Pepperdine Policy Review

Volume 16 Article 8

4-23-2024

The Rise of ISIS: A Growing Threat to the World

Grace Ralstin
Pepperdine University, gracieralstin@icloud.com

The Rise of ISIS:

A Growing Threat to the World

Grace Ralstin

School of Public Policy, Pepperdine University

Abstract

ISIS has inflicted terror onto civilians in several ways, through ransoms, kidnapping, beheadings, mass shootings, and bombings. These acts of terror are funded through the internet. They use this tool as a mechanism to spread online propaganda and radicalize people, in addition to terrorizing civilians with cyberterrorism to collect money. This analysis also compares ISIS to other terrorist organizations, specifically in their online propaganda tactics and funding. Further, it will posit policy recommendations that are aimed at helping policymakers combat online terrorist activity. The goal should be making cyberspace safer for the public and increasing challenges for terrorists to conduct their activities, deterring them from using the internet. Livemap, cyber risk assessments, lawful hacking, and education among the public (specifically youth) are all potential solutions to mitigating online radicalization and cyberterrorism.

Keywords: ISIS, ISIL, cyberterrorism, radicalization, Caliphate, Islam, Hamas, al-Qaeda, al-Shabaab, internet, encryption, cybersecurity, propaganda

The Rise of ISIS: A Growing Threat to the World

The advancement of technology in the twenty-first century has resulted in several accomplishments, such as the development of social media, smartphones, Bitcoin, and cryptocurrencies. Although the benefits of these technological advancements are easily observed, especially regarding communication, there are also many costs. For example, technological advancements in communication make it easier for illegal activity to occur, such as human trafficking, black market activity, and radicalization. Furthermore, it has become highly challenging for authorities to keep up with these illegal activities despite privacy laws protecting American citizens' rights from governments accessing such information. Most people can agree that they would like to mitigate online terrorist activities and make the internet safer, but at what price are Americans willing to reevaluate their rights, such as privacy, in exchange for increasing public safety? These are questions that should be answered when implementing cybersecurity policies.

In this analysis, the terrorist organization ISIS will be examined concerning how they use the internet to expand and fund their organization. More specifically, how they use online propaganda to radicalize people and how they use cyberterrorism and other online methods to collect money. In addition, ISIS will be compared to other terrorist organizations when evaluating online propaganda tactics and collecting funding. Lastly, policy recommendations will be given that explore the various ways policymakers could combat online terrorist activity. The goal is to make cyberspace safer for the public and increasing challenges for terrorists to conduct their activities, deterring them from using the internet.

The Story Behind ISIS

One must understand the context of how ISIS started before delving deeper into how the terrorist organization operates. First, what does ISIS stand for? ISIS stands for the Islamic State of Iraq and Syria. It is also called ISIL, which stands for the Islamic State of Iraq and the Levant, or IS, the Islamic State. Furthermore, ISIS was birthed from civil conflicts in Iraq and Syria. The civil conflict has been built over time, and the recent history of both nations explains why ISIS formed. According to Forscey and Khan, in the 1940s, Iraq and Syria declared independence from the European colonial powers and established their boundaries. Then in the 1960s, a political party called Baathists came into existence and took over Syria and Iraq (2). Saddam Hussein was the leader of the Baathist political party in Iraq. Starting in 1979, he ruled the Sunni government in a Shia-majority population. In 2003, the United States overthrew Saddam Hussein, and Prime Minister Nouri al-Maliki was elected, resulting in a Shia government (Forscey and Khan 2; Terrill 12).

Syria's Baathist dictatorship started sooner than Iraq's, with leader Hafez al-Assad becoming Syria's dictator in the 1960s. Assad's regime consisted of a Shia government with a Sunni-majority population. When Saddam Hussein was overthrown, many Iraqi Baathists fled to Syria, and Assad's son, Bashar al-Assad, became president (Forscey and Khan 2). In 2011, the Arab Spring caused Syrian protesters to demand that the Syrian government reform its government by implementing democratic principles and removing Bashar al-Assad (Habets). This civil war lasted in Syria for over five years, and the aftermath resulted in hundreds of thousands of people being killed. The Syrian government was responsible for most civilian deaths, killing civilians via bombings, artillery barrages, and chemical weapon attacks (Forscey and Khan 2).

Therefore, the recent history of Iraq and Syria concerning political and religious tension displays how the path was cleared for ISIS to come into power. It must also be mentioned that ISIS has ties to the terrorist organization Al-Qaeda. Still, the connection between the two terrorist groups was triggered by Abu Musab al-Zarqawi, also known as AMZ. Zarqawi was a Jordanian Islamist who wanted to fight the Jordanian government but failed (Hashim 69). He eventually went to Iraq after the United States invaded Afghanistan. Zarqawi initiated a militant organization called Jamaat al-Tawhid wal-Jihad (JTJ), and it caused a significant amount of terror in Iraq after the United States invaded the country. Despite JTJ and Al-Qaeda sharing similar extreme Islamic beliefs, Zarqawi joined Al-Qaeda in 2004, and Osama bin Laden took control over JTJ, forming Al-Qaeda in Iraq (AQI) (Hashim 71). In 2006, the U.S. military killed Zarqawi (Chambers 30). According to Hashim, "A top AQ operative, Abu Hamza al-Muhajir (aka Abu Ayub al-Masri), was promoted to be the AQI representative in Iraq. Soon afterward, the organization announced the establishment of the Islamic State of Iraq (ISI) under the leadership of Abu Omar al-Baghdadi" (72).

After Baghdadi founded ISI, the organization faced many challenges. For example, according to Hashim, in 2008, the United States was working with tribes and Sunni insurgents to fight against ISI. By the end of 2008, Iraq seemed to be moving towards peace and security and clearing out members of ISI (72). However, by early 2009, ISI began attempting to overthrow the government and reemerge its violent tactics, targeting civilians and killing hundreds. The situation eventually turned around in 2010, when eighty percent of the leadership of ISI had been killed or captured. One of the deaths included the founder, Abu Omar al-Baghdadi (Hashim 73). Despite the events regarding the rise and fall of ISIS, the terrorist organization eventually emerged from 2010-2013.

After ISIS officially became a terrorist organization, it gained a significant amount of power in a short period. The group started taking over small towns in northern Iraq and continued controlling other territories (Johnsen 13). Johnsen also mentioned that ISIS seized a massive oilfield in Syria and controlled a Syrian military base in Raqqa. The United States launched several air strikes on the territories the terrorist group controlled. In retaliation, ISIS took American hostages, beheaded them, and posted the videos online for several weeks (20). The ISIS members would demand ransoms, which is a common method for terrorist groups to kidnap people to fund their organizations. Despite the American hostages being taken and decapitated, the U.S. continued to bomb ISIS-controlled territories. The U.K. and France had also carried out airstrikes on ISIS targets. From 2014 to 2015, ISIS carried out around three thousand attacks (Johnsen 20). One of the attacks included the Paris terrorist attacks, which killed and injured hundreds of people through suicide bombings and mass shootings. Clearly, ISIS was unphased by the six thousand airstrikes the U.S. had launched and would continue to spread their extreme beliefs however they could. In the next section, the circumstances of how ISI successfully gained power will be examined, along with the strategies that make the organization unique compared to other terrorist organizations.

Recruitment Tactics Through Online Propaganda and Radicalization

ISIS is notorious for its various recruitment tactics, allowing the terrorist organization to gain such a significant following. It is critical to mention that ISIS successfully recruits many foreign members outside of Iraq and Syria through its tactics. According to Gates and Podder, reports from 2015 indicate that during the Iraq and Syria conflict, over 20,000 foreigners have joined various militant Sunni organizations, with most of the foreign fighters joining ISIS (107). Furthermore, Gates and Podder define what makes an individual a foreign fighter, stating that non-citizens of the conflict state join a faction, who lack “affiliation to an official military organization” and are unpaid (107). The question is raised as to how ISIS can successfully recruit foreign fighters at such high rates compared to other terrorist organizations. But the answer is simple; According to Farwell, ISIS uses persuasive propaganda tactics by exploiting “the mainstream media (ISIS videos have appeared on Western broadcast outlets as well as extremist websites), which means that these messages have reached audiences around the world.” In addition, ISIS also uses social media platforms such as Twitter, Facebook, and Instagram to spread their beliefs and “influence adversaries, friends and journalists alike” (50). In this section, ISIS’s recruitment methods will be examined and will also be compared to other terrorist organizations’ recruitment methods. This comparison explains why ISIS differs from other terrorist organizations when evaluating its popularity.

Compared to other terrorist organizations, ISIS is unique due to its online propaganda and members being active on various social media platforms in an attempt to radicalize potential members. More specifically, ISIS uses a web 2.0 environment, meaning it uses any platform where the users can generate their own content compatible with various systems, products, and devices (Buffington 37). These platforms include but are not limited to YouTube, LiveLeak, Facebook, Twitter, Instagram, Tumblr, and so forth. ISIS has used web 2.0 in extreme ways to receive widespread media attention and to gauge interest from other users on the same platforms.

For example, ISIS is known for uploading images and videos of the organization’s various methods of torturing people; this includes beheadings, shooting and burning hostages, etc. However, it is vital to mention that these videos demonstrate significant effort and are professionally recorded and directed (Gates and Podder 109; Lakomy 41). ISIS uses gruesome acts of violence not only to scare outsiders of what ISIS’s capabilities consist of but also because it is supposed to have a persuasive impact on those individuals who potentially would want to participate in such activities. Furthermore, ISIS can successfully spread its online propaganda to reach hundreds of thousands or even millions of internet users by relying "on a massive network of tens of thousands of unaffiliated supporters in the Web 2.0 environment, which uses the 'share' function to transfer the propaganda to their followers and peers. This, in turn, contributed to the creation of a specific 'snowball effect' in cyberspace" (Lakomy 41). But brutal acts of violence are not the only content ISIS produces to gain attention; the terrorist organization produces more content that is "western friendly" to show that ISIS is familiar with western culture. In addition, they create propaganda that highlights the wrongdoings of the enemy and emphasizes the glorification of the good of ISIS (Gates and Podder 109).

In comparison to other terrorist organizations, ISIS is unique in its recruitment tactics as the organization focuses on recruiting members through various platforms on the internet. Additionally, ISIS puts a significant amount of time and effort into creating online propaganda intended to persuade people to join the terrorist group, glorifying what it has to offer. However, many successful terrorist organizations exist that do not use the internet as the primary recruitment method, one of which is *Hamas.*

Hamas is a Palestinian Sunni-Islamist militant, fundamentalist, and nationalist organization founded in 1987. Hamas focuses on recruiting Palestinian youth and young adults, targeting the Gaza Strip and the West Bank. Dawa activists are usually the recruiters for the organization, focusing on finding youth and young adults to become suicide bombers and participate in terror attacks. Dawa activists are followers of Islam who partake in missionary activities. The Arabic term dawa translates to "a call" or "an invitation" (Zulkifli 113). These recruiters target "charity committees, mosque classes, student unions, sports clubs, summer camps, and other organizations run by Hamas” (Levitt and Ross 83). Hamas has so much power over Palestine despite its prominent role in the government. Hamas can integrate its radicalization into everyday life, especially among Palestinian youth and young adults. For example, according to Vertigans, Islamic publications and media communications are a popular method of coercion that displays graphic images concerning politics and religion, intending to make Palestinians feel angered and helpless. Islamic radicalization can be identified within various television and satellite channels, including children’s cartoons and music shows (“Social Barriers to Peace”). However, members of Hamas do not only target Palestinian youth and young adults; they also target people with a high level of vulnerability, such as poor Palestinians. For instance, Vertigans mentions that Hamas will organize social activities to radicalize vulnerable people by exploiting their vulnerabilities. In other words, in Gaza and the West Bank, Hamas has implemented shelters, jobs, security, education, and has supplied food (“Social Barriers to Peace”).

Another terrorist organization that is worth comparing to ISIS is *Al-Shabaab.* Al-Shabaab is a Salafi-jihadist military and political organization. The group is based in Somalia but also operates in parts of East Africa. The terrorist group has ties to Al-Qaeda, sharing similar ideologies about Islamic extremism, but Al-Shabaab differs in that it incorporates Somali nationalism into its belief system. Furthermore, this terrorist organization is similar to ISIS concerning recruitment tactics, specifically in its use of the internet to recruit foreign fighters. According to Menkhaus, Somalia is a nation that is advancing technologically despite the nation’s large diaspora of over one million people. Many diasporas have resulted in over one point five billion dollars being returned to the homeland annually, developing a solid telecommunications infrastructure for the nation (311). As a result, a rapid increase in Somali internet users occurred in the 1990s, although the diaspora population more commonly uses it.

The intertwining of the internet into everyday life in Somalia has allowed Al-Shabaab to take advantage and use media relations to further its extremist agenda by spreading propaganda and persuading outsiders to join or support the organization. For example, according to Menkhaus, Al-Shabaab has a public relations unit called the “HSM Press Office.” The group focuses on radicalizing outsiders into Islamists and promoting its extreme storylines and propaganda to an audience that already believes in Islam (312). Along with that, the terrorist group is highly sophisticated in creating propaganda online through social media posts and videos that focus on what the group opposes rather than what it supports. For instance, in 2007-2008, Al-Shabaab built a narrative of victim-mentality, specifically mentioning that jihad is an act of self-defense to support the organization’s structure as a military group. The military group is supposed to fight against threats such as Christian Ethiopian invaders backed by the United States (Menkhaus 313). Al-Shabaab shares a similar ideology to Al-Qaeda concerning the spread of Western influence and deeming the United States the enemy.

Al-Shabaab differs from most terrorist organizations regarding the spread of propaganda and recruitment because Somalia is heavily media-oriented. In other words, beyond social media and using the internet, Al-Shabaab frequently uses radio stations to be heard by Somalis inside *and* outside the nation. Einashe stated that Al-Shabaab’s radio usage is correlated to Somalian culture being an oral one, for poetry and spoken words are traditional and resemble a lot of power (“Fear for the Airwaves”). Therefore, this terrorist group differs from many other terrorist organizations despite having significant power over what their target audiences can listen to in the areas that Al-Shabaab controls. For example, Einashe discusses how Al-Shabaab has its own radio station called Al-Andalus. The Members of Al-Shabaab discuss the targets they have killed, which is intertwined with jihadi propaganda and Islamic devotional music ("Fear for the Airwaves"). Along with that, the terrorist group has a long history of terrorizing Somali journalists to spread their extremist beliefs. Al-Shabaab is notorious for planting car bombs in the cars of Somali journalists, killing dozens of them starting in 1991 (Einashe).

ISIS's Usage of Cyberterrorism

The previous section discussed how ISIS uses cyberspace to spread online propaganda to persuade people to join its ranks. Along with that, they attempt to create an illusion that they are cleansing the world of evil, and the declared enemies are the ones who should be held liable. These recruitment tactics play a critical role in allowing ISIS to grow its following, but how does this terrorist organization financially support its conventional methods of terrorism and create an incentive for existing members to stay? Nevertheless, this section will examine how ISIS uses cyberterrorism to display its dominance in the international system as a non-state actor and demonstrate how it can financially support the organization to continue terrorizing non-members.

Before examining how ISIS uses cyberterrorism in various instances, one must define the definition of *cyberterrorism.* According to Weimann, "Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives" (4). Cyberterrorism is intended to cause significant damage with the primary purpose of instilling fear into people. This type of terrorism can be equally as lethal or harmful as conventional terrorism. Furthermore, ISIS has established its intentions when examining its cyber offense against the United States. ISIS wants Americans to not only be fearful of their capabilities of conventional terrorism but cyberterrorism as well.

In addition, a pro-ISIS hacking group called “Team System Dz” hacked several U.S. government websites during the timeframe of the Trump administration, threatening former President Donald J. Trump and spreading Islamic propaganda (Holt et al.).

Therefore, ISIS poses a serious threat not only when evaluating conventional terrorism but also the method of cyberterrorism. A research study indicates that ISIS is statistically a massive threat when looking at its success in using cyberterrorism. According to a dataset from the U.S. Department of State, specifically data from 2011 to 2016 derived from the annual terrorist reports, based on the eighty-three cases within the global cyberterrorism dataset, sixty-seven point five percent or fifty-six cases happened to be cyberterrorism cases ISIS was responsible for. Out of the nineteen nations that were victims of cyberterrorism, the United States was one of the top four most targeted (Lee et al.). For this reason, the United States should be concerned about building a strong cybersecurity defense against foreign adversaries and non-state actors.

One aspect of ISIS using cyberterrorism has been examined, but how does ISIS use cyberspace to further its extreme agenda to fund the organization? This section will explore the variety of methods ISIS uses to collect money through cyberspace. But first, the primary methods that are not correlated to cyberspace will be discussed. Nevertheless, it is critical to mention the success of ISIS when evaluating the organization's financial stability. By the fall of 2015, ISIS generated approximately two point four billion dollars annually (Martin and Solomon). ISIS is heavily involved in *illicit trade*, like most terrorist groups. While there is no exact definition of illicit trade since it can be seen as interchangeable with the term illegal trade, for the sake of this analysis, the definition that will be settled on is defined by the World Customs Organization (WCO). The organization's definition of illicit trade is as follows:

> Illicit trade involves money, goods or value gained from illegal and otherwise unethical activity. It encompasses a variety of illegal trading activities including human trafficking, environmental crime, illegal trade in natural resources, intellectual property infringements, trade in certain substances that cause health and safety risks, smuggling of excisable goods, trade in illegal drugs and a variety of illicit financial flows (Shelley 9).

ISIS has a history of being involved with human trafficking, specifically trafficking Yazidi women. These women are often used for sexual services for members of the terrorist group and then traded or sold. ISIS has also used the human trafficking industry for labor, specifically to traffick oil. For example, Shelley mentions that ISIS gave traffickers an incentive to traffick oil for the terrorist group by giving them petroleum products in exchange for smuggling oil out of Iraq. Terrorist organizations commonly use trafficked labor to get around tax regulations and customs duties to get goods across borders (11). Additionally, ISIS has ties to the cigarette trade, like the terrorist groups Hamas and Hezbollah (Shelley 9-10).

Besides illicit trade, ISIS has also used cyberspace for ransoms, hacking, and activity within the black market. For example, Blannin discusses how ISIS hackers extract billions of dollars from the United States alone, using cybercrime and cyber espionage. He goes on to mention one of the methods that ISIS cyber-jihadis use includes directing their online followers to donate money to the organization through Dark Wallet, an anonymous Bitcoin transfer application (19). As analyzed in the previous section about online propaganda, ISIS has a strong enough following caused by various Islamic radicalization tactics that persuade online members to donate money to its terrorist organization. Cyber-jacking is another primary method that ISIS uses to fund the organization, stealing billions of dollars. According to Blannin, cyber-jacking is an easily learnable skill in the world of hacking, and it is not challenging to use ransomware on people's personal computers. Hackers are given a significant amount of opportunity to gain mass amounts of money for their terrorist organizations (20).

Another example of ISIS members using cyber-jacking for financial gain is by using chatbots and botnets on social media platforms. This hacking method consists of internet bots chatting with social media users, allowing the automated program to perform various online tasks. For example, in 2016, ISIS cyberhackers deployed botnets across Twitter, performing various activities such as scams that requested money or cryptocurrency, leveraging malware that led to cyber-attacks, and spreading propaganda (Sultan, "Combating the Rise of ISIS" 49). Therefore, when comparing terrorist groups and their financial gains and the different methods of managing finances, ISIS differs significantly from al-Qaeda, the terrorist group it has ties with. In the next section, Al-Qaeda's methods of collecting funding will be examined, along with the organization's ability to use cyberterrorism to achieve the ends of the group's interest.

It has been mentioned that ISIS is a splinter group of Al-Qaeda, although it consists of different ideologies, tactics of terror, and funding methods. While ISIS is significantly more successful concerning recruitment, finances, and power than Al-Qaeda, Al-Qaeda was responsible for the deadliest terrorist attack in world history. This terrorist attack was carried out in the United States and killed approximately three thousand Americans. So, how did Al-Qaeda manage to get the funding to carry out the 9/11 terrorist attacks? Before delving into Al-Qaeda's methods of securing finances for the organization, it is critical to discuss how much money the terrorist organization spent on both its terrorist attacks against the World Trade Center. In 1993, the terrorist attack cost about nineteen thousand dollars, while the 9/11 terrorist attacks in 2001 cost between three hundred and fifty thousand and five hundred thousand U.S. dollars (Martin and Solomon). Al-Qaeda has managed to secure funding for its organization in several ways, being heavily involved in illegal activity such as theft. For example, according to Martin and Solomon,

> Al-Qaeda is notorious for perpetrating bank robberies and stealing oil from Iraqi oil pipelines. However, Al-Qaeda is not only captivated by illegal activity but has also used several methods of legal activity to increase funding. While downsides to legal activity include paying taxes or allowing the government to trace the flow of money to terrorist activity easily, legal activity makes it difficult for authorities to intervene since they do not have probable cause ("Islamic State: Understanding the Nature").

Furthermore, when Al-Qaeda operated in Sudan between 1992 and 1996, they owned several businesses such as farms, trading companies, and an investment company (Martin and Solomon).

While several examples have been listed concerning the different methods Al-Qaeda uses to generate revenue, Al-Qaeda has also engaged in cyberterrorism over the years to fund its organization and terrorize people. For example, according to the *Center for Strategic and International Studies,* Al-Qaeda is known for using the internet to indulge in illegal financial operations, such as stealing people's credit card information and financial data (Lewis 8). The U.S. Department of Justice has listed Al-Qaeda as an example of a terrorist organization that also engages in cyber financial campaigns. Like ISIS, Al-Qaeda is also heavily involved in bitcoin money laundering networks. According to the *U.S. Department of Justice,* Al-Qaeda uses Telegram channels and various social media platforms to solicit cryptocurrency donations. Al-Qaeda members will pretend to be different charities. One post advocated for funding weapons for terrorists in Syria ("Global Disruption of Three Terror Finance"). Therefore, Al-Qaeda has used cyber planning to fuel its terrorist activities, perhaps not always using the internet for cyberterrorism but rather, to further its extremist goals. For instance, encryption is commonly used among terrorist organizations, and Al-Qaeda has a history of using encryption on its several websites to hide its extreme agenda from authorities. Thomas states that it is possible to buy encryption software for less than fifteen dollars (119). Besides using encryption for its websites, Al-Qaeda has also encrypted its messages when communicating with other members, an example being the premeditation of the 9/11 terrorist attacks. According to Weimann, thousands of encrypted messages that “had been posted in a password-protected area of a website were found by federal officials.” The messages were found on the computer of Abu Zubaydah, who was eventually arrested. In addition, Al-Qaeda terrorists used the internet in public places to send public emails, using free web-based email accounts (10). In a post-9/11 world, terrorists have a more difficult time communicating with one another despite the legal implications that resulted from the 9/11 terrorist attacks. Many exceptions from the Patriot Act allow the authorities to search through phone records, emails, etc., without a search warrant.

Several hacking groups around the world are highly successful in using various methods of cyberterrorism. Many of these hacking groups share the simple goal of hacking into the systems of multi-million-dollar companies and using ransomware to receive money or further their extreme agendas. Although terrorist organizations such as ISIS and Al-Qaeda successfully gain funding online, it is not comparable to some of the existing hacking groups. For example, in 2011, a group of hackers called the *Cyber Fighters of Izz ad-din Al Qassam* hacked into thousands of computers and servers worldwide. According to Buchanan, the hackers’ entry point was computers and servers that used content management software such as WordPress. Once the hackers gained access, they installed their own software that allowed them to use the devices or send messages to specific individuals (155). Eventually, the Cyber Fighters of Izz ad-din Al

Qassam targeted companies in the United States, attacking several during the first half of 2012. Buchanan also said:

> The hacking group’s motive for targeting the United States was because of a video called *Innocence of Muslims*, in which a pastor had mocked and criticized Islam, and the U.S. government would not give in to taking the video down. This resulted in the hacking group targeting American banks, specifically Bank of America, the New York Stock Exchange, and later adding Chase Bank (156).

This attack was designed to cause as much damage as possible so the banks would lose business, a prime example of cyberterrorism. Buchanan mentioned that the attack on the banks lasted for several weeks, flooding the bank systems with internet traffic worldwide. Although the U.S. government never took down any anti-Muslim videos that the hacking group kept demanding to be taken down, the attacks eventually stopped (Buchanan 156-157).

Therefore, although terrorist organizations such as ISIS and Al-Qaeda have engaged in cyberterrorism to further their extreme agenda, it is primarily money-motivated. Not only that, but many terrorist organizations will display intent to use cyberterrorism to cause a significant amount of destruction on a target, but the organization will not have the capabilities to do so. For example, evidence has been found on the devices of Al-Qaeda members' surveillance of nuclear power plants, dams, and other types of critical infrastructure (Chen 14). Although Al-Qaeda targets engineers and scientists for recruitment and could potentially pay for proxies to carry out a cyberattack against the United States, it is doubtful that a terrorist group would reach its goal of causing the amount of damage it desires. According to Chen, Al-Qaeda has published in its online magazines that it would like to carry out an electronic jihad to disrupt the United States economy. Phase one consisted of the 9/11 terrorist attacks, and phase four was supposed to occur between 2010-2013, which involved using cyberterrorism to damage the U.S. economy (13). Evidently, phase four has not been successful, and this example demonstrates how most terrorist organizations have a long way to go concerning their cyberterrorism capabilities.

Policy Suggestions

It would be nearly impossible to completely eliminate cyberterrorism and online propaganda as technology advances and more people become accustomed to using the internet more and more in their daily lives. However, several routes can be taken in public policy to mitigate cyberterrorism and online propaganda to help decrease the number of people potentially recruited for terrorist organizations like ISIS. The first policy suggestion that merits consideration is mitigating disinformation and online propaganda by using an assessment that evaluates the review of online engagement with ISIS, known as *Livemap.* According to Sultan,

> Livemap is a tool that reveals the points on a map of the activity occurring between ISIS and their social engagement network. This tool can read the messages between ISIS members attempting to recruit people online on various social media platforms. However, one challenge from Livemap is how many social media platforms have a function where private group chats require an invitation (“Tackling Disinformation” 48).

Another challenge of Livemap is accessing location services on a terrorist’s device. Charania states that ISIS leadership instructs their members to have their location services turned off at all times and never disclose their location to others. In addition, members of ISIS are demanded not to own iPhones (95).

In addition to U.S. government agencies detecting terrorist activity online, decrypting messages online should be highly prioritized in cybersecurity policy. For example, in 2007 an encrypted communication software called asrar al-mujahidin, also called mujahidin secrets, was implemented on an online jihadist messaging board (Graham 22). Encryption is one of the biggest challenges for policymakers when brainstorming counterterrorism efforts, because of civil rights such as freedom of speech and privacy, which pose a major obstacle. Many of those who are pessimistic about encryption mitigating terrorist attacks state that it will not be as simple as law enforcement intervening and being the hero that stopped a terrorist attack from occurring.

Despite warranted concerns, it is absurd to completely shut down policy suggestions concerning encryption, as it is the most significant method of terrorists communicating with one another in planning terrorist attacks. For example, the *Bipartisan Policy Center* discussed how Abdelhamid Abaaoud, a member of ISIS, helped coordinate the 2015 Paris terrorist attacks and subsequent atrocities in Brussels by giving the members involved USB sticks with encryption keys to decode their messages with one another. The members used Telegram and WhatsApp to plan the terrorist attacks (“Digital Counterterrorism” 16).

Therefore, one policy suggestion that could potentially mitigate communication between terrorists is constructing a “layered” defense against terrorist operations in the digital realm. In other words, in this approach, each layer must be a pillar for another, improving the overall security system (“Digital Counterterrorism” 19). Each layer would make it more difficult for terrorists to exploit the digital realm, making it more challenging for them to carry out their operations. Nevertheless, lawful hacking is one of the solutions built into this policy recommendation. According to the *Bipartisan Policy Center,* lawful hacking is “legally authorized efforts by government agencies to penetrate the devices and services used by terrorists and other criminals.” In addition, lawful hacking can identify end-to-end encrypted communications and locate the “endpoint,” which displays the decrypted messages the intended recipient was supposed to see (“Digital Counterterrorism” 19).

Cybersecurity policies concerning cyberterrorism conducted by terrorist organizations should also be of great concern for many nations, especially the United States. As examined throughout this analysis, terrorist organizations engage in various activities related to ransomware to fund their organizations and inflict terror online. The United States government should implement a policy that lays out the steps of a cyber risk assessment to decrease the amount of cyber-terror attacks that terrorist organizations cause. Building a strong defense against cyber terrorists would be in the best interest of the United States. It would be a preventative measure to prevent funding and successful cyberattacks against civilians and government agencies. Nevertheless, negotiation practices should be used as a method of cyber defense, and the policy should be intended to educate the public. Falco et al. discuss three stages of a digital, anonymous negotiation: pre-interaction, interaction, and post-interaction. This model is used to guide individuals victimized in a ransomware attack, similar to human hostage negotiations in the sense that trust must be built between the hacker and the negotiator. Cyber resilience is also mentioned when an organization continues to operate with the mentality that cyberattacks are inevitable (“Cyber Negotiation”). To enable cyber resilience, operators should follow the four steps:

> First, it is worth the time and money to identify the likelihood and impacts of the hacker possibly losing control of the system. Second, it should be ingrained in the management operations to enhance systems' resilience after an attack. Adequate funding should be used for any hacked systems. Third, emergency response training should be continuously practiced among staff members. Lastly, the collaboration between agencies and levels of government should be used to formulate cyber attack emergency response plans (Falco et al.).

Therefore, cybersecurity policies should be implemented that outline a plan that mitigates damages from cyberattacks that terrorists can cause, to allow various agencies to be proactive.

Another policy suggestion should address online radicalization, despite many terrorist organizations using various recruitment tactics and propaganda to persuade outsiders to join. Before delving into a policy suggestion, it is crucial to acknowledge the inevitable obstacles when examining online radicalization among terrorist organizations. First, filtering certain words and phrases on various social media platforms and websites would not be taken lightly by the public. The United States is an open democratic society that places significant value on free speech, as it is an American citizen's constitutional right. Although restricting free speech would likely decrease terrorist activity online, it would be difficult to carry out such a policy based on the legality rooted in the First Amendment. Second, even if policies were implemented that restrict free speech, private chat rooms exist on certain social media platforms. There are still several ways that terrorists can communicate with one another and potential recruits, by using encrypted messaging apps like Telegram and WhatsApp. Lastly, because restricting free speech could filter a large amount of propaganda and create an obstacle for terrorists to communicate, many terrorist organizations use code words and indirectly express their extreme or violent agendas— they are aware of legal loopholes and avoid using words and phrases that could be deemed harmful speech.

Therefore, a policy suggestion for combatting online radicalization should not reduce the *supply* of propaganda and other recruitment methods but focus on reducing the *demand*. More specifically, a policy that educates the public about online radicalization should be enacted, focusing mainly on youth and vulnerable adults. Training should be implemented in schools to make students aware of online propaganda and radicalization tactics on the internet, especially on various social media platforms. In addition, community groups should be encouraged to "expand programs and initiatives that create awareness and spread information about online radicalization among educators, parents, and communities" ("Countering Online Radicalization in America" 8). Parents and students should be educated on the signs of terrorists attempting to recruit youth through direct messaging and examples of the persuasion methods that are commonly used. With that being said, communities should be informed about online radicalization strategies. Aly et al. address multiple stages of radicalization:

> The first stage consists of pre-radicalization, in which an individual displays curiosity toward an extremist ideology. The second stage is indoctrination, when individuals have accepted the system of extremist beliefs and are willing to participate in achieving the goals of the terrorist organization. The final stage is jihadization when radicalized members connect with other recruits and members to plan and carry out attacks (4).

Many people believe that radicalization could never happen to themselves, a family member, or a friend, but the public must be aware of the possibility of it happening to anyone. For example, in 2014, three teenage girls from Denver, Colorado, were on their way to Syria but were stopped in Frankfurt, Germany, and were flown back to the United States. The three girls told the FBI they were planning on joining Islamic extremists, getting the idea from an extremist website (Aly et al. 1). Nevertheless, the policy goal should be to reduce the demand for online radicalization and propaganda and discredit the narratives that Islamic extremists and other popular terrorist organizations spread across the internet.

Conclusion

Overall, ISIS is a tremendous threat to the world despite the advancement of technology. The several ways ISIS members communicate through social media and other encrypted messaging platforms display how simple it is for terrorists to recruit individuals and plot cyber and conventional terrorist attacks. ISIS is unique in how it has gained thousands of followers by using the internet as its primary tool to reach millions of people. The online propaganda ISIS creates in posts, videos, tweets, etc., comprises a highly persuasive narrative based on Islamic extremism. The terrorist organization wishes to convert the world to a Caliphate and take down any threats that get in the way of their extreme beliefs.

ISIS uses brutal acts of violence to scare disbelievers and demonstrate their capabilities to the world; they are willing to do whatever it takes to spread the beliefs of Islamic extremism. While ISIS heavily values the internet for displaying online propaganda and recruitment methods, not all terrorist organizations use these recruitment tactics. The Palestinian terrorist organization Hamas is an example, as they use in-person recruitment methods, such as targeting youth where young people tend to be. In addition, they also exploit people's vulnerabilities and use their power in government to implement their extreme beliefs in some forms of media communication.

On the other hand, the Somalian terrorist organization Al-Shabaab is quite similar to both ISIS and Hamas. For instance, Al-Shabaab is very similar to ISIS because it also uses the internet to spread its extreme beliefs through online propaganda on social media and other platforms. They also use violence, like ISIS, to show that they are legitimate threats and scare disbelievers. In addition, al-Shabaab is like Hamas in that they have a lot of power in using methods of Islamic radicalization that go beyond the internet— specifically media communications. Al-Shabaab takes pride in using radio stations to spread its propaganda verbally.

This analysis also critically examines how ISIS uses cyberterrorism to terrorize people and fund its organization. ISIS has demonstrated its hacking capabilities on social media platforms to terrorize users for ransoms and target people with cyberattacks. In addition, ISIS is heavily involved in using the black market to purchase malware to carry out cyberattacks. Besides using ransomware to fund the organization, ISIS also uses illicit trade to have the finances to carry out conventional terrorist attacks.

Al-Qaeda’s methods of funding its organization and engaging in cyberterrorism activity were also evaluated, having similarities and differences to ISIS. For example, Al-Qaeda engages in much more illicit trade and illegal activity than cyber activity compared to ISIS. However, it has used various methods to receive money through the internet. Al-Qaeda has shown that it has many cyber capabilities like ISIS, although the two terrorist organizations do not compare to many hacking groups, such as Cyber Fighters of Izz ad-din Al Qassam. It is common for terrorist organizations to aim to cause mass destruction by using cyber warfare to attack enemies, but they often lack the skills to do so.

Therefore, there are several ways policymakers could fight against cyber and conventional terrorism, as a few policy suggestions are examined in this analysis. Livemap, cyber risk assessments, lawful hacking, and education among the public (specifically youth) are all potential solutions to mitigating online radicalization and cyberterrorism. Policymakers should not be phased by the terrorist activity that terrorist organizations such as ISIS use to harm people and advance their extreme agendas. The goal must be to make cyberspace a safe environment for all internet users and deter terrorists from interfering with the primary goal.

References

Aly, Anne et al. “Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization, Studies in Conflict & Terrorism.” *Taylor & Francis,* 2017, 40:1, 1-9. DOI: 10.1080/1057610X.2016.1157402

Blannin, Patrick. “Islamic State’s Financing: Sources, Methods and Utilisation.” *Counter Terrorist Trends and Analyses*, vol. 9, no. 5, 2017, pp. 13–22. *JSTOR*, http://www.jstor.org/stable/26351519

Bronk, Chris, and Gregory S. Anderson. “Encounter Battle: Engaging ISIL in Cyberspace.” *The Cyber Defense Review*, vol. 2, no. 1, 2017, pp. 93–108. *JSTOR*, http://www.jstor.org/stable/26267403

Buchanan, Ben. “The Hacker and the State: Cyber Attacks and the New Normal to Geopolitics.” *Harvard University Press*, 2022.

Buffington, Melanie L. “What Is Web 2.0 and How Can It Further Art Education?” *Art Education*, vol. 61, no. 3, 2008, pp. 36–41. *JSTOR*, http://www.jstor.org/stable/27696295

Chambers, Peter. “Abu Musab Al Zarqawi: The Making and Unmaking of an American Monster (in Baghdad).” *Alternatives: Global, Local, Political*, vol. 37, no. 1, 2012, pp. 30–51. *JSTOR*, http://www.jstor.org/stable/23210901

Charania, Sofia. “Social Media’s Potential in Intelligence Collection.” *American Intelligence Journal*, vol. 33, no. 2, 2016, pp. 94–100. *JSTOR*, https://www.jstor.org/stable/26497093

Chen, Thomas M. *CYBERTERRORISM AFTER STUXNET*. Strategic Studies Institute, US Army War College, 2014. *JSTOR*, http://www.jstor.org/stable/resrep11324

"Countering Online Radicalization in America." *Bipartisan Policy Center*, 2012. https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2019/03/BPC-_OnlineRadicalization-Report.pdf

"Digital Counterterrorism: Fighting Jihadists Online." *Bipartisan Policy Center,* 2018. https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2019/03/BPC-National-Security-Digital-Counterterrorism.pdf

Einashe, Ismail. "Fear for the Airwaves: In Somalia Al-Shabaab Control a Prominent Radio Station and a Fifth of the Country. Meet the Radio Presenters Who Brave Danger to Keep on Reporting Independently." *Index on Censorship*, vol. 46, no. 3, 2017, pp. 8–10., https://doi.org/10.1177/0306422017730783

Falco, Gregory, et al. "Cyber Negotiation: A Cyber Risk Management Approach to Defend Urban Critical Infrastructure from Cyberattacks." *Journal of Cyber Policy*, vol. 4, no. 1, 2019, pp. 90–116., https://doi.org/10.1080/23738871.2019.1586969

Farwell, James P. "The Media Strategy of Isis." *Survival*, vol. 56, no. 6, 2014, pp. 49–55., https://doi.org/10.1080/00396338.2014.985436

Forscey, David, and Sanaa Khan. *Country Brief: Iraq and Syria*. Third Way, 2016. *JSTOR*, http://www.jstor.org/stable/resrep02514

Gates, Scott, and Sukanya Podder. "Social Media, Recruitment, Allegiance and the Islamic State." *Perspectives on Terrorism*, vol. 9, no. 4, 2015, pp. 107–16. *JSTOR*, http://www.jstor.org/stable/26297419

"Global Disruption of Three Terror Finance Cyber-Enabled Campaigns." *The United States Department of Justice*, 13 Aug. 2020, https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

Graham, Robert. “How Terrorists Use Encryption.” *CTC Sentinel*, 2016. https://nsarchive.gwu.edu/sites/default/files/documents/4404132/Combatting-Terrorism-Center-Robert-Graham-How.pdf

Habets, Ingrid. “Obstacles to a Syrian Peace: The Interference of Interests.” *European View*, vol. 15, no. 1, 2016, pp. 77–85., https://doi.org/10.1007/s12290-016-0397-3.

Hashim, Ahmed S. “The Islamic State: From Al-Qaeda Affiliate to Caliphate.” *Middle East Policy*, vol. 21, no. 4, 2014, pp. 69–83., https://doi.org/10.1111/mepo.12096.

Holt, Thomas J., et al. “Examining the Characteristics That Differentiate Jihadi-Associated Cyberattacks Using Routine Activities Theory.” *Social Science Computer Review*, vol. 40, no. 6, 2021, pp. 1614–1630., https://doi.org/10.1177/08944393211023324.

Johnsen, Gregory D. “The Rise of ISIS.” *Great Decisions*, 2016, pp. 13–24. *JSTOR*, http://www.jstor.org/stable/44214817.

Lakomy, Miron. “Cracks in the Online ‘Caliphate’: How the Islamic State Is Losing Ground in the Battle for Cyberspace.” *Perspectives on Terrorism*, vol. 11, no. 3, 2017, pp. 40–53. *JSTOR*, http://www.jstor.org/stable/26297840.

Lee, Claire Seungeun, et al. “Mapping Global Cyberterror Networks: An Empirical Study of Al-Qaeda and ISIS Cyberterrorism Events.” *Journal of Contemporary Criminal Justice*, vol. 37, no. 3, 2021, pp. 333–355., https://doi.org/10.1177/10439862211001606.

Lewis, James A. “Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.” *Center for Strategic & International Studies*, 2002, https://www.steptoe.com/a/web/4586/231a.pdf

Levitt, Matthew, and Dennis Ross. “The Logistics of Terror: Tactical Uses of the Dawa.” *Hamas: Politics, Charity, and Terrorism in the Service of Jihad*, Yale University Press, 2006, pp. 80–106. *JSTOR*, http://www.jstor.org/stable/j.ctt1npc2n.8.

Martin, Michaela, and Hussein Solomon. “Islamic State: Understanding the Nature of the Beast and Its Funding.” *Contemporary Review of the Middle East*, vol. 4, no. 1, 2017, pp. 18–49., https://doi.org/10.1177/2347798916681319.

Menkhaus, Ken. “Al-Shabaab and Social Media: A Double-Edged Sword.” *The Brown Journal of World Affairs*, vol. 20, no. 2, 2014, pp. 309–27. *JSTOR*, http://www.jstor.org/stable/24590990.

Shelley, Louise I. “Illicit Trade and Terrorism.” *Perspectives on Terrorism*, vol. 14, no. 4, 2020, pp. 7–20. *JSTOR*, https://www.jstor.org/stable/26927661.

Sultan, Oz. “Combating the Rise of ISIS 2.0 and Terrorism 3.0.” *The Cyber Defense Review*, vol. 2, no. 3, 2017, pp. 41–50. *JSTOR*, http://www.jstor.org/stable/26267384.

Sultan, Oz. “Tackling Disinformation, Online Terrorism, and Cyber Risks into the 2020s.” *The Cyber Defense Review*, vol. 4, no. 1, 2019, pp. 43–60. *JSTOR*, https://www.jstor.org/stable/26623066.

Terrill, W. Andrew. *LESSONS OF THE IRAQI DE-BA’ATHIFICATION PROGRAM FOR IRAQ’S FUTURE AND THE ARAB REVOLUTIONS*. Strategic Studies Institute, US Army War College, 2012. *JSTOR*, http://www.jstor.org/stable/resrep11491.

Thomas, Timothy L. "Al Qaeda and the Internet: The Danger of “Cyberplanning.” *Parameters*, 33, no. 1, 2003. doi:10.55540/0031-1723.2139.

Vertigans, Stephen. “Social Barriers to Peace: Socialization Processes in the Radicalisation of the Palestinian Struggle.” *Sociological Research Online*, vol. 9, no. 3, 2004, pp. 79–84., https://doi.org/10.5153/sro.967.

Weimann, Gabriel. “www.terror.net: How Modern Terrorism Uses the Internet.” *United States Institute of Peace*, 2004, https://www.usip.org/sites/default/files/sr116.pdf

Zulkifli. “Da’Wa.” *The Struggle of the Shi‘is in Indonesia*, ANU Press, 2013, pp. 113–40. *JSTOR*, http://www.jstor.org/stable/j.ctt5hgz34.12.