International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

Online Radicalization: An Overview

Mohammad Zahid Mateen, Jamaludin Ibrahim

Kulliyah of Information and Communication Technology, International Islamic University Malaysia, Kuala Lumpur, Malaysia

Abstract: ***The Internet is a medium where the entire world exists in the form of 1's and 0's. This world as we know it today is constantly in a dynamic state of war with those who want to use technology to misuse and exploit it for spreading their propaganda and worldview among the masses. This paper looks into cyber-warfare, cyber-terrorism and its rise, and at the same time it also focuses on the "Islamic" State which is conducting a modern and sophisticated cyberwar online. The paper also discusses as to what exactly constitutes online radicalization and what leads to this. The rise of whistle-blowers and organizations like WikiLeaks has caused damages in the millions to people and even governments. This paper aims to investigate as to where do we draw the line between organizations like WikiLeaks and ISIS in terms of cyber-terrorism.***

Keywords: Cyber Terrorism; Targeted attacks, Cyber Security, Online Radicalization, ISIS, WikiLeaks, Data Breach, Cyber-War

1. Introduction

Moore's law states that the number of transistors in a dense integrated circuit doubles about every two years. The number of interconnected electronic devices is outnumbering living humans. The next leap is coming in the form of the Internet of Things. This connectivity of the world has proven to be a bane as well as boon based on who and for what it is being used. One of the primary focus of the Information Age is the phenomenon of connectivity.

This connectivity has opened up the floodgates of information and data which was previously impossible to attain in a single lifetime for any given person. The Internet has become an integral part of our lives and critical to the functioning of modern society. But this dependence clearly has downsides that extremists and terrorists have learned to exploit. This has placed the tools in the hands of cyber terrorists to enhance their methodology, techniques and attack in such a manner remotely, causing heavy damages to their intended targets. Along with the presence of an ocean of data, the Internet also provides the cover of anonymity. This provides like-minded individuals, vigilante groups and other organizations to pursue illegal activity and spread their propaganda creating a whole new body of criminal threats. Such online terrorists also known in technical terms as cyber-terrorists are boosted by the lowered threat of immediate capture due to the vast expanse between them and their target of attack coupled with the inherent complexity of tracing the attack back to them.

A plethora of data today which includes private, national level, and critical military intelligence data can be vulnerable to cyber-attacks. A major cause of this is the usage of outdated and textbook security features instead of a more stronger, validated and sophisticated cyber protection program.

This paper aims to discuss and analyse cybercrimes, cyber terrorism and cyber warfare as relevant topics in the cyber security world. When it comes to data, and compromising high level information there seems to be hardly any difference between organizations like ISIS, Anonymous and even WikiLeaks even though the latter is a lot more civilized as compared to the former two organizations. What seems to be the major difference is the way they are portrayed to the public in and by the media. This portrayal has helped these organizations to garner support and followers even though it has brought them their fair share of haters as well.

Terrorist groups across the ideological spectrum are now turning to the Internet to take the war into the cyber-world. They use it to recruit new members, to disseminate their propaganda, and to securely communicate with each other. Their activities represent a threat to both on- and off-line communities.

2. Literature Review

Despite the inherent advantages, the dependence on information technology has left nations and society much more vulnerable to cyber-attacks such as computer intrusions, scrambling software programs, undetected insider threats within the network firewalls, or cyber terrorists.

Modern terrorism is continuously transforming. It is like the infamous Hydra, where if you cut one head off, and another two generate to take its place. Such transformations and changes include not only organizational changes, but also new operational strategies and plans searching for ways to increase the effectiveness and destruction caused because of terrorist attacks.

Everyday Influences

Perešin notes that through the methods terrorist organizations misuse and misdirect media avenues, it can be seen that there is an alarmingly high potential of children becoming victims of radical fundamentalist ideologies. [1] We live in a world today which is very visual in nature. Children respond a lot to visual stimulus and emotionally charged words. Even though children are used more often for conducting the terrorist attacks, this paper touches on how the misuse of media for indoctrination of children from their earliest age becomes a part of the new carefully planned educational strategy for the creation of the "children in the martyrdom culture", with the aim of their ideological preparation for conducting terrorist attacks in the future.

The Internet as we know of its structure today, offers terrorists and violent extremists the same opportunity and

capability that it does to anyone else across the globe as long they have an Internet connection: to communicate, collaborate and convince (Von Behr et al, 2013). There is already an uncontrollable flood of radical content available online just a click away. What is alarming to note is that this volume is growing daily. The growth of the use of the Internet, with its ability to reach wide community, including children, to connect people and to make easier the dissemination of materials, has had a significant impact on the accessibility and flow of radical ideas.

Now the main question that arises is, what exactly is radicalization? The paper defines radicalisation as the process by which a person comes to support terrorism and forms of extremism leading to terrorism, whilst online radicalisation is a process whereby individuals through their online interactions and exposures to various types of Internet context, come to view violence as a legitimate method of solving social and political conflicts. (Birmingham, 2009). According to Sageman (2008), the role of the Internet is crucial for the evolution of modern terrorism. Internet enables terrorists to initiate and coordinate global activities.
The paper also elaborates that the term "leaderless jihad" come out of the term "leaderless resistance", which was introduced by Louis Beam in 1983 as a substitute for traditional hierarchical organizational structure. This was considered as untenable under contemporary conditions.

Offline and Online Wars

R. Martins expounds that warfare in the physical world, both asymmetrical and conventional, has occurred throughout history. However, a new avenue is emerging. Wars in cyberspace are a very recent phenomenon, and there is still much to be explored and understood from all sides and levels. Many official government agencies and security related organizations are having trouble moving from on the ground war tactic mindset to online war tactics. [2]

The paper further notes that since cyberspace is inherently asymmetric in nature, a lot more lessons learned from asymmetric warfare in the physical world also apply to a large extent to cyber conflicts. This paper analyses the online battle being led by Anonymous against ISIS and touches on the five asymmetrical characteristics of cyber conflicts which include:

1) The vulnerability of conventionally-powerful actors to attacks from relatively weaker adversaries
2) The unconventional nature of offensive tactics
3) The low level of intensity of those tactics
4) The ability of actors to organize and aggressively operate in an extremely decentralized manner
5) The strategic goal of breaking willpower or forcing a change of policy.

In early 2015, the world as a whole witnessed for the first time a public declaration of war by a non-state actor, the collective, Anonymous who work specifically in cyberspace as they openly challenged the (Non) Islamic State and their online resources and operations across the Web.

From a historic perspective, Anonymous' has been known to famously and repetitively target the "big three" which include big businesses, big governments, and big religious organizations. The most common online tactics of Anonymous include website defacements, distributed denial-of-service (DDoS) attacks, unauthorized access of accounts, and data exfiltration just to name a few. DDoS attacks are of the most important part of the Anonymous arsenal. Anonymous has been noted to influence public opinion and government policies by highlighting and dragging media attention on its chosen issues through the use of cyberattacks.
Moving to (N)ISIS, Baghdadi who is supposed to be the alleged leader, leads an organization that in the opinion of one expert, "has exploited these technologies more successfully than any of its contemporaries in the Islamist world."

Through their online operations, (N)ISIS operatives run a plethora of actions including:

- Recruit members
- Issue operational instructions
- Spread their extreme and distorted version of Islam's propaganda
- Provoke fear in an attempt to change the behavior and policy of their targets.

A.Shehabat and T. Mitew examines three anonymous content sharing portals [3] put into effect strategically by the (Non) Islamic State of Iraq and Sham to achieve its radically charged political ends. Their paper argues that anonymous sharing portals such as Sendvid.com, Justpast.it, and Dump.to have had a major role to play in allowing stand-alone radicals to generate content, spread their propaganda and communicate freely while routing around filtering practiced by popular social media networks. This paper draws on the Actor Network Theory (ANT) to examine the relationship between (N)ISIS radicals and the emergence of anonymous sharing platforms. The paper suggests that, even though used prior to the massive degrading operation across social media, anonymous sharing portals have played a major role in allowing (N)ISIS to maintain its networking structure in the face of planned operations against them by various governmental agencies and organization.

Virtually all users on these platforms fall in one of three often overlapping roles:

- They either dynamically produce and aggregate content
- Act as intermediaries retranslating and curating content across multiple platforms
- Passively consume the information flowing across the network.

The last category seems to be the largest category. (N)ISIS appeared to quickly recognize the importance of digital communication tools in its self-proclaimed goal to establish a global Caliphate. Images of their destruction, savagery and barbaric acts were broadcasted virally through social media networks and global media, which were clearly intended to frighten enemies and lead to further gains on the ground in both Syria and Iraq. Social media heavyweights and giants like Twitter, YouTube and Justpaste were employed extensively by (N)ISIS to conduct their information driven operations, for the purpose of producing and disseminating propaganda videos for potential recruits and spread its radical views among Muslim youth globally.

Social media platforms have played a magnanimous role in becoming a source of aiding terror organizations. Former Google CEO Eric Schmitt pointed out that ISIS and its supporters are "producing as many as 90,000 tweets and other social media responses every day".[4] The importance of utilizing media by terror networks was highlighted by Philip Sieb and Dana Janbek, who argued that media are the oxygen of terrorism.[5] Furthermore, Abdel Bari Atwan argues that the internet helped ISIS to achieve its recruiting objectives and territorial ambitions in short time.[6] That is, digital communication tools "allow terrorist groups to become regional or even global players […] [they] also allow terrorists to work more effectively […] to protect communications".

Part of the less overt efforts at suppressing jihadist propaganda online, the hacktivist group Anonymous declared 'Operation ISIS'. Andrew Griffin suggests that this operation concentrated its efforts on searching and neutralising ISIS online content on both social media platforms and websites using Distributed Denial of Service (DDOS) attacks.

Berger and Strathearn indicated that when it comes to freedom of speech, social media platforms are biased. They suggest that these platforms should make it clear that freedom of speech is limited when it comes to using their service.[7]

M.C. Libicki states that cyber-crises are not really an inevitable feature of the cyberworld. Because it is nearly impossible to disarm cyber-attackers, and because cyber-defence is rarely utilized to its full potential. In reality many of the agencies involved don't even know the capacity of the attackers or what their systems can handle in case of an attack. [8]

The paper notes an interesting point which states that in the nuclear era, the threat was from the delicate balance of fear, while, in cyberspace, doubt, uncertainty, and the resulting confusion are more rampant and obvious. This heightens the prospects of a cyber-war among quarrelling states whenever anger flares and rash decisions are made.

The paper builds on that crises have before and during phases. Many of the same principles that work to moderate or manage politico-military crises beforehand apply to cyber-crises as well. These include:

- Do not present an easy and lucrative target for the attackers.
- Foster at least a hint of intimidation for those that do not mean well.
- Look for norms that help in distinguishing aggression that warrants a response from behaviour that does not. [9]

The principles do apply differently to a large extent in cyberspace, of course, a medium in which doubt and uncertainty play much the same role that fear played in the nuclear crises during the World Wars. A state's attempts to demonstrate its ability to defend and attack are not so easy. But the basics are more or not the same.

Terrorism 3.0

O.Sultan takes into account a lot of the historical aspect and rise of al-Qaeda in the world followed by how (N)ISIS has stepped up their game by building on al-Qaeda's mistakes and are spreading terrorism at a higher rate globally. Many of the militant and insurgent organizations that would traditionally stay relegated to regional conflicts became connected through the Internet and social web starting in the mid-2000s. [9]

Al-Qaeda began moving towards new radicalization methods in the mid-00s. While initially in Arabic, by 2015 al-Qaeda was publishing an English Magazine called Inspire. Inspire shifted "from al-Qaeda recruitment, travel and training to syndication of Anarchist's Cookbook-style terror tools with Turner Diaries-style rhetoric in a magazine that has the publication quality of Vogue magazine." Al-Qaeda keeping in mind the rest of the world also published regional publications for the Indian Subcontinent (AQIS), as well as other global regions.

Key findings of this paper include:

- The World of War, Social Media and Cyber have intersected.
- Religion has little or no bearing on the likelihood that a marginalized Millennial or Gen Z'er will be radicalized.
- The majority transition from secular to radical. The people in this group do not attend local mosques or even talk to community leaders or neighbors or even the people from their home country. They sit in the dark, learning, and practicing online until they are ready to act. The majority of the radicalized people are off-the-radar for years.
- Even someone who does not find the courage to go out and launch an attack helps by producing propaganda videos and distributing the planning material online.

J. Prier demonstrates how social media is a tool for modern information-age warfare. It builds on analysis of three distinct topics:
1.Social Networking
2.Propaganda and News
3.Information Sharing.

Two case studies were used to show how state and nonstate actors are using social media to implement time-tested propaganda techniques to yield wide ranging and reaching results. [10]

The propaganda message is amplified by hijacking an existing narrative and tricking the medium's algorithm with the usage of bots to push the message.

The first case study analyses Islamic State (IS) as a nonstate actor, while the second case observes Russia as a state actor, with each providing evidence of successful influence operations using social media. Coercion and persuasion will continue to be decisive factors in information warfare as more countries attempt to build influence operations on social media.

The paper highlights the facts that the credibility of the media has been put into question by social media backed campaigns. As technology is enhancing as this sentence is

being read, it can be said that, "He who controls the trend will control the narrative, and ultimately, the narrative controls the will of the people."

The Story of Pakistan and Terrorism

Taking Pakistan as an example, we see that cyber technology plays a major role in the promoting and sharing online radical ideas in Pakistan. Online radicalization can be seen as a common factor in nearly all visible trends and pattern of sectarianism in Pakistan. [11]

The changing aspects of such trends are different in conventional radicalization but same as in online radicalization in Pakistan. Cyber terrorism has become the face of terrorism at an alarming pace which is a security nightmare and makes affairs more complex to address.

According to a report of MacAfee till the end of September 2013 there were 170 million malwares in the digital world which are causing daily hacking attacks on computers. USA president Barrack Obama has also declared that cyber terrorism is the biggest threat to USA security and they need to hire "Cyber Warriors" to tackle and counter these threats.

In the years that have followed since 9/11, Pakistan has shown an increased vulnerability to radicalization. The growth of religious radicalization in Pakistan is particularly evident in the rising number of sectarian clashes. From January 2012 to June 2013, there were 203 incidents of sectarian violence in which 717 people, including 635 members of the Shia community, were killed and 1,800 were injured.

The scope of de-radicalization programs in Pakistan is often limited, with programs usually confined to individuals in post-conflict scenarios. Many programs also fail to include preventive and pre-emptive components of de-radicalization as part of their overall strategy. Data collected during De-Radicalisation and Emancipation Programs (DREP), however, reveal that most of young militants who were trained to carry out suicide bombings came from mainstream schools. [12]

Family engagement is a very important aspect that has been neglected and to a large extent ignored in most de-radicalization programs in Pakistan. Data collected by the Sabaoon program on young suicide bombers reveals cases in which families gave up their children to militant groups for monetary compensation of approximately US$90. The Saudi program is a model that can be considered here. It involved detainees' families in the de-radicalization process by introducing a measure of accountability should the de-radicalization program.

Rise of Online Radical Propaganda

The Internet is a transformative technology that terrorists are exploiting for the spread of propaganda and radicalizing new recruits. While Al Qaeda has a longer history, (Non) Islamic State is conducting a modern and sophisticated media campaign centred around online social networking.

"According to some of the more hysterical reports, more British citizens joined IS in Iraq and Syria than enlisted in the U.K. Army Reserve in 2013 (several hundred compared to 170). Facebook alone counts close to 1.5 billion active users, almost 20 percent of the world population. Unsurprisingly, the Internet has been embraced by terrorists for the same reasons as it has by other organizations, including its capacity to expand reach and influence.7 If terrorism is understood as a form of communicative violence, and spreading propaganda and attracting attention are therefore central to it, then an online presence is logically even more vital to terrorists than it is many other organizations. Terrorists can connect directly with various audiences, and those audiences, in turn, can become active participants in an unfolding conversation. A sense of virtual community can therefore be fostered, which is often not possible with more traditional forms of broadcast media like radio and television." [13]

Th head of Al Qaeda and former deputy to the infamous Osama bin Laden, Ayman al-Zawahiri famously said, "We [Al Qaeda] are in a battle, and more than half of this battle is taking place in the battlefield of the media. And that we are in a media battle in a race for the hearts and minds of our people."

Most media outlets and journalists which have not jumped on the TRP bandwagon have declined to share the graphic video or photos, but (N)ISIS was aware that social media was an easy way to bypass the checks used by media organizations to stop the spread of propaganda.

(N)ISIS has been publishing annual reports on its progress complete with high quality illustrations and infographics like a top level MNC. In addition to leveraging on their Twitter outreach, other accounts broadcast live feeds about local (N)ISIS operations. Many of their online supporters and fans retweet its hashtags and translates messages from Arabic to Western languages. Everything done in IS's propaganda strategy has a combined effect to "building the brand."

Who Is At Risk?

A security dilemma is said to exist when one country cannot make itself more secure without making another less secure. The greater the percentage of ill-secured machines connected to the Internet, the greater the potential rewards for cyber-criminals. The more secure an infrastructure is, particularly against data theft, the more people can engage in electronic commerce without undue worry—and that also benefits all. The cybersecurity dilemma fades further when countries start depending on the same infrastructure for their cybersecurity. In one sense they already do: commercial software is a global commodity, and cybersecurity firms take customers from anywhere. Vulnerabilities for one are vulnerabilities for all; patches for one are patches for all. If and as cloud computing spreads, various countries may find themselves dependent on the security of the same providers. [14]

Radicalization and De-Radicalization

O. Ashour outlines a broad strategy for countering the narratives of violent extremists. [15] His paper argues that an effective counter-narrative should be built on three pillars. The first is an effective comprehensive message that dismantles and counter-argues against every dimension of the extremist narrative, namely the theological, political, historical, instrumental and sociopsychological dimensions.

The second pillar is the messengers. The article argues that for the first time in the history of Jihadism a "critical mass" of former militants, who rebelled not only against the current behaviour of their former colleagues but also against the ideology supporting it, has come into existence. This "critical mass" can constitute the core of credible messengers, especially the few de-radicalized individuals and groups that still maintain influence and respect among vulnerable communities. The third pillar is the dissemination and attraction strategy of the counter-narratives(s) which focuses on the role of the media.

With the rise of violent incidents related to online radicalization, outlining a global action plan for producing counter-narratives and promoting online de-radicalization becomes an essential task. In-depth research on counter-narratives, covering its multiple dimensions, constitutes an excellent foundation for guiding an action plan. The research on counter-narratives should build on previous findings, specifically in the area of ideological de-radicalization. Lessons learned from online and other interaction models (e.g. in Egypt, Saudi Arabia, Algeria, Yemen, United Kingdom and Netherlands) should be analyzed to guide and inform the process of constructing persuasive counter-narratives. Finally, enhancing international cooperation and exchange of experiences will be crucial for the success of any action plan or building process.

C. Archetti aims to demonstrate that a greater understanding of communication in the 21st century is essential to more effective counterterrorism. In fact, while "strategic communication" and "narratives" are advocated by many analysts as essential weapons in countering extremism, few seem to truly understand the reality of the digital-age information environment where such tools need to be deployed. To contribute to bridging this gap, the article outlines some problematic misunderstandings of the contemporary information environment, provides an alternative communication-based framework to explain radicalization, and draws some counterintuitive lessons for tackling terrorism. [16]

The main shortcoming of strategic communication approaches to countering terrorism lies in assuming that the information space in the digital age is far simpler and more linear than it actually is. The not unjustified, but certainly disproportionate, focus on the Internet prevents us from seeing the wider social–and never online-only–space in which extremism is rooted. In this respect, rather than focusing on the technology alone, it is more helpful to look at the convergence of different platforms, both "new" and "old" media, and at how they are used by political actors (terrorists, citizens, NGOs, governments and others) for advancing their own agendas.

Narratives, however, are much more than rhetorical devices. Far from being "just stories," they have deep roots: they are socially constructed. As identities exist at both individual and collective levels, so do narratives. In this perspective, according to Alberto Melucci, social movements (and also terrorist groups) 'offer individuals the collective possibility of affirming themselves as actors and of finding an equilibrium between self-recognition and heterorecognition'. Ultimately, although communication is crucial, it is important to understand that the message is not all. "We" can communicate as effectively as we like, but the consistency between words and deeds is of paramount importance.

To sum up: it is not possible to predict acts of terrorism; there is no simple formula that can tell when and where terrorism will arise. There are also no messages, however perfectly crafted, that can, by themselves alone, neutralise violent extremism. However, in each single local context, through community-based approaches and long-term engagement, it is possible to gain an insight into the local narratives and the networks such narratives arise from. Therefore we have to ask: What is the identity of the local community? How do its members see themselves? Who are the "relevant others" of that community? The establishment over time of radical and extremist identities through ideas and discourses can be detected. By being part of a community, it is also possible to engage with the non-radical networks that are around an extremist core. Such a community-based approach and close attention to the consistency between our narrative (words) and our policies (deeds) are in the end the most effective tools against extremism.

Is Social Media Completely to Blame?

Social media differs from traditional and conventional media in many aspects, such as in interactivity, reach, frequency, usability, immediacy, and permanence. G. Weimann notes that unlike traditional media-characterized as "one-to-many," in which only a small cohort of established institutions disseminates information to an effectively limitless audience-social media enables anyone to publish or access information and to do so in an interactive, two-way exchange. [17]

This two way communication promotes creation of small, diffused sets of communicators and groups. Virtual communities using social media are increasingly popular all over the world, especially among younger demographics. The new social media have technical advantages for terrorists: sharing, uploading, or downloading files and videos no longer requires fast computers, or any computers for that matter; it no longer requires sharing sites or savvy members capable of uploading such videos. Rather, smart phones and social media accounts are all that is needed to instantly share material in real time with tens of thousands of jihadists.

Social networking allows terrorists to reach out to their target audiences and virtually "knock on their doors." Counterterrorism is certainly lingering behind terrorists' manipulative use of the new channels.

Responding to the challenge presented by terrorism on the Internet is an extremely complicated and sensitive issue, since most of the rhetoric disseminated on the Internet is considered protected speech under the United States constitution's First Amendment and under similar provisions in other societies. A realistic way to protect the Internet, to prevent its abuse by terrorists while at the same time protecting civil liberties, is to look for the "golden path," that is, the best compromise. Finding such a path means that we will have to accept both some vulnerabilities of the Internet to terrorism and some constraints on civil liberties, but the

underlying guidelines should be to minimize both sorts of ills by looking at the trade-offs between securing our safety and securing our liberties.

Future of Cyber

How do we deal with the unprecedented ? Part of our cyber policy problem is that its newness and our familiar experience in physical space do not easily transfer to cyberspace.

When we plan for operations in a domain where adversary and friendly data coexist, we should be asking: What constitutes a twenty-first-century definition of a reasonable expectation of privacy? Google and Facebook know a lot more about most of us than we are comfortable sharing with the government.

But if we want to shift the popular culture, we need a broader flow of information to corporations and individuals to educate them on the threat. To do that we need to recalibrate what is truly secret. Our most pressing need is clear policy, formed by shared consensus, shaped by informed discussion, and created by a common body of knowledge. With no common knowledge, no meaningful discussion, and no consensus . . . the policy vacuum continues. This will not be easy, and in the wake of WikiLeaks it will require courage; but, it is essential and should itself be the subject of intense discussion. Who will step up to lead? [18]

David Schaefer expounds on the revolutionary changes in communications technology and the growing complexity of national security, Australia‘s intelligence community faces a relentless growth of the information it collects and analyses. This article explores the impact of this challenge on the foreign intelligence assessment process. In particular, three risks—the threat to information security, the pressure of coordinating assessment, and the potentially harmful influence of policymakers—are examined in detail. Among other changes, a proposed Foreign Intelligence Advisory Board, modelled on the US equivalent, but with distinctive powers suited to Australia, should help minimise problems likely to arise in the years ahead. [19]

One implication of complexity is that, with everything connected by degrees to everything else, the breadth of detail needed to comprehend problems in national security is much wider. This has occurred alongside truly revolutionary changes in communications technology and the proliferation of electronic sources. As a result, data flows of enormous quantity are now being processed by intelligence, and these are only expected to grow as more social activity migrates onto the digital realm in the future.8 In effect, national security is in the midst of an information revolution: with so many sources to monitor and so many ways to do it, experts now speak about the volume of collected data as a defining challenge for the intelligence profession.

The public revelations of intelligence material by the activist group Wikileaks and Edward Snowden have seemingly exposed an oversight in reformist thinking. In their wake, the need to share imperative has fallen under suspicion: among intelligence officials, there are indications of buyer‘s remorse, and newfound scepticism of accessible data systems.

In the case of Wikileaks, routine diplomatic reporting and military footage available to thousands of analysts were released, causing embarrassment and probably discouraging foreign sources from reaching out to US diplomats in the future. Wikileaks relied on a low-level army intelligence analyst, Bradley Manning, who recorded digital copies of the classified material without arousing suspicion. Similarly, Edward Snowden was able to disseminate some of the most closely guarded secrets of Five Eyes intelligence cooperation, which were nevertheless available to him on an internal intranet within the US signals intelligence agency. These are concerning because unfiltered access permitted the exfiltration of as much material as was within electronic reach; once penetrated, there is seemingly little scope for limiting damage.

One proposal that might strike this balance is the establishment of a Foreign Intelligence Advisory Board which reports to the policymaking authority overseeing intelligence. The goal of streamlining the consultation between agencies would benefit from the advice of retired professionals, who know best how to capture the specific knowledge of their former employers while economising on resources. Disputes about the use of interagency teams for assessment could be examined in more detail and refined as the board reviews their performance.

The Religion Card

Although research into the processes and outcomes of radicalization has yielded significant discoveries regarding antecedent risk factors and the role played by societal circumstances and individual variables, research regarding the process of radical conversion remains in its infancy. We believe that the psychology of religion may hold the key to unlocking new insights into this conversion process. As a result of assessing both Lofland and Skonovd’s religious conversion motifs and Rambo’s integrative model of religious conversion, we suggest that issues of culture, society and the individual which are prevalent in first-hand accounts of conversion to terrorism provide crucial insight into the application of theories of religious conversion to the process of radicalization, and that this application is ripe for helping to further develop existing pyramid and staircase models of radicalization.

Jihadist movements primarily focus their recruitment on unmarried males in their late teens or early twenties. High levels of community support for the insurgent group is commonly cited as an important factor in radicalization. Being a terrorist places immense physical, psychological, and social burdens on the individual; they can be isolated, face death, or imprisonment. Yet these risks are outweighed by gaining status, respect, and esteem within their community and the possibility that membership may also bring financial and/or sexual rewards, as well as increased social status.

Research has also revealed how, in addition to the individual strongly identifying with his or her group, identification with role models who support the actions of the armed group is

important in sustaining and committing the individual to political violence.

Lofland and Skonovd identified six unique religious conversion motifs, each of which offers a distinct, defining experience that makes the process of conversion discrete and individual, and which echoes the antecedent factors discussed previously. The six motifs that they suggest are: intellectual, mystical, experimental, affectional, revivalist, and coercive. [20]

To understand radicalization and engagement in violent extremism, researchers and policy makers require comprehensive models which incorporate micro, meso, macro and exo factors, such as intra-individual psychological motivations, community influences and the role of ideology in the analysis. To achieve this, we propose that scholars and practitioners examine research from across the globe that focuses on a range of groups, both active and disbanded, to explore the processes evident in people who engage in violent extremism. While viewing this process as a transformation from non-engagement to active commitment, we believe that exploring the psychology of religious conversion research offers useful insights and models for understanding these processes at a variety of levels of abstraction, while integrating a variety of conditions, factors, and actors into the analysis. Radicalization and religious conversion share many similarities and the conversion motifs and models offer ready templates that can assist in building and managing the understanding of the complex, multifaceted radicalization processes currently taking place.

Coming back to the primary cyber-terrorists, al-Qaeda, Thérèse Postel writes that it is of the utmost importance to understand the ideological influences and relationships that can push young individuals to become radicalized. The similarity through which hate groups, including white supremacists, far right extremists, and fundamentalist religious groups like Al Qaeda entice individuals to act violently on the group's behalf is most instructive for counter-radicalization and counterterrorism purposes.

Terrorism is no longer seen as state-sponsored, but rather as operating organically through a "hub and spoke structure. One of the most prominent ways in which Al Qaeda and its affiliates radicalize an individual is through ideological means. Al Qaeda's ideology can be deployed to create an impression of a "war of ideas" that can be extremely salient to individuals who are experiencing strain or anomie in their lives. [21].

3. Discussion

Radicalization: A Loose Term?

We generally define radicalisation as the process by which a person comes to support terrorism and forms of extremism leading to terrorism, whilst online radicalisation is a process whereby individuals through their online interactions and exposures to various types of Internet context, come to view violence as a legitimate method of solving social and political conflicts.

Though this definition would be true to a large extent if we are restricting radicalization to only terrorist and violent parameters. But seeing the world and world media evolve today we see that radicalization is taking place in many different spheres of life not just in the outskirts of some Arab country or African jungle but right in the midst of our so called developed or developing cities. In countries like the United States of America the world is witnessing a rise in radicalized racial hate crimes against immigrants and people of colour living in the same society. Even here there is a huge role played by the media in disseminating such extreme views and selective angles of the story that is creating an "us vs them" radicalized mentality in the country.

Unchartered Territory: Lack of Knowledge

From the day man set foot on planet Earth, there has been something to fight for. As we can see, wars in cyberspace are a very recent phenomenon, there is a lot of unchartered territory to be claimed and safeguarded from those of ill intent.

One of the major issues facing official government agencies and other organizations world over is that their teams are more prepared and geared towards a physical attack and confrontation. This can easily be seen by the amount of talk we can see about nuclear weapons as compared to that on cyber-attacks and cyber warfare. Many of the agencies are led at the helm by veterans experienced in physical combat but have little to no knowledge about the cyberworld. They need to be constantly briefed and informed about developments and their repercussions.

The need of the hour is to educate and raise awareness at all levels especially official organizations who work is directly impacted by cyber warfare and terrorism. The youth of today is well-equipped and well-informed about the latest developments in the cyber world. The world leaders could take a leaf out of the book of one of the greatest leaders to walk the face of this Earth, Ameerul-Mumineen Umar Ibn al-Khattab and implement his advice regarding youth. He after all had learned from the best educator, Prophet Muhammad himself. The Prophet's council had many young sahabas. In the time of Umar's caliphate if there used to be a problem, Umar used to call the youngsters because according to him their minds were sharp. Societies should invest in the youth to tackle the issue of cyber related issues in the long run.

The experience and wisdom of our seniors and veterans needs to be coupled with the sharpness of the youth to maximise the potential. If this is not done then there is the issue of youngsters taking the law into their own hands to reply to the radicalized organisations. This would cause more uncontrollable damage.

Double Standards

Anonymous has been called a terrorist organization in many countries because of the role it has played in destabilizing multinational corporations etc. To a large extent we see double standards and hypocrisy being employed by the media when they speak about Anonymous taking on ISIS in a cyberwar. Just because Robin Hood helped the poor didn't mean that his action of stealing could be forgiven, overlooked or whitewashed. This could be a case of

supporting the lesser of two evils, but then the main point shouldn't be missed out that at the end of the day both of them are still evil even though at different degrees of it. (N)ISIS is out in the open with who they are and what they are doing. Anonymous on the other hand enjoys a cushion of security and swinging to whichever side of the war that they want because of a total lack of accountability and anonymity.
On the other hand, we have the issue of religious radicalization. But is that the only kind of harmful radicalization? White supremacists seem to target and appeal to individuals experiencing normlessness in their lives and promise them the restoration of their centrality in society, while delivering immense benefits of belonging to a community. This is an indirect method of spreading racism, communal hatred and destabilizing a society.

Role of Media and the Internet

The world is connected even more today than it was half a decade ago. It is as though the entire world has become a large village. In such a connected environment it is becoming increasingly difficult for people to be anonymous, unknown or untraceable. (N)ISIS seems to have learnt a few lessons from Anonymous as they now try to disseminate a lot of their content anonymously so that their communication channels are not caught or blocked by the authorities.

We learn that even though used prior to the massive degrading operation across social media, anonymous sharing portals have played a major role in allowing (N)ISIS to maintain its networking structure in the face of planned operations against them by various governmental agencies and organization. (N)ISIS leveraged the immense reach of social media to share this time not just their propaganda but also the results of those propagandas. They shared pictures, videos and audio clips of barbaric acts like beheading innocent civilians which went viral around the world in a matter of just a few hours.

Such was the impact of these images and videos that social media giants like Twitter, YouTube and Facebook among others had to step up and take some action on their media sharing policies to curb this.

One of the drawbacks of the Internet is that hidden behind the keyboard, everyone is perfect. Everything is shown to be hunky-dory to potential recruits and supporters around the globe. This led to many people to rebel against their own families and chart a way to escape to Syria, mostly via Turkey. On reaching there, the dream cooked up by (N)ISIS media was shattered for many. Large numbers tried to desert them after a few weeks but things as per reports are so strict that anyone who tries to leave is labelled as a spy, outlaw or a disbeliever who deserves to be killed.

Another reason for their propaganda being spread to places without the aid of their media outlets was because of news corporations and the common masses who kept sharing their posts again and again. Allah tells the Believers in the Holy Quran:

يَا أَيُّهَا الَّذِينَ آمَنُوا إِن جَاءَكُمْ فَاسِقٌ بِنَبَإٍ فَتَبَيَّنُوا أَن تُصِيبُوا قَوْمًا بِجَهَالَةٍ فَتُصْبِحُوا عَلَىٰ مَا فَعَلْتُمْ نَادِمِينَ

O you who have believed, if there comes to you a disobedient one with information, investigate, lest you harm a people out of ignorance and become, over what you have done, regretful. [Surah al-Hujurat, Ayah 6]

This ayah clearly gives us guidelines on what to do when such events happen. Even though the work being propagated by (N)ISIS was evil already, the media and the common masses like in a game of Chinese whispers passed on the message forward by adding more spices to the mix. This gave (N)ISIS bragging rights and a global outreach coupled with striking fear at a global level which they might not have achieved had these agencies kept things to the bare minimum with facts instead of resorting to speculation and hype.

Spreading the Message

At the same time because of this global technological transformation, information and trends now take minutes to spread online where they used to take days to spread just a decade ago. As people have formed digital groups and tribes, segments of society who once found themselves ostracized now connect with others in this digital playing field.

The Rise of ISIS moved us from the world of Terrorism 2.0 that used the Internet to Terrorism 3.0, which is fully immersed in social media. ISIS has developed World War Two style propaganda campaigns that now play out in News (AMAQ agency and global coverage), Video (YouTube, News and Terror updates), Audio (sound clips and audio tweets), Social (Facebook, Instagram, Snapchat, Twitter, Weibo, etc.), Video Game mods (ARMA 3) as well as in social campaigns tied to #hashtags. While the US may be winning the ground war, we need new strategies to combat ISIS online.

The propaganda message is spread by hijacking an existing narrative which might be partially radicalized in the first place already, then amplifying that message with a network of automatic "bot" accounts to force the social media platform algorithm to recognize that message as a trending topic. This highlights the message across the platforms and is picked up by major media and publishing houses. Propaganda is an immensely powerful tool, and, if used effectively, it has the immense potential to manipulate populations on a massive scale. This can easily be seen in the case of the US Presidential elections where Russia has been alleged to have rigged the elections. Using social media to take command of the trend makes the spread of propaganda easier than ever before for both state and nonstate actors.

Cyber technology is relatively quite cheap which make it very easy to search and recruit like-minded people from all over the world. Cyber technology has become a one click solution to disseminate information globally. Just as it is a boon by making the world into a global village, it is a bane also depending on its usage. It can and is being used by many radical organizations for the propagation of their radical ideas.

It also plays a central role in financing, training and incitement to commit acts of terrorism. Through the use of cyber technology the access to the youth is very easy and they are vulnerable to be radicalized in a few minutes.

They bank on the freedom of expression right but that is being abused at many levels.

AI and the impact of ISIS, terror and trafficking groups leveraging Cryptocurrency to bypass traditional black market terror financing operations need to be assessed. As the cost of AI and Bots has reduced with time–automated terror via AI and crypto-funding of terror activities raises additional risk.

Unlikely Targets?

ISIS began to recruit from a broader base of individuals who largely had little or no relationship with Muslim communities and often no understanding of Islam. Social Media dissonance or, detachment from society and a readiness to look for disruptive ideas, typifies the nature of millions of people online today. The increase in secularism globally has also complicated the landscape with many individuals in their 20s having few expectations or direction for themselves.

The majority transition from secular to radical. The people in this group do not attend local mosques or even talk to community leaders or neighbours or even the people from their home country. They sit in the dark, learning, and practicing online until they are ready to act. The majority of the radicalized people are off-the-radar for years.

These groups recruit alienated individuals and provide them with a sense of community based upon ethnic or religious ties. Individuals are called to defend this community, and are often convinced that it is a religious duty to do so, or that their community is taking part in a mythical or apocalyptic struggle.

The sense of purpose which these ideologies bring to these people experiencing disconnection from society is a complete mirage. This an area that has which warrants more exploration and research to curb such kind of radicalization. Radicalization, whether it takes place via the Internet or in person, rarely occurs in a vacuum. The fear of “lone-wolf” terrorism is overblown for these reasons. Instead, counter terrorism and law enforcement should focus on interceding with those who are experiencing anomie in their lives. That is why it is said that one should become a teacher and friend of their child before the wrong ones do and then it is too late to do anything but cry over spilt milk. expression “one of us (R. B. G.) thanks ...”. Instead, try “R. B. G. thanks...”.Put sponsor acknowledgments in the unnumbered footnote on the first page.

4. Conclusion

To sum it up, this paper has sought to provide a targeted overview of the current literature available on online radicalizationaiming to help identify important areas of focus which need to be built on in the near future.

It is definitely not possible to predict all the acts of cyber-terrorism which are bound to occur. But, at the same time we do have the tools that will help give us indications and mechanism to reduce or minimize the damage. In the end, unique approaches which are tailor-made to the situation need to be implemented to diffuse any escalated are of conflict in the cyber-world. The literature review in this paper helps shed light and identify over time the radical and extremist identities through ideas and discourses which can be detected and prevented at an early age. Such approaches backed with the consistency of the relevant organizations are in the end the most effective tools against extremism.

References

[1] A. Perešin., "Al-Qaeda Online Radicalization and the Creation of Children Terrorists", 2014.
[2] R. Martins., "Anonymous’ Cyberwar Against ISIS and the Asymmetrical Nature of Cyber Conflicts", The Cyber Defense Review, Vol. 2, No. 3, pp. 95-106, 2017
[3] A.Shehabat, T. Mitew., "Black-boxing the Black Flag Anonymous Sharing Platforms and ISIS Content DistributionTactics" , Perspectives on Terrorism, Vol. 12, No. 1, pp. 81-99, Feb 2018.
[4] E. Schmitt "U.S Intensifies Effort to Blunt ISIS’ Message" 2015.
[5] P. Seib, P., and D.M. Janbek, "Global terrorism and new media: The post-Al Qaeda generation", Routledge. p. 114, 2010.
[6] A.B. Atwan, "Islamic State: The Digital Caliphate". Univ of California Press. p.145, 2015.
[7] J. Berger, J., and B. Strathearn, "Who Matters Online: Measuring Influence, Evaluating Content and Countering Violent Extremism in Online Social Networks. p.41, 2013.
[8] M.C. Libicki., "Can Cybercrises Be Managed?" in Crisis and Escalation in Cyberspace, RAND Corporation, 2012.
[9] O.Sultan, "Combatting the Rise of ISIS 2.0 and Terrorism 3.0", The Cyber Defense Review, Vol. 2, No. 3, pp. 41-50, 2017
[10] J. Prier, "Commanding the Trend Social Media as Information Warfare", Strategic Studies Quarterly, Vol. 11, No. 4, pp. 50-85, 2017
[11] S.Khan and K.M.Butt, "Cyber Technology, Radicalization and Terrorism in Pakistan", Journal of Indian Studies Vol. 3, No. 2, pp. 119 – 128, July – December 2017
[12] S.Noor, "Radicalization to De-Radicalization The Case of Pakistan", Counter Terrorist Trends and Analyses, Vol. 5, No. 8, pp. 16-19, August 2013.
[13] A. Aly, S. Macdonald, L. Jarvis and T.M. Chen, "Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization, Studies in Conflict & Terrorism", Vol 40, No.1, pp, 1-9, 2016.
[14] M.C.Libicki, "Is There a Cybersecurity Dilemma?" The Cyber Defense Review, Vol. 1, No. 1, pp. 129-140, 2016
[15] O. Ashour, "Online De-Radicalization? Countering Violent Extremist Narratives Message, Messenger andMedia Strategy", Perspectives on Terrorism, Vol. 4, No. 6, pp. 15-19, December 2010
[16] C. Archetti, "Terrorism, Communication and New Media Explaining Radicalization in the Digital Age", Perspectives on Terrorism, Vol. 9, No. 1, pp. 49-59, February 2015
[17] G. Weimann, "Terrorist Migration to Social Media",16 Geo. J. Int'l Aff. 180, 2015
[18] M.V. Hayden, "The Future of Things “Cyber”", Strategic Studies Quarterly, Vol. 5, No. 1, pp. 3-7, 2011.

[19] D. Schaefer, "The Information Revolution and Foreign Intelligence Assessment New Challenges for Australia?", Security Challenges, Vol. 10, No. 1, pp. 9-30, 2014
[20] N. Ferguson and E.Blinks., "Understanding Radicalization and Engagement in Terrorism through Religious ConversionMotifs", Journal of Strategic Security, Vol. 8, No. 1-2, pp. 16-26, 2015
[21] T. Postel, "The Young and the Normless Al Qaeda's Ideological Recruitment of Western Extremists", Connections, Vol. 12, No. 4, pp. 99-118, 2013