and notes that the potential disaster resultant from a cyber-terrorism can be the goal of cyber-terrorism, which for instance targets transit vehicles traffic signals to cause collisions, or shutting down power grids. The fear of these potential catastrophic outcomes can be achieved through nothing more than a terrorist group posting or tweeting their intention to carry out a cyber-attack and if social media is exploited effectively terror is likely to spread (Thomas, 2003; Wilson, 2005; Stohl, 2007; Khalil, 2014, Aly, 2016). It is clear that through effective use of social media, terrorist organizations are provided with the platform and ready opportunity to interact with their audience. Social media has become so ingrained and relied upon in many aspects of civilian life, as well as civil infrastructure, to an extent that a previously unavailable arena of attack has been opened.

Additionally, social media presents an information resource to terrorist groups, who may seek to gather intelligence, target individuals, encourage vulnerable persons to participate in action or travel to the caliphate (Denning, 2001; Cukier and Mayer-Schoenberger, 2013; West, 2014; Klausen, 2015). The wealth of information that is social media and the internet has become a valuable data resource that contains extensive professional and personal information including financial interests, medical records, criminal records, personal data, social interests, location, religious beliefs, family linkages et cetera (Denning, 2001; Cukier and Mayer-Schoenberger, 2013; West, 2014; Rudner, 2016). Denning (2001) refers to the internet as a data storage mechanism and states:

> "One way of viewing the Internet is as a vast digital library. The web alone offers several billion pages of information, and much of the information is free" (Denning, 2001. pg. 243).

There is potential for locating almost endless swathes of information on any subject that for example may include whereabouts of individuals, identification information, financial account information of individuals or states, recreational trends of a demographic, or perhaps obtaining transit information for groups of individuals (Denning, 2001; West, 2014). Thomas (2003) also discusses the internet as a resource of information in the context of operational planning. As has been discussed, the internet presents a vast volume of digital property from individuals, organizations and governments (Denning, 2001; West, 2014). There is obvious commercial benefit in collecting sensitive information that may support organizational sustainability, however Thomas (2003) goes further and refers to this information being available as assets to intelligence analysis and operational planning. Information technology, particularly social media have become so imbedded in society that it provides both an access point to and a wealth of information that terrorist organizations may see value in exploiting (Denning, 2001; West, 2014; Rudner, 2016).

Conclusion & Digital Extremism Counter-Measures

It is clear that increased communication capability, through social media and the internet are a far reaching benefit that has revolutionised operating methods of terrorist organizations. Social media benefits also include availability of exploitable data that may support operational planning, intelligence analysis as well as organizational sustainability through financial resourcing. Additionally, social media has provided terrorist organizations with a digital platform from which there is potential for exclusively cyber-based attacks, simply through message dissemination.

Furthermore, cyber space and social media presences have provided a safe space of significant imperviousness to interventions, enabling terrorists to communicate, train and exist beyond the reach of interventions.

It seems that the paramount benefit that social media and internet mechanisms have provided to terrorist organizations is communication, which is easily achieved, cost effective and far reaching.

As has been discussed previously, social media has presented terrorist organizations with many advantages in coordinating operations, reaching potential Jihadis and engaging with their intended audiences. However, these same advantages can be utilized by counter-terrorism and counter-violent extremism actors to achieve gains against these organizations. Firstly, as Berger and Morgan (2015) note, there have been practical efforts to engage with groups such as Islamic State in the social media realm with covert accounts that aim to provide access to intelligence and organizational propaganda. In a more overt manner, narratives that counter the ideology and doctrine of terrorist organisations can be more widely disseminated to the same vast audience that organizations have access to, includes in-organization Jihadis, potential radicals, the wider public audience and communities that are affected by terrorist organization activity (Braddock and Horgan, 2015).

Aly (2016) explains the communication exchange between a transmitter and receiver as being dynamic and interactive. Accordingly, if counter-narrative messages are to be effective in engaging an audience, the interactive and adaptive nature of social media must be the delivery mechanism through which these counter-narratives are delivered. Platforms such as Facebook and Twitter are interactive by design and encourage exchange between audience and transmitter, as well as being dynamic in meeting the needs of a changing target audience.

With minimal effort, social media allow communication between terrorists, with potential recruits and with the public audience. The adaptive ability of terrorist organizations in their use of social media highlights the digital potential to reach audiences, gather information, disseminate messages and coordinate activities. By viewing the social media presence as a tool for collecting intelligence, conducting digital counter-operations and also overtly discrediting terrorist organizations in their own digital space, counter-violent extremism strategists and policy makers may make gains against terrorist organizations. These same communication advantages can be realised by states and non-government agencies, hence counter-violent extremism strategies that integrate digital platforms as communication and outreach advantages are where counter-measures should begin.

Reference List:

Ali, M. (2013, September). The link between unemployment and terrorism [Video file]. Ted Conferences. Retrieved from www.ted.com/talks/mohamed_ali_the_link_between_unemployment_and_terrorism

Aly, A. (2016, 26 February). Brothers, Believers, Brave Mujahideen: Focusing attention on the audience of violent jihadist preachers. Studies in Conflict and Terrorism. Retrieved from http://dx.doi.org/10.1080/1057610X.2016.1157407

Aly, A., Macdonald, S., Jarvis, L. & Chen, T. M. (2016, 7 April) Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization. Studies in Terrorism and Conflict. 2016, VOL. 0, NO. 0, 1–9. Retrieved from http://dx.doi.org/10.1080/1057610X.2016.1157402

Anti-Defamation League. (2014, 11 July). Hashtag Terror: How ISIS Manipulates Social Media. http://www.adl.org/combatinghate/internationalextremismterrorism/c/isisislamicstatesocialmedia.html

Atran, S. (2015, 23 April). The Youth Need Values and Dreams. United Nations General Assembly [Video file]. Retrieved from https://www.youtube.com/watch?v=qlbirlSA-dc

Berger, J.M. & Morgan, J. (2015, March). Defining and describing the population of ISIS supporters on Twitter. The Brookings Project on U.S. Relations with the Islamic World Analysis Paper. Retrieved from http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf

Braddock K. & Horgan, J. (2015, 11 December) Towards a Guide for Constructing and Disseminating Counternarratives to Reduce Support for Terrorism. Studies in Conflict & Terrorism. 2016, Volume 39, Number 5, 381–404. Retrieved from http://dx.doi.org/10.1080/1057610X.2015.1116277

Broadhurst, R., Grabosky, P., Alazab, M. and Chon, S. (2014). Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. International Journal of Cyber Criminology. Volume 8, issue 1, pp. 1 -20. Retrieved from http://search.proquest.com.ezproxy.csu.edu.au/docview/1545341663?rfr_id=info%3Axri%2Fsid%3Aprimo

Coker, C. (2002). Globalisation and Terrorism [Conference Paper]. London School of Economics and Political Science. Retrieved from https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjhloiRp6vKAhVH8A4KHW5hD2QQFggnMAA&url=http%3A%2F%2Fwww.g8.utoronto.ca%2Fconferences%2F2002%2Ftokyo%2Fcocker.pdf&usg=AFQjCNHIdQKbY0XILj7iET-a7J4mXtYHgw&cad=rja

Conway, M. (2005, 8-10 September). Terrorism 'Use' and the Internet Fighting Back. Conference Paper: Cybersafety: Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities. Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwj8yczw1cLNAhUMMY8KHfGFAzAQFggeMAA&url=http%3A%2F%2Fwww.oii.ox.ac.uk%2Fresearch%2Fcybersafety%2Fextensions%2Fpdfs%2Fpapers%2Fmaura_conway.pdf&usg=AFQjCNGsB3-g-clxKhAdsL0Y3qHmCRdCeg

Conway, M. (2016, 12 April). Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research. Studies in Conflict & Terrorism. 1521-0731. Retrieved from http://dx.doi.org/10.1080/1057610X.2016.1157408

Cukier, K. and Mayer-Schoenberger, V. (2013, May/June). The Rise of Big Data. Foreign Affairs. Volume 92, issue 3. http://search.proquest.com.ezproxy.csu.edu.au/docview/1335008763?OpenUrlRefId=info:xri/sid:primo&accountid=10344

Denning, D. E. (2001). Activism, Hacktivism, and Cyberterrorism: The internet as a tool for influencing foreign policy, chapter 8 in Arquilla and Ronfeldt (ed.), Networks and Netwars: The Future of Terror, Crime and Militancy, pp. 239-288. Rand Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf

Dubouloz, C. & Wilner, A. (2010, February). Home grown terrorism and transformative learning: an interdisciplinary approach to understanding radicalization. Global Change Peace and Security. Retrieved from http://www.researchgate.net/publication/228624027_Homegrown_terrorism_and_transformative_learning_an_interdisciplinary_approach_to_understanding_radicalization

Edelman, A. (2015, 10 May). Lone-wolf terrorists could attack U.S. 'at any moment,' Homeland Security chief admits. New York Daily News. Retrieved from http://www.nydailynews.com/news/politics/lone-wolf-terrorists-attack-moment-dhs-chief-article-1.2217118

Eriksson, J. and Giacomello, G. (2006, July). The Information Revolution, Security, and International Relations: (IR) Relevant Theory? International Political Science Review, volume 27, number 3, pp. 221 – 244. Sage Publications Limited. Retrieved from http://ips.sagepub.com.ezproxy.csu.edu.au/content/27/3/221

Ferguson, P. and Huston, G. (1998, June). What Is a VPN? Part I. The Internet Protocol Journal, volume 1, number 1. Cisco Systems. Retrieved from http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_11/what_is_a_vpn.html

Grob-Fitzgibbon, B. (2010, 10 August). From the dagger to the bomb: Karl Heinzen and the evolution of political terror. Terrorism and Political Violence. Volume 16, number 1, pp. 97 – 115. United Kingdom: Routledge Taylor and Francis Group. Retrieved from http://www-tandfonline-com.ezproxy.csu.edu.au/doi/abs/10.1080/09546550490446036

Harrison, W. B. [Jnr] (2002, 7 March). Closing The Digital Divide. Global Information. Vital Speeches of the Day. Volume 68, issue 19, pp. 606 – 608. Retrieved from http://connection.ebscohost.com/c/speeches/6995469/closing-digital-divide

Heickerö, R. (2014, 28 July). Cyber Terrorism: Electronic Jihad. Strategic Analysis, volume 38, number 4, pp. 554 – 565. United Kingdom: Routledge Taylor and Francis Group. Retrieved from http://www-tandfonline-com.ezproxy.csu.edu.au/doi/abs/10.1080/09700161.2014.918435

Henschke, A. (2014, June). A decision-making procedure for responding to cyber-attacks. Occasional Paper, number 6, pp. 3 - 9. National Security College. Crawford School of Public Policy. Australian National University. Retrieved from http://nsc.anu.edu.au/documents/ocassional-paper-6-cyber-ethics.pdf

House of Commons, United Kingdom. (2012, 6 February). Roots of Violent Radicalization. Nineteenth Report of Session 2010–12. Reference: HC 1446. House of Commons Home Affairs Committee. Retrieved from http://www.publications.parliament.uk/pa/cm201012/cmselect/cmhaff/1446/1446.pdf

Jones, C. (2015, 17 March). Jake Bilardi's story shows why terrorist intervention must be tailored. The Conversation. Retrieved from https://theconversation.com/jake-bilardis-story-shows-why-terrorist-intervention-must-be-tailored-38769

Khalil, E. (2014, 1 October). Gone viral - Islamic State's evolving media strategy. Jane's Intelligence Review. IHS Global Limited. Retrieved from http://search.proquest.com.ezproxy.csu.edu.au/docview/1609437740?rfr_id=info%3Axri%2Fsid%3Aprimo

Klausen, J. (2015). Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq. Studies in Conflict & Terrorism, 38:1, 1-22. Retrieved from http://dx.doi.org/10.1080/1057610X.2014.974948

Koehler, D. (2014). The Radical Online: Individual Radicalization Processes and the Role of the Internet. Journal for Deradicalization. Winter, 2014/2015, number 1, pp. 116 – 134. Retrieved from http://journals.sfu.ca/jd/index.php/jd/article/view/8/8

Labi, N. (2006, July/August). Jihad 2.0: With the loss of training camps in Afghanistan, terrorists have turned to the Internet to find and train recruits. The story of one pioneer of this effort—the enigmatic "Irhabi 007"—shows how. The Atlantic. Retrieved from http://search.proquest.com.ezproxy.csu.edu.au/docview/223088747?OpenUrlRefId=info:xri/sid:primo&accountid=10344

Mackinlay, J. (2009). The Virtual Battlefield. In The Insurgent Archipelago: From Mao to Bin Laden (pp. 123-142). United Kingdom: Hurst and Company. Retrieved from https://doms.csu.edu.au/csu/file/57260df0-83fe-4a03-a0c9-7a8c3fbc8973/1/mackinlay-j.pdf

McCauley, C., Moskalenko, S. and Van Son, B. (2013). Characteristics of Lone Wolf Violent Offenders: A Comparison of Assassins and School Attackers. Perspectives on Terrorism. Terrorism Research Initiative. Volume 7, number 1. Retrieved from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/240/pdf

McMillan, R. (2016, 5 April). Facebook's WhatsApp Launches 'End-to-End' Encryption. WhatsApp texting service strengthens encryption so only sender and receiver can read message contents. Retrieved from http://www.wsj.com/articles/facebooks-whatsapp-turns-on-encryption-by-default-1459869097

Ministry of Education and Home Office, United Kingdom. (n.d). How social media is used to encourage travel to Syria and Iraq: Bringing note for schools. Retrieved from

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/440450/How_social_media_is_used_to_encourage_travel_to_Syria_and_Iraq.pdf

Mishra, S. (2003, 5 September). Exploitation of information and communication technology by terrorist organizations. Strategic Analysis, volume 27, number 3. Institute for Defence Studies and Analyses. United Kingdom: Routledge Taylor and Francis Group. Retrieved from http://www-tandfonline-com.ezproxy.csu.edu.au/doi/abs/10.1080/09700160308450099

Mohamedou, M-M. O. (2015, 18 June). The Islamic State, Al-Qaeda, and Postmodern Globalized Violence [Video file]. The Fletcher School, Fares Centre for Eastern Mediterranean Studies. Retrieved from https://www.youtube.com/watch?v=kFFfKJydBfs

Neumann, P. (2012, December). Countering Online Radicalization in America. National Security Program, Homeland Security Project. Bipartisan Policy Center. Retrieved from http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/BPC%20_Online%20Radicalization%20Report.pdf

Phillips, P. J. (2011). Lone Wolf Terrorism. Peace Economics, Peace Science and Public Policy. Volume 17, issue 1, article 1. Berkeley Electronic Press. Retrieved from http://web.a.ebscohost.com.ezproxy.csu.edu.au/ehost/detail/detail?sid=a5c0a290-fc3d-48d7-b99d-fa3ef0c900cc%40sessionmgr4002&vid=0&hid=4101&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=60199449&db=tsh

Pretch, T. (2007, December). Home grown terrorism and Islamist radicalization in Europe. From Conversion to Terrorism. An assessment of the factors influencing violent Islamist extremism and suggestions for counter radicalization measures. Denmark: Danish Ministry of Justice. Retrieved from http://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/2011/2007/Home_grown_terrorism_and_Islamist_radicalization_in_Europe_-_an_assessment_of_influencing_factors2.pdf

Rogan, H. (2006, 20 March). Jihadism Online - A study of how al-Qaida and radical Islamist groups use the Internet for terrorist purposes, 2006/00915. Norwegian Defence Research Establishment. Retrieved from http://rapporter.ffi.no/rapporter/2006/00915.pdf

Rudner, M. (2016, 30 March). "Electronic Jihad": The Internet as Al Qaeda's Catalyst for Global Terror. Study in Conflict and Terrorism, Volume 0, Number. 0, 1–14. Retrieved from http://dx.doi.org/10.1080/1057610X.2016.1157403

Sageman, M. (2008). Leaderless Jihad: Terror networks in the twenty first century. Philadelphia, United States of America: University of Pennsylvania Press.

Schmid, A. P. (2013, March). Radicalization, De-Radicalization, Counter-Radicalization: A Conceptual Discussion and Literature Review. International Centre for Counter-Terrorism. Retrieved from http://www.icct.nl/download/file/ICCT-Schmid-Radicalization-De-Radicalization-Counter-Radicalization-March-2013.pdf

Simon, T., Goldberg, A., Aharonson-Daniel, L., Leykin, D. and Adini, B. (2014, August). Twitter in the Cross Fire—The Use of Social Media in the Westgate Mall Terror Attack in Kenya. Plos One, volume 9, issue 8, reference e104136. Retrieved from http://search.proquest.com.ezproxy.csu.edu.au/docview/1556010857?rfr_id=info%3Axri%2Fsid%3Aprimo

Soo Hoo, K., Goodman, S. & Greenberg, L. (2008, 3 March). Information technology and the terrorist threat. Survival, vol. 39, no. 3, Autumn 1997, pp. 135-55. Retrieved from http://dx.doi.org/10.1080/00396339708442930

Stevens, T. and Neumann, P.R. (2009, 28 January). Countering Online Radicalization: A Strategy for Action. London, United Kingdom: The International Centre for the Study of Radicalization and Political Violence. Retrieved from https://cst.org.uk/docs/countering_online_radicalization1.pdf

Stohl, M. (2007, 30 March). Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games? Crime Law Social Change. Cyber Terrorism. Volume 46, pp. 223 – 238. Springer Science + Business Media. Retrieved from http://link.springer.com.ezproxy.csu.edu.au/article/10.1007/s10611-007-9061-9

Tabansky, L. (2011, November). Critical Infrastructure Protection against Cyber Threats. Military and Strategic Affairs. Volume 3, number 2, pp. 61 – 78. Retrieved from http://www.inss.org.il/uploadimages/Import/%28FILE%291326273687.pdf

Tadjdeh, Y. (2014, December). Government, Industry Countering Islamic State's Social Media Campaign (Updated). National Defence. Retrieved from http://www.nationaldefensemagazine.org/archive/2014/December/Pages/GovernmentIndustryCounteringIslamicStatesSocialMediaCampaign.aspx

Tehrani, P. M., Manap, N. A. and Taji, H. (2013). Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime. Computer Law and Security Review, volume 29, pp. 207 – 215. Faculty of Law, The National University of Malaysia. Malaysia: Elsevier Limited. Retrieved from http://www.sciencedirect.com.ezproxy.csu.edu.au/science/article/pii/S0267364913000666

The Clarion Project. (2014, 10 September). The Islamic State's (ISIS, ISIL) Magazine: All of the issues of the Islamic State's glossy propaganda magazine 'Dabiq,' named after a key site in Muslim apocalypse mythology can be found here. Retrieved from http://www.clarionproject.org/news/islamic-state-isis-isil-propaganda-magazine-dabiq

Thomas, T. L. (2003). Al Qaeda and the Internet: The danger of "cyberplanning". Parameters.Volume 33, number 1. ProQuest. Central. Retrieved from http://search.proquest.com.ezproxy.csu.edu.au/docview/198039860?OpenUrlRefId=info:xri/sid:primo&accountid=10344

Torok, R. (2013). Developing an explanatory model for the process of online radicalization and terrorism. Security Infomatics, a Springer Open Journal, volume 2, number 6. Security Research Institute, Edith Cowan University. Perth, Australia: Torok; licensee Springer. Retrieved from http://www.security-informatics.com/content/2/1/6

Torres-Soriano, M.R. (2016, 27 April). The Caliphate Is Not a Tweet Away: The Social Media Experience of Al Qaeda in the Islamic Maghreb. Studies in Conflict & Terrorism. DOI: 10.1080/1057610X.2016.1159430. Retrieved from http://dx.doi.org/10.1080/1057610X.2016.1159430

Von Behr, I., Reding, A., Edwards, C. and Gribbon, L. (2013). Radicalization in the digital era: The use of the internet in 15 case studies of terrorism and extremism. Brussels, Belgium: RAND Europe. Retrieved from http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf

Weimann, G. (2006). New terrorism, new media. In Terror on the internet: the new arena, the new challenges. (pp. 15-31). Washington, DC: United States Institute of Peace Press. Retrieved from https://doms.csu.edu.au/csu/file/1eba375e-679b-43bf-b60a-d75d35983420/1/weimann-g.pdf

West, L. J. (2014, June). Virtual terrorism: Data as a target. Cybersecurity: Mapping the ethical terrain. Occasional Paper, number 6, pp. 28 - 33. National Security College. Crawford School of Public Policy. Australian National University. Retrieved from http://nsc.anu.edu.au/documents/ocassional-paper-6-cyber-ethics.pdf

Wilson, C. (2005, 1 April). Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. CRS Report for Congress. Congressional Research Service - The Library of Congress. Retrieved from http://handle.dtic.mil/100.2/ADA444799