United to Deter: Dealing With New Means of Supporting Terror

Frank A. Florio
UNITED TO DETER: DEALING WITH NEW MEANS OF SUPPORTING TERROR

Frank A. Florio

TABLE OF CONTENTS

TABLE OF CONTENTS.................................................................127
I. INTRODUCTION...........................................................................127
II. TYPES OF TERRORISM SUPPORT .............................................131
   A. FINANCIAL ...........................................................................131
   B. SOCIAL MEDIA .....................................................................133
III. DISPARITIES AMONGST NATIONS...........................................135
   A. ENGLAND ............................................................................135
   B. FRANCE ..............................................................................137
   C. THE UNITED STATES .........................................................140
IV. THE EFFECT OF THE LAWS......................................................143
V. INTERNATIONAL SOLUTION TO THE USE OF SOCIAL MEDIA
   BY TERRORIST ORGANIZATIONS ...............................................151
VI. CONCLUSION...........................................................................156

I. INTRODUCTION

In the days and weeks following September 11, 2001, nations around the world came to understand the borderless reach of terrorism. Coalitions were formed, alliances were created, and the world was united to confront the threat. At that moment, the danger was clear. Osama bin Laden and his notorious radical group, Al Qaeda, had been active for decades as the most dangerous terrorist organization on the planet.¹ So, the United States and its allies invaded Al

Qaeda’s central hub of operations in Afghanistan with the intent to take the fight to the enemy and ensure safety at home. But this was just the beginning.

Much like the rapid growth of cellular phone technology, social media, and the Internet, terrorism has evolved rapidly. Since the death of Osama bin Laden, new methods of spreading and supporting terror continue to develop, and nations are adapting together to combat the evolving threat.

Actions generally define terrorism. How one interprets certain acts is how one determines whether terrorism occurred. “[T]errorism” and its definition differs with perspective. Internationally, however, terrorism is a legal term. For nations to unite in policy against terrorist groups and organizations, it is imperative that each nation knows exactly who and what the enemy is.

Terrorism has become an international matter, crossing borders, and targeting victims of nations outside the home territory of the terrorist group responsible for the

---

4 Id.
attacks.\textsuperscript{7} International cohesive solutions therefore are essential to combat the threat. A fair assumption is that with a consistent definition, it will be far easier for nations to draft and implement laws that locate, punish, and deter terrorist cells. On the international stage, terrorism is defined as an “independently unlawful” and intentional act that results in the “serious harming or killing of non-combative civilians and the damaging of property with a public use causing economic harm done for the purpose of intimidating a group of people or a population or to coerce a government or international organization.”\textsuperscript{8}

Since the September 11, 2001 attacks on the United States, terrorism continues to be at the forefront of international policy.\textsuperscript{9} In order to fight together, nations implement similar policies on border control, intelligence sharing, and military strategy.\textsuperscript{10} Terrorism, however, remains prevalent. As of July 2016, there have been twenty-eight terrorist attacks, claiming the lives of countless

\textsuperscript{7} Id. at 31 (“Acts may also be considered international in character when they attempt to influence foreign governments and when they implicate the interests of more than one state.”).

\textsuperscript{8} Id. at 64 (“No particular motivation need explain the act and none can justify it. Group action or involvement is not a requirement, but the act must be perpetuated by a sub-state actor. The act and/or its effects must be international in character.”).


innocent people. Additionally, the litany of attacks in 2017 in major cities such as New York City and London demonstrates terrorism poses a major threat to the world.

These incidents are not hard to punish. There is not much international dispute surrounding what to do with individuals who carry out acts of terror and take innocent lives. But there is disparity amongst nations regarding how to punish those who support terror, thereby allowing terrorist groups and organizations to grow and carry out attacks.

One aspect of counterterrorism is crime control and prevention. In the last few years, there has been an effort to counter terrorist activities using tenacious prosecution as a deterrence, especially in the United States. But this is not the case in every nation. The question then becomes, “Does it make a difference to terrorists whether prosecution and enforcement differ from one country to the other for the same type of crime?”

This Note will analyze the disparities among the United States, England, and France regarding the enforcement of laws and punishments as applied to those

---

who choose to support terror with or without intent. Part II will explain the different types of support of terrorism, including how this support has evolved in modern times. Part III will highlight the disparities in punishment among England, France, and the United States. Each country’s laws will be described and compared to the sentencing and enforcement for particular crimes. Part IV will describe the current effect of punishment on terror prevention relative to each country. Finally, Part V will analyze some laws’ positive impacts in the terrorist-financing context and will use these positive impacts to propose a unique solution to the problem of the growing use of social media by terrorist organizations and their supporters.

II. TYPES OF TERRORISM SUPPORT

A. FINANCIAL

“Terrorist financing involves the raising and processing of assets to supply terrorists with resources to pursue their activities.”  

15 In 2005, the United Nations established the Counter-Terrorism Implementation Task Force (“CTITF”) “to ensure overall coordination and coherence in the counter-terrorism efforts” among its member states.  

16 According to the CTITF, “[t]errorism financing incorporates the distinct activities of fund-raising, storing and concealing funds, using funds to sustain terrorist

---


organizations and infrastructure, and transferring funds to support or carry out specific terrorist attacks.”17

The United Nations views funding of terrorist activities separately from terrorist acts.18 Although the International Institute for Counter-Terrorism recognizes that “one man’s terrorist can be another man’s freedom fighter,”19 financial support of a terrorist group or a terrorist activity is an international crime.20 In the five years after the United States began its “War on Terror” in 2001, the United States froze more than $140 million in terrorists’ assets worldwide in more than 1,400 bank accounts.21 However, terrorism financers have adapted and have begun to hide financing through charity organizations and business fronts.22 Nations have adapted to catch terrorist financers, but punishment for these crimes varies from nation to nation.

_________

17 Id. at 3.
18 Id. at 5 (“Making the financing of terrorism a legal offence separate from the actual terrorism act itself gives authorities much greater powers to prevent terrorism.”).
22 Id.
B. SOCIAL MEDIA

Social media “allows individuals to ‘share information, ideas, personal messages, and other content ([such] as videos)’ around the world” via the Internet. Popular social media platforms include Facebook, Twitter, YouTube, and Instagram. “In 2013, it was estimated that one in four people worldwide used social networks, rising from 1.47 billion people in 2012 to 1.73 billion in 2013,” and an estimated 2.55 billion people will be using social media by 2017. Social media is low cost and extremely easy to use and therefore enables users to spread information rapidly around the world.

Terrorist groups, such as the Islamic State of Iraq and Syria (“ISIS”), exploit the use of social media for recruitment and support. In 2015, Michael Steinbach, the assistant director of the FBI’s counterterrorism division, told the House Homeland Security Committee that “foreign terrorist[s] now ha[ve] direct access [to recruiting] . . . like never before[].” A significant concern is that it takes only one sympathizer who reads terrorist propaganda on social media to carry out an attack anywhere in the world.

24 Id. at 286.
25 Id. at 286-87 (footnotes omitted).
26 Id. at 288.
28 Id.
29 Id.
Consequently, social media has become such an effective tool for terrorist groups.

As of 2015, approximately ninety percent of organized terrorism on the Internet was carried out through social media. Terrorists now have direct access to their target audience: young people susceptible to their propaganda. Through social media, terrorists can lead audiences to additional extremist websites, post execution videos, communicate and coordinate attacks, and promote propaganda to influence their audience to join their cause.

Social media is a dangerous outlet for terrorism. It appears that terrorist groups have found a direct and effective way to communicate their messages and propaganda and spread their influence. If social media platforms such as Facebook, Twitter, YouTube, and Instagram know that their platforms are used to spread terror, are they consequently complicit in the ultimate outcome? If so, what type of punishment should they receive? What about individuals who “like” and “share” the propaganda on their own personal pages? Are they responsible for any consequences that may result?

30 Wu, supra note 23, at 288 (footnote omitted).
32 Wu, supra note 23, at 289 (footnote omitted).
III. Disparities Amongst Nations

Nations are aware of the different forms of terrorism support.33 Yet, they differ in how they choose to combat financial and social media backing. Below is an examination of the similarities and differences in the laws and sentencing used to prosecute terrorism support in England, France, and the United States.

A. England


In England, it is a criminal offense to invite another person to provide funds, receive funds, or provide funds themselves with the reasonable or actual knowledge that the funds will be used to support terrorist activities.35 Additionally, it is an offense to be involved in a money-laundering arrangement that results in terrorist funding.36

36 Id. c. 11, s. 18(1)-(2).
Moreover, it is illegal for an individual to withhold information of terrorist funding that he or she has been made aware of through his or her business, profession or employment. In England, cash used to fund terrorist activities can be seized for 48 hours, or forfeited completely by a Magistrate’s Court order.

A conviction in the U.K. of financing terror or money laundering for terrorist activities, is subject to a maximum of 14 years in prison or an unlimited fine or both. However, there are very few convictions. Between September 11, 2001 and December 31, 2007 only 17 percent of all charges made under the Terrorism Act 2000 were due to financial crimes. Additionally, only 11 people were convicted under sections 15-19 of the Terrorism Act 2000 between September 2001 and 2009. The low number of prosecutions can be partly attributed to Part III of the Terrorism Act 2000, which forces the prosecution to prove the terrorist element. Evidence demonstrating that the individual charged knew or reasonably should have known that his or her actions were contributing to a terrorist activity or organization is rare. Due to the small number of prosecutions, the only sentencing guideline for these offenses is section 30 of the Counter-Terrorism Act, which states that “if an offense has a terrorist connection the court must treat that as an aggravating factor and sentence accordingly.”

37 Id. c. 11, s. 19(1).
40 Id.
41 Id.
42 Id.
43 Id. at 53, 54.
Additionally, it is a criminal offense in Britain to publish statements, that directly or indirectly encourage others to commit acts of terrorism.\footnote{Terrorism Act 2006, c.11, s.1.} This includes statements that ‘glorify’ terrorism, which may be understood as attempts to encourage others to commit terrorist acts.\footnote{Id.} A person convicted of this offense faces a maximum of seven years in prison, a fine, or both.\footnote{Id. at (7)(a).} Since 2010, the English government has censored over 90,000 pieces of terrorist related material on social media.\footnote{Jon Stone, Counter-terror police have censored 90,000 pieces of terrorist material on social media, THE INDEPENDENT (June 19, 2015), http://www.independent.co.uk/news/uk/politics/counter-terror-cops-have-censored-90000-pieces-of-terrorist-material-on-social-media-10330810.html.} The U.K. police created The Counter Terrorism Internet Referral Unit in 2010 to remove unlawful material from the Internet.\footnote{Id.} The unit is able to take down Internet material that incites or glorifies terrorist acts pursuant to section 3 of the Terrorism Act 2006.\footnote{Id.} Government authorities in the U.K. also encourage social media companies to cooperate by removing and referring terrorist activities on their social media sites to law enforcement.\footnote{Id.}

B. \textbf{France}

Money laundering and terrorist financing is addressed in Article 324-1 of France’s penal code.\footnote{C PÉN. Article 324-1.} Although the code
is directed at money laundering generally, it is used to address the financing of terrorism as well.\textsuperscript{52} “Certain professions and organizations are subject to a due diligence requirement, under which they have to produce declarations of suspicion concerning operations they find suspect.”\textsuperscript{53} Therefore, this regulatory requirement of French organizations and business requires oversight that may detect possible terrorist financing. Article 421-2-2 of the French Penal Code is also used to combat money laundering and terrorist financing\textsuperscript{54} this section criminalizes:

“financ[ing] a terrorist organization by providing, collecting or managing funds, securities or property of any kind, or by giving advice for this purpose, intending that such funds, security or property be used, or knowing that they are intended to be used, in whole or in part, for the commission of any of the acts of terrorism [listed in the penal code], irrespective of whether such an act takes place.”\textsuperscript{55}

The penalty for money laundering and terrorist financing is 5-7 years imprisonment and a fine.\textsuperscript{56} French authorities also

\textsuperscript{53} Id.
\textsuperscript{54} Id.
\textsuperscript{55} C PÉN. Article 421-2-2.
\textsuperscript{56} C PÉN. Article 324-1; 421-2-3.
cooperate with international organizations to combat money laundering and terrorist financing.\textsuperscript{57}

Further, publicly condoning acts of terrorism is a crime under Article 421-2-5 of the French Criminal Code punishable by up to 5 years imprisonment and a fine.\textsuperscript{58} The penalty is even more severe if the crime is committed online—punishable by up to 7 years in prison.\textsuperscript{59} Additionally, Article 421-2-5-2 of the French Penal Code criminalizes the habitual consultation of websites endorsing terrorism, with exceptions to those who visit the websites in good faith.\textsuperscript{60} On February 9, 2015 France passed a decree allowing the French government to “block websites accused of promoting terrorism and publishing child pornography, without seeking a court order.”\textsuperscript{61} Under the law, internet service providers “must take down offending websites within 24 hours of receiving a government order.”\textsuperscript{62} France’s President at the time, Francois Hollande, stated that the law makes companies like Facebook “accomplices” to terrorism.\textsuperscript{63}

\begin{flushright}
57 Id.
58 C PEN. Article 421-2-5-2.
59 Id.
60 Id.
62 Id.
63 Id.
\end{flushright}
C. THE UNITED STATES

In the United States, “[t]he primary statutes used to charge terrorist financing and facilitation are codified in section 18 U.S.C. §§ 2339A–2339D (the material support and terrorist financing statutes), section 50 U.S.C. §§ 1701–05 (the International Emergency Economic Powers Act (IEEPA)), and section 18 U.S.C. § 1956(a)(2)(A) (international money laundering).”64 In the United States, any person who:

“directly or indirectly, unlawfully and wilfully provides or collects funds with the intention that such be used, or with the knowledge that such funds are to be used, in full or in part, in order to carry out [a terrorist attack] shall be punished.”65

If convicted the offense carries a fine or a prison sentence of up to 20 years or both.66

The United States Department of Justice encourages Assistant U.S. Attorneys to charge terrorist financing under multiple illegal financing statutes, not just statutes specifically related to terrorism, because the “knowing” and “intent” elements to “carry out” a terrorist activity of section 18 U.S.C. § 2239C are hard to prove.67 Charging under multiple statutes leaves more room to attach the appropriate

---

66 Id. at (d)(1).
67 Terrorist Financing, supra note 66 at 9.
charging language. Conviction under section 18 U.S.C. § 2239A-D carries a sentence of anywhere from 10 years to life.

Conversely, the United States has no comprehensive legislation to combat the use of social media by terrorist groups. However, there have been instances where Facebook and Twitter have actively deleted accounts for posting graphic material. For example, on August 19, 2014 ISIS posted the beheading of American journalist James Foley on YouTube and then again on Twitter. The next day Twitter CEO, Dick Costolo promised his company would actively pursue the removal of accounts. However, a short time after Costolo’s statement, four more ISIS beheadings were posted on Twitter and four months later ISIS executions reached their peak on the social site.

Nevertheless, there has been some progress. In the first half of 2017, Twitter alone shut down nearly 300,000...
terrorism-related accounts. Additionally, “Facebook has developed new artificial intelligence programs to identify extremists posts . . . .” However, terrorist accounts usually resurface under different names at a faster pace than social media outlets (armed with manpower oversight) can handle. “The terrorists behind such accounts are hard to identify because they often sign into the [social media] platforms through virtual private networks, or VPNs, hiding their identities and locations.”

In December of 2015, the United States House of Representatives passed the Combat Terrorist Use of Social Media Act to ameliorate the lack of direction and effectiveness in the fight against terrorists’ use of social media. The bill requires the President of the United States to create a strategy to combat terrorism on social media and to present social media related training for law enforcement to Congress. Yet, the U.S. Senate has not approved the bill. Over the summer of 2015, Facebook and Twitter pushed back against the Senate’s proposals to require the companies to alert federal authorities of suspected terrorist activity on their sites.

75 Id.
76 Id.
77 Id.
IV. THE EFFECT OF THE LAWS

A. ENGLAND

Have the sentencing laws and enforcement procedures in England, France, and the United States put in place to combat financial support terrorism and social media use by terrorist organizations had any positive affect? To determine the answer to this question, the measure of the effect must be defined. For the purposes of this analysis, this note will consider acts of terror as a consequence and spawn of support through financial money-laundering and social media recruitment.

In the U.K., the choice of priority given to investigation of terrorist related money-laundering activity is determined by British law enforcement agencies.\textsuperscript{81} There were only seventeen convictions under the U.K.’s terrorism financing laws from 2001 to 2014; however, this number is not fully reflective of the number of terrorism financers who are caught and punished.\textsuperscript{82} Some terrorist financing activities involved other crimes, and in connection, British law enforcement authorities chose to punish suspects under the crime carrying the harsher punishment.\textsuperscript{83} Additionally, financers are sometimes prosecuted under non-terrorist specific money-laundering legislation.\textsuperscript{84}

\begin{flushleft}
\textsuperscript{82} \textit{Id.} ¶ 11.7, at 90.
\textsuperscript{83} \textit{Id.}
\textsuperscript{84} \textit{Id.}
\end{flushleft}
In England, if a person is suspected of terrorist activity and financing, the English government can freeze his or her assets pursuant to the Terrorist Asset Freezing Act of 2010. This act was implemented in accordance with the UN Security Council and European Community regulations. British authorities only need a to have a reasonable belief that the suspect is involved in terrorist financing to freeze a suspect’s assets. In addition, the asset freeze must be considered necessary for purposes connected with protecting the public from terrorism.

However, when it comes to social media, British lawmakers believe that sites such as Facebook and Twitter, are “consciously failing” at preventing terrorist propaganda from spreading on their platforms. In 2016, the U.K. Parliament’s Home Affairs Select Committee conducted an investigation to examine the recruitment efforts of various terrorist organizations.

Lawmakers concluded that social media platforms have become recruiting grounds for terrorists. These lawmakers wrote that companies like Facebook and Twitter “must accept that the hundreds and millions in revenues generated from billions of people using their products needs to be accompanied by a greater sense of responsibility and ownership for the impact that extremist material on their

85 Id. ¶ 11.8 at 90.
86 Id. ¶ 11.9, at 90.
88 Id.
89 Id.
sites is having.”90 They reported that the sites are undermanned in terms of finding and locating extremist accounts and Twitter does not actively report terrorist propaganda.91 However, social media platforms defend their efforts.

Moreover, they are not legally obligated to find and report everything that is written or posted on their platforms. Yet, British lawmakers concluded in a 2016 report that regulations should be in place that equate the same laws from print to social media: “[i]n short, what cannot appear legally in the print or broadcast media, namely inciting hatred and terrorism, should not be allowed to appear in social media.”92

In December 2016, Alex Younger, the head of the U.K.’s overseas intelligence agency MI6, “described the threat posed by groups such as the Islamic State or its sympathizers as ‘unprecedented.’”93 However, there have only been two terrorist-related incidents since the 2005 London bombing as of the authoring of this note (an al-Qaida inspired murder in 2013, and the Westminster attack of 2017).94 This can be attributed to British intelligence agencies innate abilities to infiltrate money laundering and terrorist support schemes.95

90 Id.
91 Id.
92 Id.
94 Id.
95 Id.
Additionally, after the London bombings, English intelligence agencies focused their efforts on the entire region of the U.K. not just major cities in the U.K. This undoubtedly made it harder for terrorism supporters to flourish and accomplish their goals. It can be inferred that with intelligence dispersed throughout the region, infiltration into terrorist networks is markedly easier. Likewise, after the London bombing of 2005, intelligence agencies within the U.K. opened their lines of communication and cooperation with each other and expanded their number of personnel.

B. FRANCE

In France, there is a “requirement for all persons transporting money, securities or stocks worth more than $10,582.50 to declare it to customs.” Additionally, there are certain professions and organizations subject to the due diligence requirement under French law in which they are required to produce information regarding suspicious financing activities. France works closely with international organizations directed at combating the financing of terrorist organizations, and complies with United Nations resolutions.

96 Id.
97 Id.
99 Id.
to pursue and interrupt international terrorist money laundering schemes.\textsuperscript{100}

France also adopted a financial intelligence unit called TRACFIN.\textsuperscript{101} It operates under the authority of the Ministry of Finance and Public accounts and its “mission is to fight against clandestine financial circuits, money laundering and terrorist financing.”\textsuperscript{102} The unit collects, analyses, puts together and processes all information leading to establishing the origin or the destination of criminal financial transactions . . . .”\textsuperscript{103} There were 28 convictions of money laundering in France in 2011 alone.\textsuperscript{104}

When it comes to social media, French authorities take an extremely firm approach enforcing their already strict laws. The French actively detain citizens for their social media posts if the posts are in any way considered to be a threat or terrorist propaganda.\textsuperscript{105} For example, in January 2015, French authorities detained 54 people and jailed several others for remarks shouted in the street or posted on social media.\textsuperscript{106} Furthermore, after the Charlie Hedbo attacks in Paris, a man was sent to prison for a year after he was arrested in Nanterre (a city east of Paris) for “posting a video

\begin{itemize}
\item \textsuperscript{100} Id.
\item \textsuperscript{102} Id.
\item \textsuperscript{103} Id.
\item \textsuperscript{106} Id.
\end{itemize}
on Facebook that mocked policeman Ahmed Merabet, who was shot at point blank range” by one of the Charlie Hedbo terrorist attackers.\textsuperscript{107}

Nevertheless, the strict laws do not prevent everything. There are still examples of terror infused in or with social media in France such as a June 14, 2016 attack, where a pledged Islamic terrorist, brutally stabbed and murdered a police officer and his wife, and posted the aftermath on a Facebook live streaming video.\textsuperscript{108} The attacker was seen pledging his allegiance to ISIS in the video and contemplating what to do with the murdered couple’s 3 year-old son.\textsuperscript{109} It is apparent that harsh French laws still cannot control situations such as these from happening.

Despite France’s punitive social media and money laundering laws, France has seen a recent uptick in terrorist attacks.\textsuperscript{110} Since March of 2012 there have been 16 major terrorist attacks in France.\textsuperscript{111} These attacks include “the killing of soldiers and schoolchildren by a lone gunman in the Toulouse region, shootings at the Charlie Hebdo offices in Paris, and a coordinated assault by gunmen and suicide bombers on a concert hall, a major stadium, restaurants and bars in Paris” and the Bastille Day massacre.\textsuperscript{112}

\begin{flushleft}
\textsuperscript{107} Id.
\textsuperscript{109} Id.
\textsuperscript{111} Id.
\textsuperscript{112} Id.
\end{flushleft}
C. United States

The United States has seen similar results as France. There have been 9 major terrorist attacks in the United States since July of 2009.113 A July 2016 report published by Fordham Law School’s Center on National Security said, “around 9-in-10 of the 101 terrorism cases opened by U.S. prosecutors between March 2014 and June 2016 involved suspects who used social media.”114 The United States is not as strict when it comes to social media laws and enforcement as France, even though it appears social media is being used to spread terror here as well.

However, from the standpoint of terrorist financing, the United States combats the issue just as well as France and the U.K. The United States’ preventative approach has been successful in making it exceedingly more difficult for terrorists and their facilitators to “access and abuse the regulated U.S. and international financial system.”115 One effective tool has been the U.S.’ focus on the importance of financial intelligence collected and disseminated by domestic financial institutions.116 Additionally, regulations

---

113 Paul Sperry, America Has Suffered a Terror Attack Every Year Under Obama, NEW YORK POST, (June 16, 2016), http://nypost.com/2016/06/16/america-has-suffered-a-terror-attack-every-year-under-obama/.
116 Id. at 22.
and government guidance “have aided financial institutions in identifying and managing risk.” As well, this has “provided valuable information to law enforcement, and created the foundation of financial transparency required to deter, detect and punish those who would abuse the U.S. financial system to launder the proceeds of crime and move funds for illicit purposes [including terrorist financing].”

The laws and enforcement procedures regarding terrorism financing that have been implemented by the U.S., France, and the U.K., appear to be working to a large degree. Today, it is more common to see lone wolf attacks orchestrated at low financial costs as opposed to large coordinated attacks like 9/11 that involve large amounts of financing and personnel. Terrorist groups like ISIS have transitioned to low cost recruitment and coordination over social media. Therefore, it is up to the international community to come together to fight the issue by implementing a unified plan to combat those who use social media in support of terrorism.

117 Id.
118 Id.
V. INTERNATIONAL SOLUTION TO THE USE OF SOCIAL MEDIA BY TERRORIST ORGANIZATIONS

As noted above, the international community has been able to reign in broad financing of terrorist organizations by cooperation and intelligence sharing. Cooperation and intelligence is key to combating any aspect of terror. Therefore, cooperation and intelligence should be at the core of any solution to the increasing threat of social media and terrorism. Ban Ki-moon, Secretary General of the United Nations, described the threat of social media and terrorism as follows, “[t]he internet is a prime example of how terrorists can behave in a truly transitional way; in response, States need to think and function in an equally transitional manner.”

Furthermore, regarding groups like ISIS, “[s]ocial media has empowered ISIS recruiting, helping the group draw at least 30,000 foreign fighters, from some 100 countries, to the battlefields of Syria and Iraq . . . [i]t has aided the seeding of new franchises in places ranging from Libya and Afghanistan to Nigeria and Bangladesh . . . [i]t was the vehicle ISIS used to declare war on the United States . . . [a]nd it is how the group has inspired acts of terror on five continents.”

Something must be done.

One solution this author proposes is to use encryptions to decode certain coded messages posted to social media, similar to what France recently suggested to

---


the European Union. The French proposed working with social media outlets to limit the use of encrypted messaging by radical terrorists.\textsuperscript{123} Encrypted messaging and VPNs are mainly used to maintain privacy, but nations should impose regulations limiting the use of encryption technology used on social media outlets if social media companies are not able to limit the propaganda.\textsuperscript{124} Additionally, governments should maintain oversight of flagged language shared over social media. As previously mentioned, social media groups conduct their own oversight of terrorist propaganda. However, social media outlets are severely understaffed to adequately supervise the situation.\textsuperscript{125} A state oversight solution will allow government intelligence officials to take on some of the burden that social media outlets are unable to meet.

Once implemented, nations can share collected data with each other. The measure may potentially warn of future attacks discussed in code on social media, and can be useful as evidence in prosecutions of criminal terrorists using social media prior to, during, or after their attacks. It will also solve the concern shared by social media companies that are weary of laws forcing them to report terrorist activity. With the government involved in oversight of flagged posting activity, the full brunt of liability will no longer be on the social media outlet. In fact, the United States’ Department of

\begin{flushleft}
\textsuperscript{125} Id.
\end{flushleft}
Homeland Security has already begun such “flagging” measures with general online use. Considering the threat social media now presents in this arena, a similar flagging scheme should be implemented specifically for social media sites.

ISIS, Hamas, Hezbollah, and the al Qaeda branch in Syria, al-Nusra front, are all on Twitter, and neither Twitter nor national governments are shutting them down. This needs to change. In addition to “flagging,” accounts registered to known terrorist organizations must be terminated. Implementing what British lawmakers prescribed in 2016 may be the best solution: If it is illegal to print it, it should be illegal to post it. Accounts that post illegal terrorist activity should be immediately terminated. If the social media outlet does not shut down the account, then the situation should become a matter of national security, and government authorities with jurisdiction should step in.

The main concern shared by social media outlets, is legislation that would require them to report any wrongdoing. This concern is legitimate. It is impossible to catch every instance of propaganda or coordination, and

---


social media companies should not be held responsible if they miss one. However, enforcing account shut downs for flagged language, propaganda, or simply because the account itself is the account of a known terrorist group or sympathizer is much different than the duty of searching and reporting content.

What about free speech rights in countries like the United States? One may assume that shutting down social media accounts may cause legal issues, however, the United States Supreme Court in *Holder v. Humanitarian Law Project*, held that if someone has aided a terrorist organization, his or her free speech rights are no longer protected.129 Additionally, the Supreme Court defined terrorist aid as material support for a terrorist group that does not require knowledge by the perpetrator that the support would directly aid the group, only knowledge of the group’s connection to terrorism.130 This may be interpreted to apply to the use of social media to support a terrorist activity or group. A similar rationale should be taken with legislation amongst the international community. The author proposes that any individual, through their social media account that posts any type of material that is flagged, or that can be interpreted as support, sympathy, or propaganda for a group known to be or associated with terror, should not automatically be considered protected by the full weight of any country’s speech laws.

Once the laws are implemented, it is also crucial for the international community to carry out a consistent punishment. Enforcement and reprimand for violating the laws must be congruent. If anything, the international

---

130 *Id.* at 16-17.
community’s fight against terror demonstrates that a unified direction and cohesiveness amongst nations is the key to success. When allied nations in the fight against terror are presented with a similar problem, a similar solution should be the answer.

France has some of the harshest social media laws in the world and yet, they are still subject to attacks. Conversely, the United States has some of the weakest social media punishments in the world yet, the results are the same. So, what should be done?

One solution may be found using a preemptive, preventative action theory for suspected violators on social media. Instead of imposing long prison sentences and running the risk of wrongful convictions for social media posts, detention and questioning should be the course of action. On its surface this seems like a harsh course of action. However, when compared to the potential consequences of inaction, the author asserts that it is a necessary step to combat the threat. It is not a new suggestion and in fact, detention and questioning an individual for posting suspicious language on social media has happened before in the United States. In 2013, a Saint Louis man posted on twitter language that referenced the Boston Bombing when

132 Id.
stating his apartment was for rent to interested Bostonians visiting for the World Series. The man was arrested and charged for the post.

Through detention and questioning, more information can be gained, bargains can be made, and further necessary action can be taken. Additionally, this may not only deter online social media terrorist supporters from using social media, but it may also deter terrorist organizations from promoting social media’s use. For example, if ISIS knows that the international community has implemented the enforcement regulations discussed in this Note on social media, and the response to the violations is detention and questioning, why would the group risk having any members detained who may potentially give up valuable information?

Moreover, the solution may not only be preventative, but may also operate as a deterrence. If a perpetrator is found to have purposefully supported terror during detention and questioning, then the suspect should be subject to the criminal terrorism laws of the country with jurisdiction. This immediately makes the risk not worth the reward. If a terrorist uses social media to coordinate a terrorist plot, he or she should be caught, questioned and punished.

VI. CONCLUSION

Terrorist organizations have adapted. They still require funding, but their illegal money supply is not as easy to obtain as before. Money laundering regulations

134 Id.
135 Id.
implemented around the world coordinated through intelligence sharing and cooperation amongst the international community has contributed to such. Instead, groups like ISIS have taken to social media to recruit sympathizers to carry out lone wolf attacks in the name of their organization. Their ends are still accomplished, but their means have become radically simplified. It is time the international community adjusted and recognized this new avenue as a growing threat for terror.

Terrorist organizations have taken advantage of an industry spawned by the ideals of western culture. They have used something innately western and the embodiment of freedom and of expression to attack just that. A proper response by the international community is needed. If all nations can work together against each new arena the enemy tries to use against us, we can all help to ensure our mutual safety.

“The only thing necessary for the triumph of evil is for good men to do nothing.”

Edmund Burke