Combatting Cyberterrorism: Recognizing the Islamic State's Global Threat

Chas H Riley
University of Arizona
CYBV 498: Senior Capstone – Defense and Forensics
Professor Jordan VanHoy
April 7th, 2024

Abstract

This research paper delves into the extreme violence perpetrated by the Islamic State (IS) and the false claims of its destruction. The paper highlights that despite the efforts of the international community to eradicate IS, the group continues to be a significant threat to global security. One of the reasons for their continued success is their ability to adapt and become more efficient in cyber-attacks and propaganda dissemination.

This research paper argues that the Islamic State has become very effective in using social media to recruit new members and spread their message of hate and violence. This paper also emphasizes the need for open dialogue to combat radicalization and prevent vulnerable individuals from being drawn into the violent ideology of groups like the Islamic State.

This research paper concludes that the fight against Islamic State is far from over and requires a multifaceted approach. Governments and international organizations must take steps to counter the Islamic State's propaganda and recruitment efforts while also addressing the underlying social, economic, and political factors that contribute to radicalization. Additionally, individuals and communities must remain vigilant and engaged to prevent the spread of extremist beliefs. By working together, we can effectively combat the threat posed by Islamic State and other violent extremist groups.

Table of Contents

Introduction

Extremism Without Limits

On June 13th, 2014, Ali Kadhim and his other Iraqi army cadet peers received warning that 100 Islamic State (IS) fighters were encroaching their base located two hours north of Baghdad, Iraq. The recruits changed into civilian attire and attempted to flee, but they were captured. Almost 2,000 boys and men were stuffed into trucks and later lined up in front of freshly dug ditches (Erbil, 2014). Group after group, the brand-new cadets were shot to death by firing squads. When Ali Kadhim felt a bullet miss by inches from the back of his head, he fell forward, feigning death. Of the estimated 1,997 deaths during the Speicher and Badoush massacres, Ali was the only survivor. This act of terrorism is the deadliest in Iraq's history, and only second in the world after the September 11th attack in the United States (Arango, 2014).

The Islamic State is relentless in its pursuit to destroy all infidels at any cost. This among many other examples is the reason the Islamic State must be proactively resisted at all times through the spread of awareness and active prevention both physically and in cyberspace. Many experts from all fields of study are in agreeance that the cyber capabilities of IS are growing. The purpose of this paper is to raise awareness of the current threat the Islamic State possess, their rising cyber presence, and how to combat this cyber-extremism going forward. By identifying these capabilities and possible solutions, we will have a better understanding of how to combat this growing threat.

Who is the Islamic State?

On the night of November 13th, 2015, a concert held by the band “Eagles of Death Metal” at the Batalclan Concert Hall in Paris, France. At around 8:00 PM, an attendee named Benjamin Cazenoves posted a Facebook status update while in the packed concert hall. Translated from French to English, the post read, "I am still at the Bataclan. First floor. Gravely injured. They should storm the place as soon as possible. There are survivors inside. They are killing everyone. One by one. On the first floor, quick!!!!

In a coordinated attack, three teams made up of nine Islamic State members attacked multiple locations around Paris. Armed with automatic weapons, suicide vests and other explosives, the assailants killed around 130 and wounded another 494 (Lait et al., 2024). This attack was the first of many to be conducted in a western country. After the release of audio and written statements of the Islamic State claiming responsibility of the attack, the once unknown group was being discussed in all forms of media (Felbab-Brown et al., 2016).

Origin of the Islamic State

Since the World Trade Center terrorist attack of September 11th, 2001, the war on terror has lasted almost a little over 20 years. With the understanding that al Qaeda was responsible for the largest terrorist attack the world had ever seen, the United States response was immediate. Since the initial invasion of Iraq, the price of this 20+ year war cost the United States an estimated $8 trillion and 900,000 deaths (Kimball, 2021).

The 9/11 attacks had been orchestrated by the then al Qaeda leader, Bin Laden. These motives were made clear from Bin Laden’s “Letter to America” where he claimed the reasons for the attack were due to the presence to the United States military in Saudi Arabia and for the

unconditional support of Israel occupying the Palestinian territories. In the summer of 2001, al Qaeda's numbers were around 3,000 with a steady flow of new recruits, multiple training facilities, and a formal headquarters. This success led Bin Laden to believe that the group was capable of withstanding the US military and that the overall conflict would spread more radicalization and thus, bring about more members for al Qaeda. However, as soon as the Afghanistan invasion began in 2001 and the Iraq invasion in 2003, al Qaeda losses led to more decentralization until those in leadership positions within the group were forced to flee or be killed off (Saltman & Winter, 2014).

So where does the Islamic State fit into all of this? Al Qaeda and the Islamic State somewhat share the same origin story. There is a misconception that the Islamic State appeared as if out of nowhere in June of 2014. This is due to the notoriety the group received after seizing control of Mosul, Iraq. The roots of the Islamic State started with the al Qaeda ideology. Abu Musab al-Zarqawi formed a group that worked with al Qaeda, but eventually split off and officially started the Islamic State in Iraq or ISI. Even though ISI worked with and allied itself with al Qaeda in the beginning, the leaders of both had a different vision for what an Islamist state should be.

Osama Bin Laden believed in an outward-looking strategy that put focus on destabilizing the west before attempting to create their caliphate. A caliphate is an Islamic utopian society where the ruler or caliph is considered the political and religious successor to the prophet Muhammad in the Islamic faith. Although both leaders shared a very similar ideology based on jihadism and a violent interpretation of Islam, IS differed with the focus of their resources. The Islamic State instead wanted to focus inward to develop their caliphate first, before looking

globally. Their goal was to cleanse or purge Muslim-majority states of all impurities, which means anyone who didn't agree with or share their radical views.

The ISI successor, Abu Bakr al-Baghdadi, announced in April of 2013 that ISI would from then on be named ISIS or the Islamic State of Iraq and al-Sham. It was shortly after this time that ISIS and al Qaeda disagreed with the legitimacy of rule for the opposing group, which led to thousands of jihadists dying in the conflict. This short war undoubtedly confirmed the Islamic State as the more violent of the two groups (Saltman & Winter, 2014).

Terrorism vs Cyberterrorism

Born on October 28, 1991, Moner Abusalha, nicknamed Mo by his loved ones, grew up in Vero Beach, Florida with his mother, father, and his three other siblings. Friends and loved ones claim Mo had a great childhood. He grew up in a gated community, had a lot of friends, and was said to be outgoing and funny by his friends. Anyone who knew Mo knew his biggest passion was basketball. He played for a junior traveling team in his younger years and when he started high school, he made the school's basketball team. Interview after interview, the only statements made regarding Mo's character were centered around how nice, easy-going, normal, and good-natured he was (Robles & Fitzsimmons, 2014). In May of 2014, Mo made international news for committing an act of terror that no one could ever have foreseen.

On May 25th of 2014, a garbage truck is filmed driving over a hill and into a small collection of buildings. Moments later, the now unseen truck packed with 16 tons of explosives, detonates, killing himself and an unknown number of Syrian troops gathered at a restaurant. The 22-year-old Mo, who was once known to attend religious services with his parents consistently in his youth, had just committed a suicide bombing for the Islamic State.

How does an average young American adult drop out of college and leave their entire life behind to fight and die for a violent terrorist group? Days before Mo's attack, he was seen in a propaganda video for the extremist group stating, "I advise all American people to come and make jihad in Syria…Everyone should support the Syrian people." A close friend and veteran fighter told a journalist, "I think he came from the USA to Syria not because he's a Muslim, or because he has a jihadi mind-set — no. Just because he's human. His humanity pushed him to come to Syria and stop the injustice…I feel sad because I lost my friend, but I feel happy because he reached his goal: to die and enter paradise (Giglio, 2014)."

Understanding Terrorism

To understand cyberterrorism, we must first know the meaning of terrorism. Merriam-Webster (2024) defines terrorism as, "the unlawful use or threat of violence especially against the state or the public as a politically motivated means of attack or coercion." Understandably, this definition may sound a little ambiguous. Throughout the word's existence, the definition has changed over time. If you've ever heard the phrase, "one man's terrorist is another man's freedom fighter," then this ambiguity is understood. As is the trend throughout history, the titles affiliated with each group involved are usually assigned by the victor of said conflict. An example of this trend could be applied to the American Revolution where colonists would have been considered terrorists if the war against Britain was lost. Instead, history looks at the conflict as the victor group being patriotic freedom fighters who overthrew a tyrannical government.

Realistically speaking, terrorism has existed since the beginning of mankind. However, the word "terrorism" wasn't officially added to the English language until 1840 by Noah Webster. During this period, the gruesome "Reign of Terror (1793-1794)" was started by the

newly established French government after the French Revolution. Terrorism was used to describe those who acted against, disagreed with, or were even thought to have disagreed with the French government. Anyone deemed a terrorist by the government were primarily killed by the guillotine during mass executions (Merriam-Webster, 2024).

In modern times, an important distinction between an act of war and an act of terrorism is who the violence is acted out upon. Violence that targets the public or innocent people with the intent to cause fear and/or destruction would be considered a terroristic act. Whether the act is politically motivated, religiously motivated, or even motivated by senseless hatred, the act of violence can still be considered terrorism. There are many examples of the Islamic State committing terrorism on a large scale and on a small scale. Whether it's dispersing videos of civilians being beheaded to spread fear and discontent or suicide bombings meant to kill hundreds at a time, the Islamic State has committed many atrocities. The Syrian Observatory for Human Rights (SOHR) has even compiled a list of just the executions of the Islamic State and show that the group has executed 4,144 people in just under two years. In this compiled list, a majority of these executions include beheadings, shootings, stoning, throwing people off of rooftops and setting people on fire (Dearden, 2016).

Understanding Cyberterrorism

With the basic understanding of terrorism, cyberterrorism is a much easier concept to grasp. However, we must know the cyber realm is in order to make a distinction between the two. As the world advances technologically, so do the capabilities of those who have access to it. With the creation of the internet, virtual space, also known as cyberspace, was also created. The U.S. Army War College (Hillebrand & Ault, 2023) defines cyberspace as, "A global domain

within the information environment consisting of the independent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (p. 206).”

Cyberspace is a complex environment with a lot of complicated, but necessary moving parts. Simply put, cyberspace is a virtual world that is found on the internet. People all over the world can communicate, share ideas, learn new ideas, or interact with anything or anyone also connected to the internet. This tool has granted anyone with access to the internet almost unlimited information in seconds. This new age of information has led to new rapid advancements, but also new dangers. Criminal activity and terrorism have a similar relationship to their cyber counterparts.

What separates a physical criminal act, and a cyber-criminal act is the significant downside of a perpetrator being able to cause this damage while being anywhere in the world that has an internet connection. Also, when it comes to terrorism vs cyberterrorism, terrorism can have a lot of grey areas, while cyberterrorism is a little more black and white. This is due to the laws and measures put into place that prevent cyberterrorism. To bypass these security measures, cybercriminals must actively do so with hostile intent. Without knowledge or intent, a willing individual cannot accidentally commit a cyber-attack that would result in cyberterrorism.

An individual or team can initiate a cyber-attack in many ways. For the cyber-attack to be successful, an attacker must bypass the preventive security measures put in place by the intended target. A simple comparison could be a robber vs a safe. A simple safe requires less knowledge and skill, while a bank safe requires a lot of knowledge and just as much skill.

This same concept can be applied to other crimes. Just like the physical-attack counterpart, the type of cyber-attack can vary based on the attacker's goal. Instead of just robbing the bank, a cyber attacker may want to make the bank inaccessible for its' customers. Maybe the attacker only wants to steal information without the bank's knowledge. Minimal experience in the cybersecurity realm will undoubtedly lead some to believe that an attack in cyberspace is not as damaging as a physical attack. However, a cyber-attack could result in just as much, if not more damage than a physical act of terrorism.

The U.S. Army War College (Hillebrand & Ault, 2023) defines a cyberspace attack as, "actions taken in and through cyberspace that create denial (i.e., degradation, disruption, or destruction) or manipulation effects in cyberspace and are considered a form of fires (p. 206)." This means that a cyber-attack against a person, organization, a government body, or the people of that government body, is considered just as illegal as a physical attack. Since a cyber-attack is considered an act of violence, as long as the threshold of terrorism is met, the cyber-attack is considered an act of cyberterrorism.

Into the Fog of Cyber War

On May 8th, 2021, a large explosion is heard by Mohammad Taqi, a nearby resident of the Dash-e-Barchi neighborhood. Moments later, there was a second explosion, and then a third. Without hesitation, Mohammad rushed towards the direction of the explosions. The bombs went off just outside of the Sayed Al-Shuhada school, a girls' school located in Kabul, Afghanistan. The first bomb was placed in a vehicle next to the school, the second and third bombs were placed to target the children as they exited the school to seek safety, a common tactic for the Islamic State.

Upon arriving, Mohammad describes what he saw to the reporter. “Suddenly I found myself amongst bodies. Hands and heads were cut off [severed by the explosions]. Bones were smashed. All of them were girls. I saw dead bodies piled on top of each other.” Another impactful statement given to reporters that day came from an uncle of one of the victims. “She was 15 years old…she was very intelligent and didn’t miss a single day of school. Yesterday, her mother told her not to go to school, but she said no, I will go today, but I will not go tomorrow. She told the truth, and [now] we buried her here today.” Mohammed Reza Ali, a volunteer helping the victims and their families also stated, “The entire night we carried bodies of young girls and boys to a graveyard and prayed for everyone wounded in the attack…Why not just kill all of us to put an end to this war?”

A majority of the casualties were young girls. In the country of Afghanistan, the claims of the civilian population and the trend of insurgent groups targeting women, female educational and healthcare institutes, points towards these terrorist groups hatred towards the education of girls. In this particular attack, the original total of deaths was set to 50 because some of the children were so close to the first blast that their bodies were completely destroyed. The total death count was increased when parents were unable to find their children at any of the hospitals in the area that had taken in victims. Because of this, Afghan officials later raised the number of dead to 85 and the number of injured to 147 (Deaton & McKenzie, 2021).

Known Cyber-Attacks of the Islamic State

Shortly after NATO forces expelled the Islamic State out of Iraq in December of 2017, the Hellenic Institute of Strategic Studies (HISS) collected and analyzed cyber-attacks and trends. The goal was to identify the then current cyber capabilities of IS, as well as predict

possible capabilities in the near future. Summarizing the findings of HISS, the Islamic State has modernized and adapted well to the cyber-landscape. Compared to its terroristic predecessors and affiliates, the Islamic State is the most active and proficient terrorist organization in cyber-space. This proficiency has led to the group not only becoming cyberterrorism pioneers but has also forced NATO countries to increase their cybersecurity efforts.

Junaid Hussain, a radicalized British-born 15-year-old, created a pro-Islamic State hacker team known as, "Team Poison". In 2012, this team was able to hack its' way into Britain's Defense Ministry, multiple accounts of NATO members on Facebook, and other NATO accounts on government websites. With the information they were able to pull from these accounts, the hacker team stole bank account information, and enough personal information to dox as many government officials as well as their families (Giantas & Stergiou, 2018).

In 2013, Hussain officially joined the Islamic State and became one of the propaganda leaders of the group. The same year, Hussain also created a hacker collective known as Cyber Caliphate or the Cyber Caliphate Army (CCA). One of the significant attacks of CCA occurred in mid-2015 when they hacked into multiple social media accounts that were owned by US CENTCOM. Through these hacked social media accounts, they released videos that threatened infrastructure crippling cyber-attacks as well as propaganda. These unsubstantiated claims suggested that the terrorist group was capable of hacking into and spying through western communication systems. In the released video, the unknown individual states, "Praise to Allah, today we extend on the land and in the internet. We send this message to America and Europe. We are the hackers of the Islamic State, and the electronic war has not yet begun…What you have seen is just a preface of the future. We are able until this moment to hack the website of the

American leadership and the website of the Australian airport and many other websites…The electronic war has not yet begun (Paganini, 2015)."

There have been other occasions when the Cyber Caliphate has hacked into US CENTCOM accounts. In 2015, the CCA hacked into CENTCOM's Twitter and YouTube accounts. The group then uploaded propaganda videos to the YouTube channel and tweeted phrases such as, "AMERICAN SOLDIERS, WE ARE COMING, WATCH YOUR BACK. ISIS.", and "i love you isis." That same year, Hussain was killed in Syria from an airstrike. Siful Haque Sujana, a computer systems engineer in the United Kingdom, replaced Hussain's position. Access to educated individuals is a testament to the Islamic State's talent pool (Giantas & Stergiou, 2018).

In an article by Andrew Griffin (2015) and published by "Independent", an online news source company based in the UK, the cyber proficiency of the Islamic State can also be seen in their orchestrated denial-of-service (DoS) cyberattacks against 19,000 French websites. These DoS attacks were claimed to be in response to mass demonstrations of protests against the recent Paris shootings of the newspaper company "Charlie Hebdo" in January of 2015. This newspaper company is well known for their satirical articles and illustrations. Two Islamic State terrorists attacked "Charlie Hebdo" for its' satirical depiction of the leader of Daesh, Al-Baghdadi (Seelow, 2015).

Soren Seelow (2015) covered the killings in their article, "Charlie Hebdo attack: 'You will pay because you insulted the Prophet'." On the morning of January 7th, 2015, two hooded men wearing bulletproof vests and armed with military style rifles, burst into the company's regularly scheduled meeting. In the span of a few minutes, seven cartoonists and editors, two

police officers, the building's maintenance worker, and two other invited guests were killed in the attack.

Videos recorded from bystanders capture the assailants saying phrases such as, "Allahu Akbar," "You will pay, because you insulted the Prophet," and "We avenged the Prophet Mohamed, we killed Charlie Hebdo!" The worst moment captured on video shows police officer Ahmed Merabet falling to the ground after being presumably shot. As the hooded men approach the officer on the ground, one of the men is heard saying, "You want to kill us?" Officer Merabet is then heard saying, "No, I'm good, boss." The man who asked the question then shoots Officer Merabet in the head (Seelow, 2015).

Possible Future Scenario

As the Islamic State's cyber capabilities improve, so does the potential damage of their attacks. Although the next example of attacks listed below were not executed by IS specifically, these attacks are examples of what IS could be capable of in the near future. The only limiting factors are their access to resources like funding and the recruiting of field experts. However, based on trends since the group's founding, both resources are attainable. IS has constantly recruited experts from many different fields and has had access to financial gain through criminal activity with the seizing of banks, oil refineries, extortion, and looting (Neumann et al., 2017).

Even the Neumann's article, "Caliphate in Decline: An Estimate of Islamic State's Financial Fortunes," which argues against the high figures of financial success of the Islamic State, still confirms their financial success over the last few years. This counterargument study still confirmed that IS was generating $435 to $550 million from oil refineries in 2015, $20 to $40 million from kidnapping ransoms in 2014, $500 million to $1 billion from looting,

confiscations, and fining the local population also in 2014. This article states that those amounts have decreased since their loss of territories, which is a reasonable conclusion. The point of this success is to reasonably assume that IS is capable of generating wealth, which the group has successfully generated in the past. Although IS generates lesser amounts today, they are still wealthy and capable of acquiring more.

Russian Hackers vs Department of Homeland Security (DHS)

In late 2014, a "Trojan Horse" malware program was inserted into the system that runs many of the United States' critical infrastructures. The Department of Homeland Security stated that this malware was coded to cause economic catastrophe by controlling the critical processes of wind turbines, nuclear power plants, power transmission grids, oil pipelines, and gas pipelines. National Security sources spoke to reports about the source of this almost catastrophic malware. After discovery of the attack by multiple companies affiliated with the attacked infrastructures, the code was analyzed and identified as the malware "BlackEnergy" (Paganini, 2014).

The Security Affairs article also claim that BlackEnergy was created by a Russian hacker with the purpose of making bank frauds, distributing spam, and preforming DDoS attacks. This new variant has been altered to target government entities and private companies that benefit the overall country's important infrastructures. Reports by ESET, a leading cybersecurity firm, has found this new variant of BlackEnergy targeting over 100 government and related organizations in just Poland and the Ukraine. US National Security sources also confirmed that this new variant was sponsored by the Russian government but did not go into more detail due to national security reasons.

The experts in charge of assessing the current and the potential damage insist that if this attack against critical infrastructure were to be successful, there would be, “serious risk for the stability of any government, the damages could be of different nature, including huge economic losses and losses of human lives (Paganini, 2014).” The most alarming news about these attacks is the malware had successfully made entry into the White House’s internal network. Even after making a successful entry, the White House staff only noticed the attack after reports from other related entities reported attacks. This attack on a massive scale, could have resulted in the catastrophic societal collapse of the United States for an unknown amount of time.

Is the Threat Over? Deniers vs. Sceptics

There is a misconception that the Islamic State is either no longer a threat or no longer exists, but there is strong evidence and agreement among experts that support the counterclaim that IS presence is still felt around the globe. Yes, IS has been weakened since their territory losses in Iraq and Syria back in 2017. Although IS was in a temporarily weakened position, the Islamic state is continuing to strengthen once again. This strengthening can also be attributed to their cyber capabilities and presence. On many occasions, prominent political figures have claimed that the Islamic State has been wiped out or defeated. Examples of this claim have been pushed to the public for political gain, have been misquoted to support an agenda, or the notion has been relayed for views by news networks.

On the 16th of January in 2019, Vice President Mike Pense claimed, “Thanks to the leadership of this commander in chief and the courage and sacrifice of our armed forces we’re now actually able to begin to hand off the fight against ISIS in Syria to our coalition partners, and we’re bringing our troops home. The caliphate has crumbled, and ISIS has been defeated

(Samuels, 2019).” On that same day, and a few weeks after President Trump claimed that ISIS was defeated, the Islamic State killed American troops in Syria with an IED (O'Keefe, 2019). In August of 2020, on the third day of the 2020 Republican National Convention, Republican representative from Texas Dan Crenshaw stated, “The defeat of ISIS was the result of America believing in our heroes, our president having their backs and rebuilding our military, so we'd have what we needed to finish the mission (Kapur, 2020).”

On November 21st, 2017, The Kurdish-led Syrian Democratic Forces (SDF) made a statement that claimed that the caliphate of the Islamic State “is over” after the terrorist group’s defeat in Syria (BBC, 2019). On the same day, Iranian President Hassan Rouhani also declares that the Islamic State is no more (Glenn et al., 2019). The SDF once again claims IS had been destroyed on March 23rd, 2019. On April 21st, a few weeks later, Islamic State suicide bombers killed at least 250 people in the three cities Colombo, Negombo, and Batticaloa of the country Sri Lanka. At 5:44 AM on Dec 9, 2017, the Iraqi Prime Minister Haider Al-Abadi made a tweet on “X” (formerly known as Twitter) also declaring victory over the Islamic State (Glenn et al., 2019).

Even with the constant push for a narrative that the Islamic State is no more, there are many examples of experts and political representatives’ giving statements that contradict these assertions. Anthony H. Cordesman (2020), the former Emeritus Chair in Strategy, cites reports from the U.S. Central Command (US CENTCOM). These unclassified reports show the Islamic State of Iraq and Syria (ISIS) activity patterns are indicating that ISIS is becoming even more active. Cordesman dissects the quarterly full Operation Inherent Resolve (OIR) report for April 1, 2020, through June 30, 2020, and backs his argument by quoting the report. “One research organization’s assessment in May said that the spike in ISIS attacks in the first half of the quarter

had “raised new fears about the revival of the group,” and appeared to be “early signs of an ISIS recovery.”

Cordesman (2020) also goes on to explain as U.S. forces continued to drive ISIS forces out of Iraq and Syria, the local governments were unable to recover and maintain control of reclaimed regions. This once again created more power vacuums as American forces continued to prepare for an eventual withdrawal from both countries. This argument is strengthened by the DOS (U.S. Department of State) reported in 2019. This report shows government failures in both Iraq and Syria. Both populations suffer from mass displacement, financial and physical insecurity, high unemployment, humanitarian crises, and access to basic services. In this report, the DOS stated, “(this situation will) leave ordinary civilians vulnerable to recruiting by ISIS and other extremists.”

Cordesman’s (2020) in his closing statement argued that “Tactical successes against terrorist movements do not defeat terrorism. ISIS is no exception. It is still active in Syria, Iran, and other countries. Furthermore, U.S. official intelligence and military reporting makes this all too clear, regardless of political claims to the contrary. So does the historical record… the ability of terrorists and extremists to exploit the Internet and global media remains a serious tool for terrorism and extremism that goes far beyond national boundaries and any given terrorist or extremist organization.

On March 7th, 2019, General Joseph Votel, the US CENTCOM commander at the time, spoke in front of Congress. During this testimony, General Votel warned that the Islamic State was bidding their time with a “calculated decision to preserve the safety of their families and preservation of their capabilities by taking their chances in camps for internally displaced persons and going to ground in remote areas and waiting for the right time to resurge (Glenn et

al., 2019).” A few weeks prior to Rep Dan Crenshaw’s IS remarks at the 2020 Republican National Convention, in an article published by the U.S. Department of Defense, Marine Corps Gen. Kenneth F. McKenzie Jr. stated, “While ISIS no longer has the ability to hold ground, the terrorist organization isn't completely defeated (Kapur, 2020).”

The need to downplay a danger is common among those in leadership positions. This idea can be applied to many situations. A leader’s attitude is contagious. When a leader panics and is unsure of themselves, this spreads to everyone else. A leader who is cool, calm, and confident, provides comfort and instills confidence from subordinates. However, in this context there is a tradeoff. Downplaying a threat can lead to a societal shift towards ill-preparedness. Consequences can also occur from overexaggerating a known threat, which would lead to a society reacting out of fear rather than rational thought.

There must be a middle ground. The safety of the masses must take precedence over an election. The Islamic State can receive a mighty blow, while also staying a threat. Just because the cameras aren’t recording the violence, doesn’t mean it’s not happening daily. Censoring conversations and making empty claims will not make the threat go away. In October of 2019, Lindsey Graham made a statement that summed up the point of my argument perfectly. The Republican representative of South Carolina, told Fox News in an interview that, “The biggest lie being told by the administration is that ISIS has been defeated (Kapur, 2020).”

Combatting the Reach of the Islamic State

Through the examination of the Islamic State’s ability to adapt with the growth of the internet and the incorporation of cyberterrorism tactics, we need to be proactive in our approach to combat this growing threat. The current model the western world has adopted is censorship

and the wild assumption that if we don't talk about the danger, it cannot hurt us. This corrective course of action is demonstrated constantly with how the media handles dangerous ideologies online.

In early 2016, the Sons Caliphate Army (SCA), a subgroup of the Cyber Caliphate, claimed credit for more than 15,000 cyber-attacks against both Twitter and Facebook accounts. Zuckerberg gave an interview at the Mobile World Congress in Barcelona regarding extremist groups like the Islamic State on social media platforms like Facebook. In his speech he stated, "If we have opportunities to basically work with governments and folks to make sure that there aren't terrorist attacks then we're going to take those opportunities and we feel a pretty strong responsibility to help make sure that society is safe." Zuckerburg ensured that Facebook would continue to remove posts that the social media services say incite violence and promote terrorism, as well as the accounts that made those posts. Twitter also followed suit earlier that month as it suspended 125,000 accounts connected to the Islamic State. Both social media platforms also plan to improve the algorithms coded to find harmful posts made by groups like the Islamic State (Guynn, 2016).

In the same USA Today article, "Islamic State video makes direct threats against Mark Zuckerberg, Jack Dorsey," Veryan Khan, the president and CEO of the Terrorism Research & Analysis Consortium (Trac) was asked to respond. She stated, "though Twitter may have made a dent, the bounce back for the Islamic State will be fairly effortless…The Islamic State has been preparing their sympathizers for this type of event. Loads of 'Just Paste Its' and 'Dump To' bins as well as 'how to' videos have been circulating over this month on how to create dozens of backup accounts easily including creating false working phone numbers for those using Tor (Guynn, 2016)."

In Saltman & Winter's (2014) article "Islamic State: The Changing Face of Modern Jihadism," their team created and analyzed the statistics surrounding the propaganda that was disseminated by IS on social media platforms. There were two methods that IS used in conjunction that allowed propaganda to be shared in mass.

First, IS has a better understanding of the algorithmic code than the social media platforms that created the code and they have found multiple loopholes to exploit the codes' vulnerabilities. IS was able to exploit hashtags by using them discreetly to identify the post as IS material, and then the post would be tagged to hijack trending topics to reach users all over the world. An example of this is IS using the hashtag "#Brazil_2014" during the football world cup.

Secondly, IS members were found to have developed complex coding and incorporated that coding into smartphone apps. With apps such as "Dawn of Glad Tidings," which was designed to access Twitter, anyone who downloaded this app from the Google Play Store for .99 cents would automatically have their own personal Twitter account synchronized to IS users without their knowledge. The designated IS user could then post from these hijacked Twitter accounts freely and in mass. This in combination with using attached links, hashtags, and images to avoid triggering algorithms that detected spam. Before Google became aware of the apps' existence, J. M. Berger reported that the amount of propaganda disseminated by IS propaganda was immense. In a single day, IS tweeted almost 40,000 posts.

Another example that further shows that IS is capable of defeating social media platform coding is when the team was able to track and account becoming banned and then recreated for the 21st time. With this recreation of the account, it was easily able to re-amass 20,000 followers. This was not the first account that was identified doing this. Jihadism researcher Pieter van Ostaeyen after seeing how often this process occurred stated, "IS supporters on social media are

like mushrooms in a moist meadow – you pluck one, only for four to replace it." This finding and the response of the team only highlight how ineffective the preventive measures of these social media platforms are at blocking or filtering out content from groups like IS.

Saltman & Winter's (2014) also highlights a factor that sets IS above all other terrorist organizations past and present, Islamic State sympathizers. Throughout IS' presence online, the group has convinced many people to leave their own countries to join their fight in the Middle East. The group has also gained followers all around the globe with computer science knowledge and expertise that create, and share IS propaganda from all over the world.

Addressing the Problem

With the rapid advancements of AI and AI-powered algorithms, even with unfathomable information available to each of us, the information that is the most available can be the most dangerous. With the age of information, conspiracies are on the rise. Once an individual takes interest in an idea that sounds unfounded to the majority, an unfortunate domino effect occurs. Simply clicking a video on a social media platform takes the user down a rabbit hole of inconsistencies lacking both correlation and causation. Very quickly, a user can find themselves in an echo chamber filled with others just as vulnerable. These easily accessible, yet highly isolated places are a breeding ground for distrust or even animosity towards others who do not share the same beliefs as the group.

Individuals that are directionless or lack purpose or self-esteem are vulnerable here. Echo chambers like these could result in beliefs such as the Earth being flat, or the moon landing being faked. Even worse, these spaces could create a tribalistic responsibility to punish those who have

wronged the group. As outlandish as this claim may sound to some, there is evidence to support this claim.

Videos such as the one made about Moner “Mo” Abusalha have been and are still being made with the intent to recruit impressionable new members from all over the globe. Recently on October 20th, 2023, Benjamin Carpenter from Knoxville, Tennessee, was convicted of domestic terrorism for his part in translating, producing, and distributing propaganda for the Islamic State (Barnes, 2023). In 2018, the International Centre for the Study of Radicalization (ICSR) surveyed 80 different countries and concluded that there were 41,490 people affiliated with the Islamic State in just Iraq and Syria. Around 20% of those people, or 7,366 people, were recorded returning to their home countries or were in the process of returning. By 2018, data also showed that around 4,300 attacks were carried out in at least twenty-nine different countries by Islamic State affiliates (Cook & Vale, 2018).

How is IS successfully recruiting members from foreign countries? The propaganda IS produces targets those who share commonalities. According to Paula Las Heras (2022) from Global Affairs, the largest contributing factors that online recruited members share is adolescence, the lack of friendships, the need to belong, a need for social recognition, and a lack of meaning or value for their own existence. IS members prioritize these traits when seeking those to radicalize. The most common tactic among IS recruiters is to develop a relationship with the adolescent. Their claim that social media recruits more IS members than any other method is shown in the statement, “In 2007, the Saudi Interior Ministry claimed that 80 per cent of all young Saudis who had been recruited by jihadists in the country had been recruited using the internet (Heras, 2022).”

In Lauren Williams article (2016), “Islamic State propaganda and the mainstream media, Williams claims there are three idealized Islamic principles that IS is trying to relay to potential recruits. The recruitment videos should portray daily Islamic life as utopian in nature. To relay this, the videos will show three different narratives either separate or together. The narratives are persecution, brutality, and utopianism. Persecution shows how the world has wronged IS while brutality aims to do two things, the first is to desensitize viewers and the second is to convince those who are already desensitized.

For utopianism, the videos would have happy, healthy children playing, sophisticated infrastructures like schools and hospitals, and westerners talking about how great everything is. An example of this is a 15-minute-long video recorded in what appears to be a state of-the-art hospital. Dr. Tareq Kamleh, an Australian pediatrician who left Australia to join IS in the Syrian city of Raqqa, talks about how great IS is and how others should join him to make a difference (YouTube, 2015).

FBI Director James B. Comey stated on July 14, 2016, that unlike other groups, ISIL has developed a narrative that encompasses all aspects of life, including career opportunities, family life, and a sense of community. This message is not aimed only at those who are openly showing signs of radicalization but is also viewed by many who browse the internet daily, engage in social media, and receive push notifications. Ultimately, several of these individuals are looking for a feeling of inclusion and may not have the intention of engaging in terrorist activities. (FBI, 2016)

Propaganda and its’ ability to recruit members is undeniable. To further support the notion that IS propaganda is radicalizing foreign internet users, Giantas & Stergiou (2018) collected data on dispersed propaganda online and attacks that were attributed to IS around the

world. With their findings, they concluded that internet propaganda “has conducted or inspired more than 140 terrorist attacks in 29 countries other than Iraq and Syria which cost the lives of 2,043 people and injured thousands more. Social media alone has allowed ISIS to glorify their agenda in a positive light while villainizing western culture.”

Conclusion

From the three sources reviewed, three things are clear. Firstly, the Islamic state has not been destroyed. They are actively conducting operations in many countries around the globe, and they are still recruiting new members. Secondly, IS has not and will not stop until their enemies are defeated. Even by the Quran standards of not killing the innocent, they do not count “infidels” or those who have different beliefs as innocent. They have shown that innocent human life is not valued, and their goal is to cause as much destruction as possible without the fear of even death. Lastly, IS is highly organized and ruthlessly effective. Among terrorist groups, IS continues to raise the bar when it comes to terrorism and cyberterrorism. The damage caused and complexity of their cyber-attacks continue to grow.

The cyberterrorism of the Islamic State has two main components: recruitment and creating fear. Combatting or even countering the cyber acts of the Islamic State requires a very complex solution. The answer to this problem is a difficult one that cannot be solved overnight. With that said, the method currently in effect is a mixture of disinformation and censorship from western society. The radicalization rate among the general population cannot be stopped through online censorship. For the same reason that executing those with opposing views creates a stronger opposition through martyrdom, censoring propaganda only leads to animosity and newfound skepticism from now potential recruits. To defeat a harmful idea or ideology, the

dogma must be placed in the spotlight. Scholars arguing or discussing the fallacies of the IS belief system will never have the same repercussions as a curious mind looking for an answer in an echo chamber that promises to give their life meaning.

Combating cyberterrorism with online censorship is just ineffective and even counterproductive. Propaganda at any point in history has never been defeated by not talking about it. Just like the examples I listed above, the radicalized are only reverted after they see the truth. More often than not, it usually takes those individuals witnessing the violence of the Islamic State before reality takes hold and regret sinks in. Discussing the realities of terrorism is a hard concept to be honest about. Modern political tribalism sets the standard for disingenuous half-truths. This constant dishonesty has led many people to question the validity of the government and powers meant to protect. If those in charge of society are shown to constantly lie to get ahead, how can we expect those that are lied to, to know when they hear the truth? To stop the spread of radicalization, more than just the government and military need to have open conversations about this growing threat.

References

Arango, T. (2014, September 4). *Escaping death in northern iraq*. The New York Times. https://www.nytimes.com/2014/09/04/world/middleeast/surviving-isis-massacre-iraq-video.html

Barnes, R. (2023, October 20). *Federal jury convicts Knoxville Man of Terrorism Charge*. Eastern District of Tennessee | Federal Jury Convicts Knoxville Man Of Terrorism Charge | United States Department of Justice. https://www.justice.gov/usao-edtn/pr/federal-jury-convicts-knoxville-man-terrorism-charge

BBC. (2019, March 23). *Islamic State Group defeated as Final Territory lost, US-backed forces say*. BBC News. https://www.bbc.com/news/world-middle-east-47678157

Cook, J., & Vale, G. (2018). *From Daesh to 'Diaspora': Tracing the Women and Minors of Islamic State*. International Centre for the Study of Radicalisation (ICSR). https://icsr.info/wp-content/uploads/2018/07/Women-in-ISIS-report_20180719_web.pdf

Cordesman, A. H. (2020, September 9). *The real world capabilities of Isis: The threat continues*. CSIS. https://www.csis.org/analysis/real-world-capabilities-isis-threat-continues

Dearden, L. (2016, April 30). *ISIS has executed more than 4,000 people in less than two years*. The Independent. https://www.independent.co.uk/news/world/middle-east/isis-has-executed-more-than-4-000-people-in-under-two-years-of-the-islamic-state-in-syria-a7007876.html

Deaton, J., & McKenzie, S. (2021, May 10). *Death toll rises to 85 in Afghanistan girls' school bomb attack*. CNN. https://www.cnn.com/2021/05/09/asia/afghanistan-girls-school-attack-intl-hnk/index.html

Erbil, R. (2014, November 1). *Official statistics: 1997 Total number of missing Speicher and Badoush massacres*. Rudawarabia.net. https://www.rudawarabia.net/arabic/middleeast/iraq/011120148

FBI. (2016, July 14). *Worldwide threats to the homeland: ISIL and the new wave of terror*. FBI. https://www.fbi.gov/news/testimony/worldwide-threats-to-the-homeland-isil-and-the-new-wave-of-terror

Felbab-Brown, V., Maloney, S., & Alaaldin, R. (2016, July 28). *The evolution of terrorist propaganda: The Paris attack and Social Media*. Brookings. https://www.brookings.edu/articles/the-evolution-of-terrorist-propaganda-the-paris-attack-and-social-media/

Giantas, D., & Stergiou, D. (2018). From Terrorism to Cyber-Terrorism: The Case of ISIS. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3135927

Giglio, M. (2014, August 7). *One man's journey to become the first American suicide bomber in Syria*. BuzzFeed News. https://www.buzzfeednews.com/article/mikegiglio/one-mans-journey-to-become-the-first-american-suicide-bomber

Glenn, C., Nada, G., Caves, J., & Rowan, M. (2019). *Timeline: The rise, spread, and fall of the islamic state*. Wilson Center. https://www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state

Griffin, A. (2015, January 15). *France has been hit by an unprecedented 19,000 cyberattacks since the Paris shootings*. The Independent. https://www.independent.co.uk/tech/charlie-hebdo-france-hit-by-19-000-cyberattacks-since-paris-shootings-in-unprecedented-hacking-onslaught-9980634.html

Guynn, J. (2016, February 25). *Islamic state video makes direct threats against Mark Zuckerberg, Jack Dorsey*. USA Today. https://www.usatoday.com/story/tech/news/2016/02/24/facebook-mark-zuckerberg-twitter-jack-dorsey-isil-video-threats/80861126/

Heras, P. (2022). *How ISIS recruits its members. Global Affairs. University of Navarra*. Global Affairs. https://en.unav.edu/web/global-affairs/como-recluta-el-isis-a-sus-miembros

Hillebrand, G., & Ault, B. (2023, December). *Strategic Cyberspace Operations Primer*. Center for Strategic Leadership. https://csl.armywarcollege.edu/USACSL/Publications/Strategic_Cyberspace_Operations_Guide.pdf

Kapur, S. (2020, August 27). *Updates and analysis from day 3 of the Republican National Convention*. NBCNews.com. https://www.nbcnews.com/politics/2020-election/blog/2020-08-26-rnc-updates-n1238051#ncrd1238313

Kimball, J. (2021, September 1). *Costs of the 20-Year War on terror: $8 trillion and 900,000 deaths*. Brown University. https://www.brown.edu/news/2021-09-01/costsofwar

Lait, M., Jafari, S., & DiCarlo, P. (Eds.). (2024, March 27). *ISIS Fast Facts*. CNN. https://www.cnn.com/2014/08/08/world/isis-fast-facts/

Merriam-Webster. (2024). *The history of the word "terrorism."* Merriam-Webster. https://www.merriam-webster.com/wordplay/history-of-the-word-terrorism

Neumann, P., Heibner, S., Holland-McCowan, J., & Basra, R. (2017). *Caliphate in decline: An estimate of Islamic State's financial fortunes*. Caliphate in Decline: An Estimate of Islamic State's Financial Fortunes | START.umd.edu. https://www.start.umd.edu/publication/caliphate-decline-estimate-islamic-states-financial-fortunes

O'Keefe, E. (2019, January 16). *U.S. troops killed in Syria suicide attack claimed by Isis*. CBS News. https://www.cbsnews.com/news/us-troops-reportedly-killed-syria-suicide-attack-isis-today-2019-01-16/

Paganini, P. (2014, November 8). *Russian hackers infiltrated many US critical infrastructure*. Security Affairs. https://securityaffairs.com/29977/cyber-warfare-2/russia-hacked-us-critical-infrastructure.html

Paganini, P. (2015, May 17). *ISIS cyber caliphate hackers are threatening Electronic War*. Security Affairs. https://securityaffairs.com/36883/cyber-crime/cyber-caliphate-electronic-war.html

Robles, F., & Fitzsimmons, E. G. (2014, May 31). *Before syrian suicide blast, a quiet life in the suburbs*. The New York Times. https://www.nytimes.com/2014/06/01/us/Moner-Mohammad-Abusalha-Vero-Beach-Florida-Syria.html

Saltman, E. M., & Winter, C. (2014). *Islamic state - the changing face of modern jihadism*. International Centre for the Study of Radicalisation (ICSR). https://www.goodreads.com/book/show/24262950-islamic-state---the-changing-face-of-modern-jihadism

Samuels, B. (2019, January 16). *Pence says "ISIS has been defeated" hours after attack that killed US troops in Syria*. The Hill. https://thehill.com/homenews/administration/425640-pence-says-isis-has-been-defeated-hours-after-attack-that-killed-us/

Seelow, S. (2015, January 8). *Attentat à " Charlie Hebdo " : " vous allez payer car vous Avez insulté Le prophète "*. Le Monde.fr. https://www.lemonde.fr/societe/article/2015/01/08/vous-allez-payer-car-vous-avez-insulte-le-prophete_4551820_3224.html

Williams, L. (2016, February 26). *Islamic State Propaganda and the mainstream media*. Lowy Institute. https://www.lowyinstitute.org/publications/islamic-state-propaganda-mainstream-media

YouTube. (2015, April 25). *Isis Propaganda Video Claims State of the Art Health Care*. YouTube. https://www.youtube.com/watch?v=sgKVZrk3X_Q