The Islamic State’s Information Warfare: Social Media and Propaganda Engineering

For decades, the United States has faced a growing threat of Islamist terrorism towards the homeland. The rise of the self-identified Islamic State, commonly known as ISIL or ISIS\(^1\), has been effectively utilizing social media outlets as an informational instrument to promote its cause, recruit more members, and cause havoc amongst the globe. Through various social media platforms, movies (i.e. *The Flames of War*), YouTube videos, and their very own online multilanguage magazine *Dabiq*, which has recently been replaced with their new online multilanguage magazine *Rumiyah*, the Islamic State has become adept at manipulating media to gain support and create an ideological movement. “The analysis of the digital audiovisual campaigns released by ISIS since January 2014 suggests that ISIS has established a new kind of terrorism, using marketing and digital communication tools not only for "socializing terror" through public opinion as previous terrorist groups did, but also for making terror popular, desirable, and imitable.”\(^2\)

The Islamic State is well funded, organized, and grounded in the authority of religious texts and words of Islamic scholars. It now controls multiple border crossings along with various weapons and infrastructures throughout their controlled territory in Syria and Iraq. Their extreme violence and use of various media outlets for recruitment and scare tactics is a growing concern in this fight. The Islamic State has developed new tactics, to include a multi-million dollar media campaign, to create a unified worldwide Islamic State with Sharia Law as the basis. The phenomenon of the rise of the Islamic State correlates with the rise of technology and social media, compared to al-Qaeda which did not have a very good media campaign to spread their message. “Between March 2014 and November 2016, 124 individuals in the U.S. affiliating with ISIS have been interdicted by law enforcement, whether traveling to fight, recruiting, fundraising, planning to travel, promoting ISIS, or initiating or carrying out attacks which averages about 5.1 ISIL arrests per month on American soil. In comparison, in the ten years following 9/11, an estimated 176 Americans were indicted, arrested or identified as terrorists/terrorist supporters affiliated with al-Qaeda.”\(^3\)

The Islamic States success stems from the creation of the new Caliphate in July of 2014 in Syria and Iraq, after nearly 90 years of the fall of the Ottoman Empire. Abu Bark al-Baghdadi was declared the new Caliph of Caliphate and The Islamic State now controls territory in both Syria

\(^1\) The Islamic State will be referred to as either The Islamic State, ISIL, or ISIS throughout the paper depending on the source of information.


and Iraq, with affiliate branches in Libya, Saudi Arabia, Sinai, West Africa, Yemen, Khorasan, and the North Caucasus regions. Additionally, the Islamic State has a robust supply stream of resources, money, and fighters which continues to support its overall mission of global jihad expansion. Although coalition forces are hoping the Islamic State falls in Syria and Iraq, their ideology and mass expansion both physically and virtually is a force to be reckoned with for many more years to come.

America’s response to this threat has been solely based around a battle of arms, rather than a battle of ideas. The United States must recognize that the foundation of this war of ideas is built upon theological Islamic ideology and therefore must render information as its most influential instrument of national power to counter their messages in cyberspace. Information as an instrument of power has been poorly wielded by the U.S. government to defeat the Islamic State; ignorance of the fact that terrorism is being carried out in the name of Islam to wage jihad against America makes it harder for U.S. policy-makers to defeat this ongoing threat. These extremists are now taking their ideological movement to the internet in order to recruit, radicalize, and attack their enemies both physically and virtually. Whether dead or captured, the internet provides jihadists with a virtual immortality. Indoctrination, recruitment, financing, training, and ideological messages continue 24 hours a day, 7 days a week in the cyberspace battlefield.

Globalization has given rise to a ‘skill revolution’ that enhances the capabilities of groups to carry out their agenda more effectively than ever before. Social media outlets and virtual communications have allowed the Islamic State to grow into a powerful organization that the world has not seen before.

**SOCIAL ENGINEERING –ISLAMIC STATE PROPAGANDA TOOLS**

Technology is an enabler; we have to get to the root of the problem which is the ideological goals of the human behind the technology. The single most effective tool for detecting Islamic State supporters has been through their social media activity; in the first 9 months of their existence, the Islamic State recruited an estimated 20,000 foreign fighters and an estimated 4,000 Westerners via social media. However, tracking terrorists on social media is not that simple; for example, the planning for the 2015 Paris attacks went completely undetected by French intelligence.

---


“ISIL is well versed in the power of the media, they have been joined by a new generation of millennial recruits. The average age of foreign fighters who traveled to join ISIL is 24, meaning tools like Facebook, Twitter, and Instagram are what they’ve grown up with.” In the context of global jihad, this is a dangerous combination.

A study done by the Brookings Institute revealed that ISIL released 845 audiovisual campaigns between January 2014 and September 2015, or more than one every day for a year and a half. Qualitative analysis of all 845 campaigns shows that more than 15 percent are directly inspired by real films, videogames and contemporary popular culture, such as the films Saw, The Matrix, A V Vendetta; or videogames like Call of Duty, Mortal Combat X and Grand Theft Auto. The study further revealed that ISIL supporters control more than 46,000 Twitter accounts through which they release their messages.

Senior Islamic State leaders are calling for ‘all’ individuals to join their cause and attack the kuffar. These types of broad orders are given out through social media platforms and propaganda tools such as al-Qaeda’s magazine Inspire and the Islamic State’s magazine Dabiq, and are directed towards anyone who may be reading or listening. There is a shift in the traditional chain-of-command now becoming a virtual chain-of-command, making dismantling or disrupting emerging operations and strategic direction an extraordinarily difficult thing to achieve for the Intelligence Community.

Building a Brand Online: The Caliphate

The Internet serves as a critical instrument of power for enabling and directing the goals and objectives of many terrorist organizations. The Islamic State’s sophisticated use of the Internet demonstrates their operational effectiveness while simultaneously undermining the goals of the

---

9 A person who rejects God and the word of Prophet Mohamed.
US government and US interests. The Internet allows the Islamic State to build their brand, sell their image and messages, recruit members and supporters to their organization, build wealth, and virtually spread Islamic State franchises all around the world. As a result, the Islamic State has been more successful in conducting attacks and recruiting members since the declaration of its Caliphate in 2014 than any other terrorist organization in history.

Why do terrorist organizations rely on the man-made Internet, a system that should be looked at as *haram* (Arabic for forbidden) in the Islamic world due to its accessibility and knowledge of Western cultures and traditions? The Islamic State, along with other terrorist organizations, rely on the Internet to serve as its foundation to reach audiences that could otherwise not reach geographically. Rather than attacking the Western man-made Internet in forms of cyber hacks, they are using it to survive and thrive. If the Islamic State does attempt a hacking act, it is usually to continue to spread their message on popular websites, or to steal personally identifiable information to target individuals for future attacks.

The Internet has multiple characteristics that make it an ideal tool for terrorist organizations to manipulate, below are the more obvious characteristics that have been utilized by terrorist organizations globally.

The first characteristic is the Internet’s ability to allow individuals to communicate at the speed of light. Terrorists can use various messaging platforms, blogs, website forums, live video streaming sites, etc. to have conversations in real-time to anyone anywhere in the world. Social media platforms such as Twitter, Facebook, and encrypted platforms such as Telegram, serve as a means of communication to reach would-be recruits. Once the initial chat begins between a terrorist and a supporter, the individuals can then go into a direct-messaging format within the social media tool and begin privately talking, in real-time, about their goals and group.

Second, using the Internet is a low-cost proposition. The Islamic State can now affordably direct training events, establish relationships, build an online media business (news agencies, magazine production, etc.), wire money, gather intelligence, and the list of possibilities goes on. Although the Islamic State is estimated to make an annual budget of around $2 billion\(^\text{10}\), which is used to operate their Caliphate and pay their soldiers, they are able to conduct their online activities in a free cyberspace environment.

Third, the Internet allows terrorist organizations to thrive anywhere in the world. The Islamic State has built its Caliphate in Syria and Iraq, with the intention of expanding worldwide. The headquarters of the Caliphate resides in parts of Syria and Iraq, where a lot of the leaders, training, money, status, and religious significance lies. Both of these countries are extremely difficult to travel to and from, have a very dangerous living environment with on-going strikes by coalition forces, and cost a lot of money to get to. The Internet has allowed the Islamic State

to give orders to those who cannot afford to make the trip to Syria to stay where they are and strike the enemy at home; something al-Qaeda was never able to message globally. The Islamic State has a global cyber power and presence that rivals all other terrorist groups.

Fourth, the Internet is constantly evolving and growing allowing for more advanced software developments and memory/bandwidth space on servers. This advancement will continue to enable terrorists to develop and disseminate lengthy, sophisticated, and technologically complex information via the Internet. For example, “a militant Islamic chat room posted a twenty-six minute video clip with instructions on how to assemble a suicide bomb vest, along with a taped demonstration of its use on a model of a bus filled with passengers.”

As technology advances, Internet users can now find terrorist training materials, bomb making manuals, inspiration by Islamic scholars, religious texts, and a multitude of other propaganda right at their fingertips. The Islamic State has taken a new step in online recruitment by filming and distributing the brutal 2014 beheadings of American and British individuals in Syria. American journalists James Foley and Steven Sotloff, American aid worker Peter Kassing, and British humanitarian aid worker Alan Henning were brutally beheaded by Mohammad Emwazi, aka “Jihadi John” and posted the brutal acts on YouTube for the world to see.

The Islamic State first uploaded the video to YouTube and “tweeted a graphic blow-by-blow series of stills showing the knife cutting his throat, the removal of his head, and the placement of his severed head on his lifeless body. This act created an earthquake on social media, as thousands of these tweets went viral.” Social media companies are now becoming more scrutinized and targeted by law enforcement to corporate with them in their investigations into the online portion of recruitment and identification of terrorists.

The Islamic State knows that by gaining worldwide media attention by popular news stations such as CNN, Fox News, or Al Jazeera, they are able to reach audiences that may not be familiar with the Islamic States successes or tactics. The major news stations are potentially acting as a gateway for an individual who may become more curious or encouraged by the Islamic State,

---


thus expanding their own research beyond what is aired on the news. This flow chart explains the steps taken by Islamic extremists from the moment of a terrorist act, to getting international media attention and everything in between.¹³

![Flow Chart Explaining the Steps Taken by Islamic Extremists](image)

Lastly, the Internet allows for various media platforms to develop encryption technologies that allow terrorists to become anonymous and invisible. Users of end-to-end encrypted messaging platforms like Surespot, Telegram and Wickr can communicate with each other undetected because the encryption key is nearly impossible to decrypt. This capability is a major challenge for law enforcement officers and the intelligence community to find, track, and deter terrorists utilizing this capability. FBI Director James Comey calls this phase ‘Going Dark’ where terrorist will socialize overtly on social media, then switch to either private messaging within the platform or switch mobile applications completely:

“Today, there are countless providers, countless networks, and countless means of communicating. We have laptops, smartphones, and tablets. We take them to work and to school, from the soccer field to Starbucks, over many networks, using any number of apps. And so do those conspiring to harm us. They use the same devices, the same networks, and the same apps to make plans, to target victims, and to cover up what they’re doing. And that makes it tough for us to keep up. If a suspected criminal is in his car, and he switches from cellular coverage to Wi-Fi, we may be out of luck. If he switches from one app to another, or from cellular voice service to a voice or messaging app, we may lose him. We may not have the capability to quickly switch lawful

http://resources.infosecinstitute.com/the-role-of-technology-in-modern-terrorism/
surveillance between devices, methods, and networks. The bad guys know this; they’re taking advantage of it every day.”

**Advancements in Propaganda Engineering**

On September 11, 2001, Facebook\(^{15}\), Twitter\(^{16}\) and YouTube\(^{17}\) did not exist. The way al-Qaeda disseminated its propaganda, therefore, was by “sending written statements and videos to news outlets such as Al Jazeera, launching big attacks guaranteed to make the international news and communicating with other jihadists in relatively obscure online forums.”\(^{18}\) Usama Bin Laden would send out his audiotapes and video messages to news outlets like Al Jazeera in order to get his messages spread to those who may be watching. In his videos, Bin Laden is wearing army fatigues with an AK-47 behind him, sitting Indian-style in a cave; his image came across a solider and military commander, and his messages were all in Arabic. This image is very opposite of the new Caliph, Abu-Bakr al-Baghdadi who declared the Caliphate reborn from a pulpit in Mosul, Iraq in July 2014 wearing a black clerical robe, which was filmed and posted to YouTube and tweeted via Twitter for millions to see.

It wasn’t until years later when al-Qaeda really started to utilize the internet for radicalization and recruitment purposes to build their army of followers outside of the Middle East. The release of al-Qaeda in the Arabian Peninsula’s (AQAP) online English-language magazine *Inspire* really started the movement of recruiting more Western recruits, and more and more people started to seek guidance from al-Qaeda.

*Inspire* magazine was created in 2010, thought to be the work of Anwar al-Awlaki, an American-born Islamic cleric who spoke English and Arabic fluently. Awlaki was educated in the United States and became an Islamic Imam at various mosques in the states before deciding to move back to Yemen in 2004 where his family resided. Awlaki’s fluency in English, his gracious and inspiring demeanor during his sermons (in person and online), his clerical credentials both inside the United States and in the Middle East, plus his knowledge and experience of American culture allowed him to successfully recruit Americans to join the jihadist movement. Awlaki’s online sermons on YouTube are viewed by thousands of people; one sermon got over 70,000\(^{19}\) views and his online success continues to thrive even after his death. Samir Khan, a 24 year old who was born in Saudi Arabia but grew up in New York, was one of Awlaki’s biggest fans. Khan praised the 9/11 attacks and was angry by the Iraq invasion, and therefore started a website

---


\(^{15}\) Created in 2004

\(^{16}\) Created in 2006

\(^{17}\) Created in 2005


devoted to jihadist propaganda, which was edited from his parents’ home in North Carolina. Khan eventually moved to Yemen in 2009 to where he united with Awlaki, eventually becoming the editor and co-creator of *Inspire*.20

Ironically, two Americans were the masterminds behind this key propaganda tool, which was a significant contribution to the recruitment and radicalization process of Westerners. Young and motivated want-to-be jihadists possibly started to admire Awlaki’s dedication to jihad and really started to listen to him on YouTube and eventually started reading the messages in his new magazine.

The magazine consisted of articles that reinforced the al-Qaeda narrative, and promoted an individual strive towards jihadism. The magazine praised martyrs, and gave instructions on how to conduct everything from simple terrorist attacks, to constructing improvised explosive devices (IED). Awlaki was killed by US forces via drone strike on September 30, 2011 in Yemen along with Samir Khan.

“There communications with potential American recruits have been further facilitated by such native-born Americans as Adam Gadahn and Omar Hammami, who have become official spokesmen for the al-Qaeda core group in Pakistan, and al-Shabaab in Somalia. Although these individuals joined these fronts as volunteers, their prominent role as communicators reflects the strategic importance the movements place on communicating with an American audience.”21

Now, many jihadists begin their journey toward radicalization on the internet; it has become an individual decision rather than a community phenomenon. Individuals start to become disillusioned with Christian views and Western cultural traditions and believe that Islam is their only path to spiritual freedom. The internet also allows individuals to join group chats, and make more friends online than they would likely have in person. These group chats are filled with like-minded individuals, where they are able to vent and reinforce their frustrations amongst each other.

**DABIQ MAGAZINE: Advancements in Media Production**

Much like al-Qaeda, the Islamic State created their very own online multi-language magazine titled *Dabiq*. Dabiq is a town in North East Syria where the Islamic State believes that the ‘End Times’ battle between the Christians and defending Muslims will take place in for the final jihad, based on their eschatological theology. Although the validity of this view of the ‘End Times’ is debatable within Islam, the Islamic State cares deeply about this battle and is glorifying this theme very effectively.22

---

*Dabiq* magazine, now on its 15th issue and is very sophisticated; it features high-quality photos and up-to-date interviews of scholars and Islamic State soldiers. It praises recent terror attacks throughout the world along with praising the individuals who committed the acts as martyrs. It encompasses religious doctrine throughout each issue, while also emphasizing the need to engage in jihad as a Muslim’s rightful duty. Issue 15 of the magazine has an article title “Why We Hate You and Why We Fight You” where the Islamic State clearly express their views towards the West:

“The fact is, even if you were to stop bombing us, imprisoning us, torturing us, vilifying us, and usurping our lands, we would continue to hate you because our primary reason for hating you will not cease to exist until you embrace Islam. Even if you were to pay jizyah and live under the authority of Islam in humiliation, we would continue to hate you. No doubt, we would stop fighting you then as we would stop fighting any disbelievers who enter into a covenant with us, but we would not stop hating you.”

Additionally, another article in Issue 15 titled “Words of Sincere Advice: From an American Convert in the Islamic State to the Former Christian who Accepted Islam” continues to give guidance and direction for any individual who may want to commit an act of terror. This article is a powerful form of social engineering, which has an American giving advice on how to conduct terrorist attacks:

“As for a final word of advice to you regarding your operation, do not make intricate plans, but instead, it simple and effective. If you can obtain a weapon, do so and use it, as soon as possible and in a place that will cause the most damage and panic, bringing death and injury to the enemy of Allah, disbelievers.”

*Dabiq* has recently been replaced with a new online multi-language magazine titled *Rumiyah*, which means “Rome” in Arabic. *Rumiyah* features shorter articles, yet has the same quality of photos, direction, and guidance as *Dabiq*. There is little evidence as to why the Islamic State decided to change the name and publication style of their magazine, but the new title suggests that the Islamic State is planning to expand its Caliphate to the West, rather than focusing its efforts specifically in Dabiq or the Middle East. *Dabiq*, and now *Rumiyah*, and whatever magazine comes after will continue to be a tool of inspiration, radicalization, and recruitment for the global jihad movement.

Both al-Qaeda and the Islamic State are comprised of youthful foot soldiers and a youthful online audience; therefore it should not come as a surprise that the internet is the primary tool for radicalization, recruitment, and dissemination of propaganda and operational guidance.

“Whereas only a handful of jihadist websites existed in 2001, there are reportedly thousands today. In their early years, jihadist websites demanded a knowledge of Arabic, but the number of

---

English-language websites reportedly has increased to several hundred, making al Qaeda and the Islamic State’s messages more accessible to the West.”25 Al-Qaeda and the Islamic State have increased their propaganda capacity in other Western languages, such as German and French, in hopes to inspire more Western individuals to conduct lone wolf attacks on their behalf.

Homegrown Violent Extremist Online Radicalization and Mobilization

The use of technology enables the Islamic State to recruit by the tens of thousands, which provides evidence that they are equipped to conduct an imminent attack, be it cyber, kinetic, or a combination of both. Their vision to expand their physical and virtual Caliphate stems from their tangible recruitment efforts throughout the world. In order to ensure their efforts succeed, the Islamic State has a multi-media campaign to recruit, radicalize, and mobilize homegrown violent extremists to their cause.

Homegrown terrorism is one of the more difficult types of terrorism to deter; these individuals are often indistinguishable from the rest of the population and, therefore, very difficult to recognize or uncover. Lone wolves are inspired by these Islamist leaders through propaganda and thus adhere to the duty they are called upon. “But the online jihad is no longer a matter of waiting for word from the top. Production has exploited new web platforms that allow users to also become producers of material. Although websites can still be distinguished hierarchically between official communications and more democratic discourse, the online jihad has become a parallel universe to the physical world of bombs and burnt flesh.”26

The Islamic States now-deceased spokesman, Abu Mohammed al Adnani, urged the group’s supporters “if you can kill a disbelieving American or European – especially the spiteful and filthy French – or an Australian, or a Canadian, or any other disbeliever from the disbelievers waging war, including the citizens of the countries that entered into a coalition against the Islamic State, then rely upon Allah, and kill him in any manner or way, however it may be.” He continues to order “smash his head with a rock, or slaughter him with a knife, or run him over with your car, or throw him down from a high place, or choke him, or poison him.”27 Adnani’s message resonated with a lot of supporters and his demands are easily accessible on the internet even after his death.

The Islamic State understands how to do propaganda in the age of social media; we are now seeing more individuals using Twitter, Facebook, YouTube, and many more popular social

media platforms as an outreach platform to directly talk to supporters of the Islamic State. The 2015 Paris attacks, the Boston Marathon bombing, Fort Hood shooter Major Nidal Hasan, the San Bernardino shootings, the Orlando Pulse Night Club shooting, and many others exemplify how Islamic ideological propaganda can impact in those in the West.

The following incidents committed by homegrown violent extremists highlight the social media element and human element attached to their respective attacks. It’s not only the Islamic State’s use of media campaigns to recruit fighters and conduct attacks that makes the threat formidable, it’s the fact that these information campaigns are resulting in the actions leading to security concerns or death of innocent civilians.

**Boston Bombers: Bomb Making from Inspire Magazine**

*On 13 April 2013, brothers Dzhokhar Tsarnaev and Tamerlan Tsarnaev placed two pressure cooker bombs at the finish line of the Boston Marathon race where they exploded and killed 3 individuals and injured over 250.*

Throughout the investigation into the bombings, it was discovered that the brothers learned their bomb making skills from the first issue of AQAP’s *Inspire* magazine. The first issue of *Inspire* had featured an article titled “Make a Bomb in the Kitchen of Your Mom” which was how the Boston Marathon Bombers learned to make their pressure cooker devices that went off at the race, according to statements Dzhokhar Tsarnaev told the authorities. The first issue of *Inspire* had featured an article titled “Make a Bomb in the Kitchen of Your Mom” which was how the Boston Marathon Bombers learned to make their pressure cooker devices that went off at the race, according to statements Dzhokhar Tsarnaev told the authorities. The magazine continues to encourage more attacks in the United States and creates the image of Tamerlan as a successful martyr.

**San Bernardino: Pledging Allegiance to the Islamic State via Facebook**

*On 2 December 2015, Tashfeen Malik and her husband Syed Rizwan Farook killed 14 people and injured 22 after the couple went on a shooting spree at Farook’s place of employment at a Public Health facility during the company’s holiday party in San Bernardino, California.*

Throughout the federal investigation into the shootings, it was revealed that the couple was radicalized before they started dating, and had discussed jihad and martyrdom once they started to become more serious in their relationship. The investigation also revealed that the couple was making bombs in their home, and had stock piles of ammunition. “Tashfeen Malik passed three background checks when she moved from Pakistan but none looked at her social media. Secretary of State John Kerry suggested that while "social media has placed a whole new

---

burden” on the visa security process, it should be possible to review the activity going forward. President Obama has ordered a review of the K-1 visa program in wake of the attacks.”

Prior to committing their terrorist attack, Tashfeen Malik pledged her allegiance to the Islamic State on Facebook, which was seen and recognized by the terrorist organization. Issue 13 of *Dabiq* praises the Malik and Farook as martyrs, giving them a two-page forward describing their willingness to give up everything for the sake of fulfilling their duty to Allah. The piece states the way Farook answered the call to “strike the crusaders in their own lands” was unique because rather than carrying out jihad alone, he did the attack with his wife. The piece continues to state that their actions should awaken other American Muslims to act. The issue shows a picture of their child’s crib, and states that even though they had a 6 month-old child to care for, they were still willing and able to carry out their duties. The magazine also seeks to recruit more terrorists by shaming them, stating Malik was willing to attack when many “men” aren’t, and proceeds to show a bloody picture of Syed after being shot by local law enforcement with the caption “May Allah accept him.”

The San Bernardino terrorist attack became a symbolic propaganda tool for the Islamic State. This was the first time in US history that a Muslim couple attacked fellow Americans, suggesting that females are capable of committing jihad just as much as a man. To leave their daughter and family behind also became a prominent social engineering tool for the terrorist organization in hopes of recruiting more American’s to follow in their footsteps regardless of their Western lifestyle.

These HVE’s were inspired by the Islamic State through online communications and propaganda, and then pledged their allegiance to the group and its leader, Abu Bakr al-Baghdadi through social media. These terrorists were praised as martyrs by their fellow supporters, while the Islamic State credited the acts via Twitter and other social media platforms. It is easier for homegrown terrorists to self-radicalize in the comfort of their own homes stealthily through the internet; these individuals may be your next-door neighbor leading what seems to be a perfectly normal life. The challenge lies within the context of understanding what motivates moderate Muslims and Westerners to change their ideology and sympathize with the teachings of Islamic leaders.

There are many examples of how Western citizens have been radicalized and indoctrinated online by terrorist organizations to commit terrible acts of violence in our homeland. “The process of radicalization is getting shorter and the choice of soft targets and weapons is becoming more unpredictable.” Nearly forty thousand young men, and increasingly young


31 Deen, Adam. “I used to be an Islamic Extremist. This is the Truth about how you Can Prevent Further Terror Attacks,” *Independent News*. 2016. [http://www.independent.co.uk/voices/i-used-to-be-an-islamic-extremist-this-is-the-truth-about-how-you-can-prevent-further-terror-attacks-a7145816.html](http://www.independent.co.uk/voices/i-used-to-be-an-islamic-extremist-this-is-the-truth-about-how-you-can-prevent-further-terror-attacks-a7145816.html)
women have left their homes to fight for the Islamic State in Iraq and Syria; however the former Islamic States spokesman Adnani’s call to stay and fight the enemy where you are has resonated with Westerners. There has been an increase in Islamic State supporters remaining in the U.S. or Europe to commit an act, rather than leaving to fight in the physical Caliphate.

The year 2015 was the worst year for Islamic terrorist attacks in the United States; the FBI has open investigations into Islamic State inspired homegrown violent extremists in every single state in the U.S., according to statements made by FBI Director James Comey. Figure one below shows the increase of Muslim-Americans who were suspected and perpetrators of terrorism since 9/11, showing 2015 with the highest bar:

---


Cyber Advancements in Terrorist Recruitment and Planning

2015 PARIS ATTACKS – PLAYSTATION NETWORK

The Islamic State has taken credit for the 13 November 2015 Paris attacks that killed 130 people and injured 368. The Islamic State praised their success over social media and in Issue 12 of Dabiq. Not only did they praise their success via social media, there has been reports that suggest the planning and coordinating of the attack may possibly be linked to Sony’s PlayStation 4 (PS4).

Although there is no hard evidence to support the claim that PS4 was used in planning and coordinating the Paris attacks, communication on Sony’s PlayStation Network (PSN) is notoriously difficult for authorities to monitor. This is not the first time that PS4 has been linked to terrorism; in May 2015, “a 14-year-old Austrian boy plead guilty to using his PS4 to contact Syrian ISIL militants and download bomb schematics. In addition to top-level chat systems in PSN and Xbox Live, players can also communicate through both text and voice chat within games themselves, which would be nearly impossible to comprehensively monitor.”

“By last count, PSN boasted some 110 million users – 65 million of them active – making it a large group to track” even though developers of Sony’s PlayStation and Microsoft’s Xbox Live have built in the ability for law enforcement to monitor criminal activity.

On PS4, users can message each other via the Sony Entertainment Network (SEN). Messages can be sent to anyone, whether or not you're "friends" on the service (becoming "friends" on SEN works similarly to Facebook: you send a friend request that is either accepted or denied). Further, users could communicate by using the video game “Call of Duty,” for instance “to spray a message in bullets on a wall that then is quickly gone from the screen. They could use a system of coding through any sort of game, making their moves represent what they want to communicate.” The PSN has their own virtual chat options, however so do the specific games that individuals may have bought and are playing. This type of incident is very significant because these non-verbal communications would be nearly impossible for law enforcement to track, especially if they are off the PSN network.

---

Planning and coordinating attacks through video game networks is very significant in today’s threat environment; the players can get motivated and inspired by playing games that involve killing people, and they may want to take their virtual weapon skills to a real battlefield. The Islamic State is very strategic in the social engineering aspect of these video games. The photo shown here was put out by ISIL in their online magazine *Dabiq* telling it’s fighters that “This is our Call of Duty and we respawn in Jannah,” which is translated to coming back to life in paradise, as opposed to coming back to life as the video game avatar.

**CYBER CALIPHATE: ISLAMIC STATE HACKING**

The Islamic State narrative is very powerful through its social media campaign. The Islamic State’s cyber threats are very disturbing, and their hacking schemes have led to various security concerns involving government networks and personnel. ISIL hacking has been increasing as they continue to employ and recruit extremists with technical backgrounds.

The now-deceased Islamic State hacker and former leader of the Cyber Caliphate Junaid Hussain, aka Abu Hussain al-Britani, has set a high standard in cyberspace for Islamic State propaganda and cyber related attacks. Hussain was killed in Syria by a US drone strike in August 2015 and his wife, Sally Ann Jones, is currently on a Government list of the most dangerous British recruiters for the Islamic State. The Islamic State’s cyber achievements have been limited, however as their Caliphate grows, so does their cyber army. The Cyber Caliphate is known for their defacement of websites, DDoS attacks to temporarily knock sites offline, and takeovers of social-media accounts.

The U.S. charged and arrested a Kosovo native, Ardit Ferizi, aka Th3Dir3ctorY, in October 2015 for hacking into a U.S. database and stealing personal information on more than 1,350 military and government personnel on behalf of the Islamic State. Ferizi later passed the data to Junaid Hussain who spread the information on his Twitter page. The information Ferizi obtained included U.S. personnel’s email addresses, passwords, locations and phone numbers, according to the Justice Department. In the first case of its kind, the department charged Ferizi with providing material support to a terrorist organization, computer hacking and identity theft violations. He was living in Malaysia at the time of his arrest and, if convicted, faces 35 years in prison.

---


In January 2015, the Cyber Caliphate seized control of U.S. Central Command’s (CENTCOM) Twitter and YouTube feeds, posting propaganda videos and contact information for top military officials. In November, the same hackers seized more than 50,000 Twitter accounts and used them to spread their propaganda amongst the followers. These specific hacking events were a 1 day exploit for each operation, and the damage may be extensive because they identified the personal identifiable information of top military officials. This event occurred months after the Islamic State issued a statement calling for attacks on military and law enforcement personnel. “Though theatrical, these hacks did not produce physical damage and required little expertise. Seizing control of the CENTCOM Twitter feed, for example, was likely accomplished with a simple phishing attack — infecting the command’s network via a virus disguised in a legitimate email.”

On April 5, 2015, the Cyber Caliphate seized control of a French television network, TV5Monde, for several hours. The network labeled it as one of the highest-profile hacks of the year. When the station came back online, security was still so bad that they conducted an on-camera interview in front of a screen listing their system’s passwords. The Cyber Caliphate controlled 11 networks, along with the company’s website and social media accounts. The network had a message written in three languages - French, Arabic and English - including threats to the network and "a glorification of Sharia.” This type of attack shows the sophistication and expertise the Cyber Caliphate has on its hacking team. Yves Bigot, director of TV5Monde, said "It's been a very powerful attack, because we have very strong firewalls which had been checked and were said to be very safe, so obviously it's a very knowledgeable and powerful cyberattack.”

As the Islamic State continues to aspire to attack the homeland and Western interests abroad, the United States has implemented strategies in information warfare specific to the cyber spectrum to thwart this terrorist organization.

---


41 Ibid.


43 Ibid.
What could be done to prevent these incidents from happening in the future?

First, we must understand the enemy. The Islamic State is just a reflective part of a much older ideological movement with a more moderate and sophisticated information plan. We are currently losing this war and we will continue to lose if information is not wielded by the U.S. government. The U.S. government must launch their informational power tools to discredit and counter the Islamic ideology through various media campaigns; we are not going to kill or arrest our way out of this war. The Islamic State cannot match the U.S. tank for tank, plane for plane, therefore they have turned to cyber and lone wolf attacks; they use social media to task and/or motivate its followers to join their Caliphate and conduct lone wolf attacks throughout the world. There has to be living documents of digital communication and information warfare strategies in place that can be easily updated to keep up with the fast paced environment of cyberspace.

1.1 **INCREASE PUBLIC DIPLOMACY EFFORTS**

One of the most vital ways to use information as an instrument of power is through public diplomacy. The purpose of U.S. public diplomacy is to reach foreign public audiences with information and ideas that are influential enough to promote America’s ideals and liberties. The only difficult issue with engaging in public diplomacy efforts with the enemy is the religious element attached to their goals. The primary weapons needed in confronting the war of ideas are the Under Secretary for Public Diplomacy and Public Affairs, and broadcasting tools like the Voice of America and now social media platforms.

During the Cold War public diplomacy and international broadcasts were arguably the most influential instruments in fighting Communism. “At the height of the Cold War, the United States Information Agency (USIA) had a $1 billion dollar budget and around 10,000 employees. However, in 1999 the USIA had been abolished and its functions were dispersed to the Department of State (DOS) and the Broadcasting Board of Governors (BBG).” Under DOS, the Under Secretary of Public Diplomacy and Public Affairs inherited the information and education programs, whilst the BBG inherited all international broadcasting functions, including Voice of America; both are poorly underfunded and understudied. The BBG’s budget for fiscal year 2016 includes a “Countering the ISIL Narrative” with a Raise Your Voice campaign of a mere $3.4 million and Voice of America campaign of $2.4 million.  

---

Public diplomacy efforts should be developed with our Middle Eastern partners. The enemy is not going to listen to white Christian American’s telling them that their actions are wrong. The U.S. must work with Middle Eastern partners such as King Abdullah II of Jordan and President Abdel Fattah el-Sisi of Egypt to broadcast a more peaceful Islam.

1.2 **INCREASE FEDERAL, STATE, AND LOCAL PARTNERSHIPS IN CYBERSPACE**

The Department of Defense (DOD) has an unclassified version of its cyber strategy which lays out five initiatives to combat cyber threats. Additionally, congress has also introduced the Cyber Intelligence Sharing and Protection Act which “directs the federal government to provide for the real-time sharing of actionable, situational cyber threat information between all designated federal cyber operations” and “amends the National Security Act of 1947 to require the Director of National Intelligence to allow the intelligence community to share cyber threat intelligence with private-sector entities.” Both of these strategies are good documents to build upon for future strategic plans in defending cyber threats.

On the battlefield in Syria and Iraq, the DOD should utilize its Psychological Operations (PSYOPS) as its primary tool during physical deployments in international arenas. PSYOPS efforts should be enhanced with information warfare capabilities through military branches within US Cyber Command where soldiers now have the ability to defend our nation in cyberspace in support of PSYOPS missions to reach wider audiences. Information Warfare and PSYOP should be the primary tool in military planning, not an afterthought to military action. Military information warfare and action should be used in conjunction with each other but focused more heavily on the information campaigns, rather than prioritizing combat over information or vice-versa in war.

Additionally, sending troops into war, whether in the physical battlefield or virtual battlefield, without prior knowledge of the religion, culture, language, and ideology of the enemy will only lead to failure. Training troops in these areas prior to a deployment or enemy engagement is an important capability not only in defense planning, but for long-term success of defeating this threat.

The DOD should not work alone in its virtual efforts; the private sector also need to be refocused to have a counter-narrative campaign. “ISIS counter-narrative campaigns obtain more engagement and more views when they are distributed through non-government channels.” Both the government and private sector need to work with the moderate Muslim populations to help formulate the right messages to counter non-state groups. “Understanding values and belief

---


Since the internet is constantly changing, updating, and advancing, proactive thinking and alternative analysis thinking is a key capability to stay ahead of cyber threats. The DOD can ask all of the right questions, but they must have plans in place to counter any “what-if” scenarios and be prepared for any strategic surprises.

Trying to defeat radical Islamists solely with combat missions will not lead to long term results. Groups like the Islamic State are ideologically equipped to recover from such loses of personnel and equipment. Ariel Merari, a prominent Israeli expert on terrorism, noted that “for every terrorist killed or captured, there are 10 waiting to take his or her place.” Although, military efforts in the fight against the Islamic State should not be diminished, there is a need for additional strategies that focus strongly on enforcing the use of information as an instrument of power in the federal, state, and local levels to accompany military efforts.

1.3 Increase Social Media Exploitation

Although trying to find the next terrorist is like trying to find a needle in a haystack, social media platforms like Twitter and Facebook have security policies in place to remove any posts of threats of violent, or messages that promote violence, be it criminal or terrorism related content. Twitter and Facebook sometimes remove profiles from individuals if their threatening messages continue to trend. However, removing a Twitter or Facebook profile does not stop the individual; that individual is capable of creating another profile minutes after they realize the company shut down their existing one.

Social media exploitation and vetting should be incorporated into US visa policies for individuals who want to enter the United States from a foreign country. This incorporation into US policy could be an extra step in the efforts spot and prevent the next HVE from entering the United States to conduct an attack. However, as terrorists discover that law enforcement is incorporating social media vetting into their processes, they may delete their social media accounts, create a profile under alias, or make their profiles private until the application process is complete. These are security concerns that will have to be addressed during the policy implementation process, along with privacy concerns.

Conclusion

The underlying solution to address the current threat is for policy-makers to develop foreknowledge on how to counter and defeat the ongoing Islamic ideological message in order to properly succeed in the virtual and physical battlefields. There needs to be a foundation of knowledge in the eschatological themes in Islam, along with knowledge of the Quran, the Hadiths (words of the Prophet), and the texts of Islamic scholars that make up the foundation for jihad – such as the works of Sayyid Qutb, Abdullah Azzam, S.K. Malik, Ayman al-Zawahiri, and Anwar al-Awlaki – in order to start understanding the mindsets and goals behind these terrorists to strategically counter their messages on social media and decrease recruitment rates. Cyber makes it possible for our enemies to sabotage critical infrastructure without ever landing an operative on US shores.

We are not going to convince individuals that fighting for their God is wrong; we have to convince everyone else who may want to join or sympathize with the Islamic State that their world is not peaceful and that freedom exists. The majority of the Islamic State’s victims are Shia Muslims, therefore we should leverage that data and use it against them (i.e. the Jordanian pilot that was buried alive) and convince other Muslim’s that they could potentially be a target as well if they do not abide by the demands of the Islamic State’s laws.

Although coalition forces continue to make efforts in destroying the Islamic State in Syria and Iraq, their affiliate branches throughout the Middle East still remain strong. Coalition efforts may force Islamic State members to flee the area to join the Islamic State affiliate branches, or make their way to Europe. It is unknown whether or not Europe or the United States is prepared to handle the mass amount of refugees that may try to migrate into those nations to flee the coalition forces. Furthermore, coalition forces will not be able to stop the online messaging from the Islamic State, its supporters, and the civilians in Syria and Iraq who may be distraught about the coalition forces running their homes. Negative online messages from civilians’ only helps the Islamic State’s messaging by proxy that the United States and its partners are evil and should be destroyed.

So long as the radical Islamic propaganda is not countered, jihadists will always have a steady stream of potential recruits. “Though studying the jihadists on the ground and in the battlefield is a vital component to understanding their modus operandi, it is not the only place we must look for answers. We must examine the space where jihadism exists unabated: the internet, where they continue to form a unified online jihadist network that knows no physical boundaries.”

---


http://www.independent.co.uk/news/world/middle-east/isis-urges-more-attacks-on-western-disbelievers-9749512.html


Deen, Adam. “I used to be an Islamic Extremist. This is the Truth about how you Can Prevent Further Terror Attacks,” Independent News, 2016. http://www.independent.co.uk/voices/i-used-to-be-an-islamic-extremist-this-is-the-truth-about-how-you-can-prevent-further-terror-attacks-a7145816.html


