Combatting the Rise of ISIS 2.0 and Terrorism 3.0

Oz Sultan

ABSTRACT

In the early 1990s, a then-nascent al-Qaeda took steps to redefine both the nature of conflict and the nature of ideological foundations for waging war. The United States military deployment to the Middle East following the Iraqi invasion of Kuwait drove Osama bin Laden to deviate from both defined Islamic theology and fiqh (Islamic jurisprudence) and take a more 'guerilla' approach to combating what he saw as US aggression. Bin Laden deviated from both religion and traditional conventions of war to declare US Troops, supporting contractors, Arab troops, and even fellow Muslims and non-combatant villagers as enemies of al-Qaeda—should they prove to be obstacles to al-Qaeda's goals of regional control and hegemony.

This new characterization of non-combatants and Muslims within conflict zones as the 'enemy' opened up horrific new doors to civilian casualties and collateral damage while setting the stage for the transformation seen across terrorist groups in the past decade.

Counterinsurgent battles from hegemonic struggles waged by waning colonial powers across Africa and Asia in the 1950s and 1960s gave way to the education of militants and insurgent groups from the 1970s-1990s that resulted in well-trained geographically disparate insurgent and terror organizations. These organizations that would traditionally stay relegated to regional conflicts became connected through the Internet and social web starting in the mid-2000s.

Through the 1990s-00's, we witnessed the al-Qaeda (EMEA) threat and the growth of Al-Shabab (MEA), Abu Sayyaf (Philippines), Jemmah Islamiyah (SE Asia), Wilayat Khorasan (Afghanistan, now ISIS-K) and Boko Haram (Africa). The attitude of these groups–some based on Salafist ideals–moved away from religious ideology and

Oz Sultan is a Tech and Marketing Industry veteran with 20 years' experience developing innovative solutions for Brands and Fortune 100 companies. He is also at the forefront of American Muslim affairs, as well as diplomatic and interfaith engagement.

Over the past ten years, Oz has leveraged social media signaling and analysis of trend and social media data to focus on Big Data analysis and how patterns can aid in solving complex problems around us.

Oz has developed a Digital Anti-ISIS framework and counter-radicalization and disruption methodology for stopping online terror.

One fundamental aspect of his work is to get governments and corporations to see the risk of Cyber Terrorism, Crypto Ransom and Social Media converging in what he calls the "greatest risk facing America."

Recently he was a counterterrorism, social media and Big Data advisor to the Trump Campaign. He is a regular contributor to *IJR, TexasGOPVote, The Ish,* and *Newsmax.*

towards a type of cult-like indoctrination methodology. The ideology that could quickly radicalize and weaponize youth fighters and conscripts became essential elements in building insurgent movements.

Adding a degree of complication to this new environment was the nature of different sectarian groups developing within a single conflict arena. For example, during the Iraq War in 2004, there were between 63 and 68 active insurgent and separatist groups. Many had territorial or rights aims, while other groups aligned with different ethnic and Islamic religious sects. This move towards a diffused organization and more cause-oriented sectarian division allowed for the ground transformation that we couldn't have predicted.

Al-Qaeda began moving towards new radicalization methods in the mid-00s. While initially in Arabic, by 2015 al-Qaeda was publishing an English Language Magazine called *Inspire. Inspire* has moved 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 affiliates also publish regional publications for the Indian Subcontinent (AQIS), as well as other global regions.

The Social Media Transformation of Culture

Anyone born before 1980, which covers Great War, Boomer, Gen X and part of the Millennial Generations, had a transference of cultural, ethnic and religious traditions through oral literary tradition; church, synagogue or mosque; community; and family. But Millennials (born mid-80s–90s) Generation Z (born mid-90s-00s) and the Homeland Generation (born 2005-on) have an entirely different understanding of life, culture and religion because of the Internet and new methods of social

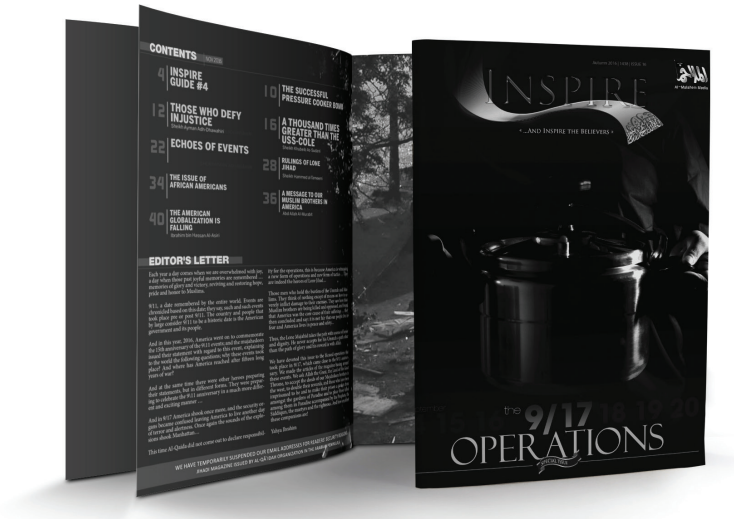

Figure 1. For illustrative purposes only, *Inspire Magazine* is an example of propaganda used by al-Qaeda to broaden its reach and further its cause.

engagement. Further, past generations had different cultural beliefs from location to location, but due to the Internet and the social web, people now have shared experiences across global regions.

Almost 30% of Millennials and a larger percentage of Generation Z were not raised with a religious upbringing and did not have the same cultural or vocational expectations that their parents had.

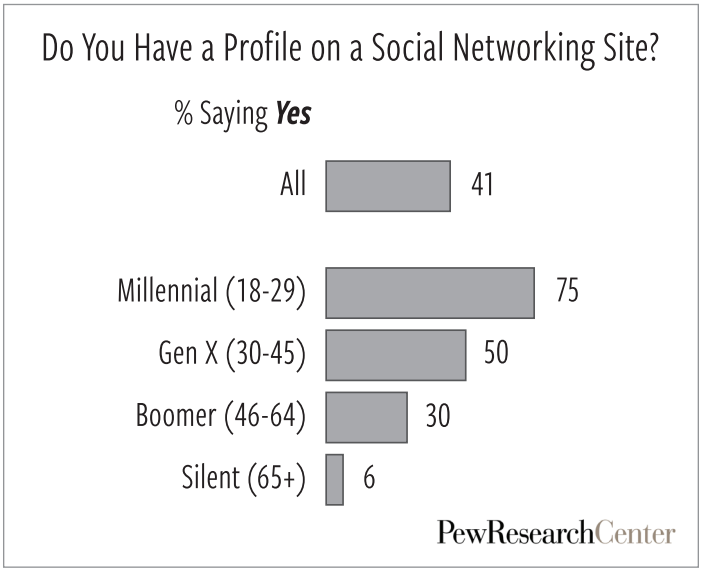

Figure 2. Social Networking

This has given rise to dramatic cultural and experience transference gaps between generations. It has also led to massive shifts in society. A brief survey from the Sultan Interactive Group of Occupy protesters in 2011, showed very little association or understanding of Freedom Riders or social movements of the 1960s, and more focus on disrupting established economic structures.

Today, seventeen to thirty-five year olds are more prone to receive influence, identity, and opinions from social media and social media influencers within their social networks. Social media itself has given way to new social norms, changed expectations and the establishment of online culture jamming. This trend is both local and global. 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 the Jillennial

In the 2000s, al-Qaeda conscripts originated from marginalized Salafi and Deobandi communities in Europe, however, the nature of jihadist recruitment and rhetoric changed completely with the rise of ISIS. 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.

Last year, our Sultan Interactive Group conducted a one-year analysis of 80,000 ISIS-leaning or ISIS-sympathizing Twitter accounts. This included looking at the nature of Twitter account holders, demographics, age, sex, ethnic origin, education, income, lifestyle, religious affiliations, political engagements, previous criminal records, the percentage of youth in jails, the conviction for crimes as well as a societal disengagement index.

Key findings from the research:

> All the recent attackers in France were in their twenties, both of the attackers of San Bernardino were in their twenties as well, so were the majority of attackers in Europe post-2001, from the 2004 Madrid attacks to the 7/7 subway bombings in London, as well as the actors behind numerous foiled attacks. Millennial Jihadists (Jillennials) become a good point to start our data exploration for understanding what they do differently that would help us pick their online patterns and behaviors.

Millennials are more connected to their parents than their parents were connected to their grandparents; parents pay 59% of millennials' cell phone bills, and they do not mind returning to their parent's house and asking for financial help. Twenty-eight percent of millennials get married between the ages of 18 to 32 versus 48% of the baby boomers generation. They are less religious (36% versus 61% of boomers), less patriotic (49% versus 81%), surprisingly less environmentalist (32% versus 44%) and more supportive of LGBT rights (51% versus 32%).

We have found millennials in Europe have 250 friends on average on Facebook, while individuals with a probability of radicalization have less than 100. We found 55% of European Facebook users share their selfies versus almost 1% for the second group of potential ISIS recruits. These millennials can spark a riot in less than two hours using Twitter only, and we call it #HashtagIncitements. If it is among the closely connected cohort of potentially radicalized youth, it can happen within 20 minutes or so.

Key findings of our research validated several conclusions:

- **First,** *the World of War, Social Media and Cyber have intersected. We need a new Crypto Social Cyber Approaches to SOPs, Defensive Postures, and Military Theatre responses:*
  - US Coalition-supported troops, Free Syrian Army (FSA), Kurd (YPG), Russian, and Iranian-backed forces in Syria are often quickly outed on social media with pictures and video disclosing operations. Cyberwarfare is often compromised by social media responses, and with the ease of access to Crypto Ransom weapons, we see operational risks arise.
  - Radicalization exists in a virtual landscape, with virtual conversations and synthetic inducements for people to radicalize. Most often there is the creation of virtual power structures in cyberspace that allow power relations that do not exist in the real world.
  - We can imagine an avatar who relies more on emoticons than words, taking a seat next Ayman al-Zawahiri or Abu Bakr al-Baghdadi. While the players behind the character may change, the digital persona remains the same, thus providing an immortal inspiration to admire and emulate.
- **Secondly,** *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.

- **Thirdly,** *The Process of Radicalization opens a Pandora's box:*
  - 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. With dozens of Online Encouragements and a higher ordinance in the artificial chain of command, anyone can become a commander-in-chief of their sleeper cell that does not exist in reality.

As such, the profile of the Jillennial is different from profiles that have been previously developed. These are validated by arrests over the past 24 months.

Typically they are:

- Millennial (21–34), Disenfranchised
- Western (White) or Second Generation Immigrant
- Secular (Non-religious)
- Looking for Meaning (ISIS baits for this)

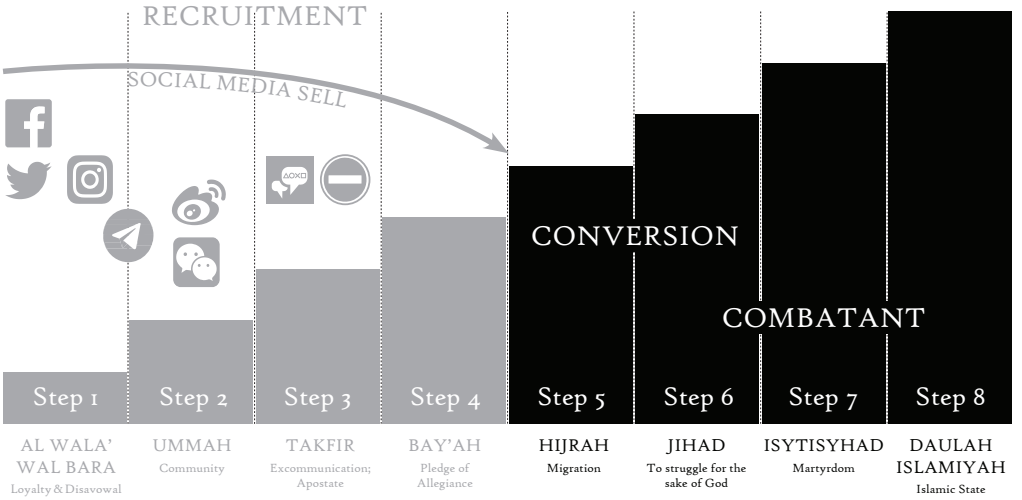

Figure 3. ISIS's Online Recruitment Process

Globally and within the US, we see an increased need to educate, engage, and defend against this risk profile. We live in a world of social media marketing campaigns where Instagram posts, video game mods, and Twitter are being used as tools to recruit. These campaigns are so successful they even ensnared a disenfranchised and marginalized US military member in July 2017.

ISIS's primary recruitment methodology leverages online social media tools and messaging that run like marketing campaigns similar to the best marketers in America. Quilliam International estimates that ISIS operates a network of about 1,000 social and digital media operatives globally, making their staff more numerous than many large public relations agencies.

Their recruitment process starts with glossy English-language publications like Dabiq, and social seeds and hashtags across the social web. Dedicated websites on the Darkweb and readily available ISIS propaganda online are coupled with a recruitment process that is socially geared towards the disenfranchised millennial audiences.

The Social Media phase of ISIS's recruitment process

Once a prospect starts communicating with an ISIS recruiter, they are quickly sold a 'bill of goods' that include incentives, opportunities to lead or to find a "meaningful life and place". The recruitment process involves an initial pledge to Islam, as well as the standard cult tactics of cutting off friends and family for a new "peer and social group". Once this occurs, they are led to excommunicate their family, all religious elements in their life, and take an oath of allegiance to ISIS.

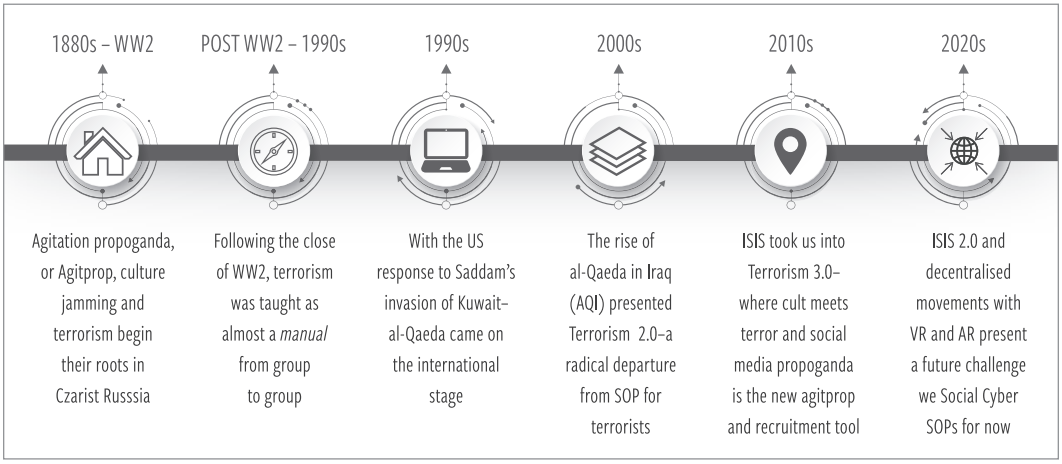

Figure 4. Terrorism 3.0 and ISIS 2.0

To disrupt this process, we must focus on new strategies of engagement, social media SOPs, and develop guidelines for remediating social media, marketing, and recruitment threats that live in the same real-time, online terror ecosystem. Beyond recruiting, people, nations, and corporations now face the same degree of risk. Manchester is a case study in the impacts of people, a country (UK), a town (Manchester), businesses, physical property (SMG, the arena operator) and a pop icon (Ariana Grande).

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. If ISIS can have four glossy online media magazines in addition to sophisticated online posts, video, tweets and retweets from a single IED attack, then the West needs to bridge the social media gap through cyber-focused Intel to fight back effectively.

In the Spring of 2017, ISIS put out a call to their recruits for attacks focused on civilians in Europe, the US, and Australia. This call was fulfilled with attacks in Manchester, London, France, and a bomb attempt in Brussels during the summer of 2017.

As ISIS was able to spread unabated over the past six years–mainly due to global hand-wringing and bureaucratic indecision over Russian and Iranian involvement in Syria–ISIS expanded their footprint. Wilayat Khorasan became ISIS-K in Afghanistan, and the ISIS involvement with Abu Sayyaf and the Maute Group in the Philippines shows a new strategic partnership. ISIS is focused on a grassroots expansion–raising the challenge of an ISIS 2.0 once their Deir Ezzor and Raqqa strongholds are eliminated. ISIS is partnering with regional terrorist groups to extend their reach, creating a global fallback network when the Caliphate collapses in Syria.

ISIS 2.0 increases global risk by a hundredfold while raising new questions. When ISIS is defeated in Syria, will they aim to acquire another State or maintain destabilized regional pockets that keep the West in a perpetual, low-grade war? Further, as we prepare to tackle these new challenges, are we considering the long-term implications, as well as what this will mean to societies in 2035, and to government agencies or the military from 2018 onwards?

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.

Our long-term goals should be to develop integrated protocols and SOPs that have measurable KPIs to counter ISIS and evaluate online social sentiment. We also need to be cognizant of the risks that Crypto, social media and cyber pose in a landscape where we will be using cyber to fight Social Media Terrorism and Crypto Terror. We also need to focus on improving information sharing between US military services, IC, government agencies, Nations, and the business community.

The intersection of these areas also present a further risk as technology moves into AR/VR and touchable Holograms–the threat of Terrorism 4.0 is only a few years out. ISIS has shown us the threat within the real-time, social media environment. The time to tackle that threat is now.