NOTE

THE INCITEMENT OF TERRORISM ON THE INTERNET: LEGAL STANDARDS, ENFORCEMENT, AND THE ROLE OF THE EUROPEAN UNION

Ezekiel Rediker*

INTRODUCTION

Consider this sentence: “The Shining Path is a heroic organization.” Over the past thirty years, the Shining Path has waged a violent guerrilla war against the Peruvian government, prompting the European Union to designate the group as a terrorist organization.¹ In certain European countries, speech inciting or glorifying terrorist organizations is criminalized.² As a result, citizens risk prosecution if they do not carefully limit what

* J.D. candidate, May 2014, University of Michigan Law School. I thank my editors, the European Union Law Colloquium, and Professor Daniel Halberstam for guidance on this Note.

² See infra Part III.
they say about the Shining Path, or other terrorist organizations. But where does free speech end and *incitement* to terrorism begin?

The debate over free speech and incitement to terrorism is actively being played out on the Internet. In recent years, Islamic fundamentalists have used the Internet as a tool to radicalize discontented citizens throughout Europe.\(^3\) Several of these radicalized citizens have committed terrorist attacks.\(^4\) In response, the European Union (EU) has taken strong action to police the Internet. Specialized European agencies have developed sophisticated means of policing cyberterrorism. CleanIT is the most well-known Internet policing program: it seeks to shut down websites associated with the dissemination of terrorist information.\(^5\) Increased law enforcement has been accompanied by international and regional initiatives to criminalize cyberterrorism. In 2004, the European Council coordinated the Convention on Cybercrime, which raised criminal penalties for Internet crimes and hate speech.\(^6\) In the aftermath of the Convention, the European Union passed a Framework Decision aimed at criminalizing the incitement of terrorism.\(^7\)

Despite increased enforcement, there is widespread uncertainty about what constitutes the incitement of terrorism in the European Union. The EU has taken the unfortunate half measure of advocating that member states criminalize the glorification of terrorism, but has provided little guidance about what constitutes terrorism or glorification. As a result, states have adopted fractured approaches. The law must be clear enough for any person to judge whether or not his speech might be in violation, but the fractured approach renders such judgment impossible. National courts have reacted against *incitement* prosecutions by narrowly construing the language of broad legislation.\(^8\) On the regional level, the European Court of Human Rights (ECtHR) has been one of the leading judicial bodies in judging the balance between free speech and *incitement* to terrorism, using a multitude of factors to guide its analysis.\(^9\)

This Note argues that the European Union should reconsider the ambiguous language of its Framework Decision in line with judgments by national courts and the ECtHR. Although the Lisbon Treaty formally abolished framework decisions in favor of directives and regulations in the

---


8. See infra Section III.B.

9. See infra Section III.C.
area of criminal justice, the EU should assemble a set of directives to clarify its position on cyberterrorism and free speech. Elements worthy of consideration include subjective intent, the likelihood of violence, and causality. The EU should be particularly mindful of the challenges posed by the Internet, especially as it relates to public vs. private speech in the incitement context. A clearer EU standard on the incitement of terrorism would serve as a model for member states to ensure that legal standards are sufficiently clear, thereby avoiding the welter of conflicting approaches and judgments that offer little guidance to citizens or prosecutors. Any accompanying law enforcement should seek to understand root causes of discontent, while engaging at-risk communities to counter terrorism and violence.

I. BACKGROUND: CYBERTERRORISM, PROPAGANDA, AND THE DEBATE ON “INCITEMENT”

In October 2005, British police raided an apartment in West London. There, they arrested Younis Tsouli, the 22-year-old son of a Moroccan tourism official. Tsouli’s Internet alias was “Irhabi007,” a name under which he labored as one of the most notorious “cyber-jihadists” in Europe. He regularly distributed radical propaganda, including statements by the late Abu Musab Al-Zarqawi, Al-Qaeda’s leader in Iraq. He used his studies in information technology to hack into different databases, including the Arkansas Highway and Transportation Department, to distribute large video files glorifying terrorist acts. Tsouli used stolen credit card numbers to create jihadi websites and was implicated in complicated terrorist plots centered in numerous countries throughout Europe.

Younis Tsouli was described as “Al-Qaeda’s most famous web propagandist.” He facilitated contacts between thousands of individuals, capitalizing on the virtual anonymity of the Internet to advance his cause. UK prosecutors charged Tsouli alongside Waseem Mughal, a British-born graduate of biochemistry, and Tari al-Daour, a United Arab Emirates-
born law student. The three pled guilty to charges of incitement to murder and conspiracy to murder. Tsouli was sent to jail for ten years. The other men received shorter sentences.\footnote{Id.}

The United Nations Office on Drugs and Crime (UNODC) divides cyberterrorism into six different categories: propaganda, financing, training, planning, execution, and cyber-attacks.\footnote{United Nations Office on Drugs and Crime, The Use of the Internet for Terrorist Purposes 3 (2012) [hereinafter UNODC Report].} Propaganda, which is not per se illegal, lies on one end of the spectrum.\footnote{Id. at 6 (“While propaganda per se is not generally prohibited, the use of propaganda by terrorists to incite acts of terrorism is considered unlawful by many Member States. The Internet provides an abundance of material and opportunities to download, edit and distribute content that may be considered unlawful glorification of, or provocation to, acts of terrorism.”).} On the other end are cyber-attacks, which generally refer to the use of computer networks “to disrupt computer systems, servers, or underlying infrastructure, through the use of hacking, advanced persistent threat techniques, computer viruses, malware, phlooding, or other means of unauthorized or malicious access.”\footnote{Id. at 11.} Cyber-attacks are clearly illegal. Cyberterrorism is defined broadly and includes a number of possible elements. The Internet is a versatile medium that allows extremist groups to reproduce content on a widely accessible scale. The Dutch domestic intelligence service once “describe[d] the Internet as the ‘turbocharger’ of radicalisation.”\footnote{European Parliament, Comm. on Foreign Affairs, Cyber Security and Politically, Socially, and Religiously Motivated Attacks 13 (2009) [hereinafter EU Parliament Report] (by Paul Cornish).} In the UK, security agencies have been described as fighting a “covert war in cyberspace against extremist Islamist Internet sites.”\footnote{Kim Sengupta, Spies Take War on Terror into Cyberspace, INDEPENDENT, Oct. 3, 2008, http://www.independent.co.uk/news/uk/crime/spies-take-war-on-terror-into-cyberspace-949706.html.} According to the charges against him, Younis Tsouli was a leader of this covert war, inciting terrorist acts and contributing logistical support to terrorist plots.

The Internet creates fora where users may download and distribute content associated with terrorism. Scholars have used several metaphors to understand the role of the Internet: some argued that it is “not a ‘virtual training camp’” but is instead a “resource bank maintained and accessed largely by self-radicalized sympathizers.”\footnote{Anne Stenersen, The Internet: A Virtual Training Camp?, 20 Terrorism & Pol. Violence 215, 216 (2008).} The Internet is an online library for Islamic religious literature, political opinion, and detailed instruction manuals on guerilla warfare and tactical operations training.\footnote{Id. at 215.} Many of the manuals borrow heavily from the U.S. Army Field Manual.
Others are the original work of jihadis with military experience.\textsuperscript{25} Former soldiers from the Afghan Wars, Palestinian militants, and Internet users without combat experience have all contributed to the abundance of Internet literature.\textsuperscript{26} One “al-Qaeda jihadi Internet forum” has uploaded a fifty-one page manual entitled “The Art of Recruitment,” intended to show how individuals can be recruited and “eventually establish active terrorist cells.”\textsuperscript{27} In certain cases, radical groups offer interactive tutorials on subjects ranging from weapons handling to writing malicious code to sabotage computer networks.\textsuperscript{28} The line between training camp and library can be thin.

Policymakers argue that the threat of radicalization in Europe is growing. They cite the explosion of extremist websites in recent years: “from a handful in 2000 to several thousand today.”\textsuperscript{29} Gilles de Kerchove, the EU anti-terrorism coordinator, estimated in 2008 that “about 5,000 Internet sites were being used to radicalise young people.”\textsuperscript{30} Scholars have argued that cyber-terrorism can be viewed as a microcosm of strained relations between Europeans and a growing population of Muslim citizens. European States have actively struggled with how to manage social integration within their borders. To date, Muslims in Europe, especially recent immigrants from the Middle East, remain some of the poorest and politically alienated citizens.\textsuperscript{31}

EU member states have quickly responded to the threat of radicalization. Certain states have passed laws criminalizing the use of propaganda to incite acts of terrorism.\textsuperscript{32} Propaganda, specifically the incitement of terrorism, is one of the more controversial forms of cyberterrorism, since le-

\textsuperscript{25} Id. at 217. (“The Internet contains a vast amount of written training material. There are pamphlets and handbooks available on almost any topic considered relevant for training and preparation. Some of the most common topics are: conventional weapons, improvised weapons and explosives, field tactics, guerrilla warfare, organisational and field security, and physical training. Some of the manuals are plain text, while others, especially manuals aiming to teach practical skills, may be illustrated with explanatory sketches or photos.”).

\textsuperscript{26} Id. at 219.

\textsuperscript{27} EU PARLIAMENT REPORT, supra note 21, at 13.

\textsuperscript{28} Id. at 12 (“With instruction manuals so readily available, the Internet has become a place of teaching and instruction. Interactive tutorials can be offered, in a wide range of subjects from weapon handling through to the skills needed to write malicious code and sabotage computer networks. Tactical and operational training can be conducted through simulators and even online computer games, including Massively Multiplayer Online Role-Playing Games (MMORPGs).”).

\textsuperscript{29} Internet Jihad, supra note 3.


\textsuperscript{31} Anja Dalgaard-Nielsen, Violent Radicalization in Europe: What We Know and What We Do Not Know, 33 STUD. CONFLICT & TERRORISM 797, 798–99 (2010) (“Terrorist attacks, foiled plots, and trials of recent years indicate that ever younger Europeans who did not spend extended periods outside Europe have become involved with militant Islamism and, apparently, radicalized over a very short time span.”).

\textsuperscript{32} UNODC REPORT, supra note 18, at 6.
gal standards vary from country to country. Ben Saul, a Professor of Law at the University of Sydney, wrote, “Propaganda has long been the handmaiden to violence: inciting, justifying and naturalising it; ploughing the ground for violence by softening our psychological defences to it and desensitizing us to its brutalising effects.” But the division between free speech propaganda and the actual incitement of terrorism is often blurred.

The UNODC considers incitement a pre-stage of terrorism. Incitement is often seen as an activity that helps to legitimate terrorism or contributes to terrorist recruitment efforts. The issue of legitimization, however, is particularly vague. There is no fixed definition of incitement, although numerous examples abound in both literature and policy documents. Incitement “can consist of public provocation to commit terrorism or public praise for terrorist acts, dehumanisation of the victims of terrorist attacks, or mere understanding for the underlying reasons for terrorist acts.”

One of the more developed legal understandings of incitement to violence has emerged in the context of genocide. Incitement to violence has been included in international instruments since the end of World War II. The Nuremberg Tribunal convicted and executed Nazi newspaper publisher Julius Streicher for inciting the murder of Europe’s Jews, even though he had not committed any of the murders himself. The Genocide Convention of 1948 formulated the “incitement of genocide,” legal standards that have since been used by the International Criminal Tribunal for the former Yugoslavia and the International Criminal Tribunal for Rwanda.

---

34. UNODC REPORT, supra note 18, at 6. (“Recruitment, radicalization and incitement to terrorism may be viewed as points along a continuum.”).
36. United States Holocaust Memorial Museum, Incitement to Genocide in International Law, HOLOCAUST ENCYCLOPEDIA, http://www.ushmm.org/wlc/en/article.php?ModuleId=10007839 (last updated June 20, 2014) [hereinafter HOLOCAUST ENCYCLOPEDIA] (“The trial of leading German officials before the International Military Tribunal (IMT), the best known of the postwar war crimes trials, formally opened in Nuremberg on November 20, 1945, only six and a half months after Germany surrendered. Among the twenty-four defendants was Julius Streicher, publisher of the antisemitic German weekly Der Stürmer. On October 1, 1946, the IMT convicted Streicher of crimes against humanity in connection with his incitement to the mass murder of Europe’s Jewish population. Streicher was executed for his crimes.”). See also Robert Bernstein et al., Inciting Genocide Is a Crime, WALL ST. J., Available at http://online.wsj.com/news/articles/SB10001424052702303592404577364283553552766.
37. Van Ginkel, supra note 35, at 11 (“[O]ne can better compare the criminalisation of incitement to terrorism to the international crime of incitement to genocide, formulated under the Genocide Convention and also incorporated in the Statute of the International Criminal Tribunal for the former Yugoslavia (ICTY) and the International Criminal Tribunal for Rwanda (ICTR) and in similar terms in the Statute of the International Criminal Court (ICC).”).
Incitement in the context of genocide occurs when one individual uses forms of communication to encourage others to commit crimes. Communication may include broadcasts, publications, drawings, images, or speeches. A necessary precondition of incitement, according to the Genocide Convention, is that the incitement takes a public form and is thus distinguished “from an act of private incitement (which could be punishable under the Genocide Convention as ‘complicity in genocide’).”\(^{38}\) Incitement to genocide must be proven to be “direct,” meaning that the speaker and the listener perceive the speech to be a “call to action.”\(^{39}\) Moreover, incitement to genocide is an inchoate crime: “a proof of result is not necessary for the crime to have been committed, only that it had the potential to spur genocidal violence.”\(^{40}\) In the international context, the speaker’s intent is the most important element of the offense, rather than the actual effect of the speech.\(^{41}\)

The International Court of Justice considered intent as a crucial element during the “incitement” cases associated with the Rwandan Genocide.\(^{42}\) In 1994, Rwandan Radio operators actively encouraged Hutus to hurt and kill Tutsis. “The Rwanda Media Case emphasized that incitement to commit genocide required calling on the audience (be they listeners or readers) to take action of some kind.”\(^{43}\) Absent such a call, inflammatory language may qualify as hate speech but does not constitute incitement. Israeli scholar Yael Ronen explains, “[t]he weight exerted by the inciters on the incitees lies not in the issuance of direct orders; but in sowing and nurturing in their audience the ideological foundation from which the willingness to act then emerges.”\(^{44}\) Ronen stressed that this is accomplished through “[p]ersistent, pervasive vilification and disparagement of the target.”\(^{45}\) Yet Ronen’s definition goes well beyond what the Genocide Convention requires: any speech that prepares the ground for hate among listeners should be criminalized. Drawing from the Genocide Convention, the International Criminal Tribune for Rwanda in \textit{Akayesu} noted that

---

39. \textit{Id.}
40. \textit{Id.}
41. \textit{Id.}
42. \textit{Id.} (“The incitement provision of the Genocide Convention took on new importance in the wake of genocide in the Central African nation of Rwanda . . . In 1997, the United Nations International Criminal Tribunal for Rwanda (ICTR) indicted three Rwandans for ‘incitement to genocide’: Hassan Ngeze who founded, published, and edited \textit{Kangura} (Wake Others Up!), a Hutu-owned tabloid that in the months preceding the genocide published vitriolic articles dehumanizing the Tutsi as \textit{inyenzi} (cockroaches) though never called directly for killing them; and Ferdinand Nahimana and Jean-Bosco Barayagwiza, founders of a radio station called \textit{Radio Télévision Libre des Milles Collines} (RTLM) that indirectly and directly called for murder, even at times to the point of providing the names and locations of people to be killed.”).
43. \textit{Id.}
45. \textit{Id.}
speech must be “public” and “perceived” by both speaker and listener, creating a direct call to action.46

Experts attempt to draw a distinction between direct and indirect forms of incitement, but prevailing legal definitions vary widely. Indirect incitement, often referred to as “glorification” or “apologie,” straddles the fence between legality and illegality. Ronen argues that the criminalization of incitement must include not only direct calls for action, but also any justification or glorification of terrorist acts.47 On this point, Ronen disagrees with the UN Secretary General Ban Ki Moon, who has argued that incitement must be separated from glorification.48 The Secretary General acknowledged that statements of glorification may applaud past acts and might offend the sensitivities of individual persons and society, particularly the victims of terrorist acts.49 But he nevertheless emphasized that vague terms of uncertain scope, such as glorifying or promoting terrorism, are not used when restricting the freedom of expression.50

Despite certain disagreements, experts agree that the offense of incitement to commit a terrorist act will be human rights compliant where incitement is supported by an intention to promote terrorism and a causality link between the incitement and the likely realization of a terrorist act.51 In other words, there must be a link between incitement and act. Glorification without a link to an act should be protected by freedom of speech. Yet even this clarification leaves a host of unresolved questions. What if a group glorifies terrorist acts in general but no specific act is ever committed? What if one group prompts another to commit an act but there is no link between the two groups? Would a teacher be liable if he or she presented a past act of terrorism in a favorable light if a student was then moved to correct a perceived present injustice through an act of terrorism?

II. Free Speech Standards and the International Response to Cyberterrorism

Since September 11, 2001, the international community has orchestrated an organized response to terrorism on the Internet. This Part aims to illustrate the evolution of the free speech standards and corresponding

47. Id.
49. Id. ¶ 61.
50. Id.
international efforts to police cybercrime. Section A traces the evolution of European legal standards governing the freedom of expression and compares them with the American Brandenburg standard. Section B analyzes the international instruments designed to protect the freedom of expression, specifically the International Covenant on Civil and Political Rights (ICCPR). Section C examines the Convention on Cybercrime and global efforts to police terrorism on the Internet.

A. The Evolution of European Standards on the Freedom of Expression

Contemporary standards governing the freedom of expression in Europe have been shaped by the European Convention on Human Rights (ECHR), which was signed on November 4, 1950. Primarily, the Convention sought to address the atrocities of the Second World War. In this way, the Convention was part of a wider human rights agenda, which also included the Universal Declaration of Human Rights. One scholar noted, “It should be taken into account that the European Convention was part of the moral answer to the Nazi ideology after the Second World War and that the patterns followed by the European Court in its case law have been a tribute to this cause.”

The Convention guaranteed a broad range of human rights to citizens of member countries of the Council of Europe, which included almost all European nations. The Convention established the European Court of Human Rights as a forum for individuals to bring fundamental rights claims against European governments. Judgments finding violations are binding on the States concerned and they are obliged to execute them. Yet the Convention recognized that freedom of expression was not an absolute right. The freedoms enshrined in certain sections were counterbalanced by the language from others:

...
As the twentieth century unfolded, European governments sought to use the ECHR as a tool to balance their obligations regarding the freedom of expression. On one hand, the European system considered freedom of expression as a “necessary counterweight” to balance the executive, legislative, and judicial branches of government.\(^{56}\) On the other hand, freedom of expression had limits, especially when it concerned speech that could harm a community. Many European governments passed legislation rendering hate speech unlawful.\(^{57}\) The historical experience of European countries led governments to support free speech, but only up to a certain point past which speech became harmful to society.

European states took another major step on defining freedom of expression when they passed the Charter of the Fundamental Rights of the European Union (Charter). The Charter acquired full legal effect when the Treaty of Lisbon came into force in 2009.\(^{58}\) Freedom of expression is enshrined in Article 11, which reads, “Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.”\(^{59}\) According to the European Court of Human Rights (ECtHR), any restriction on freedom of expression must be expressly established by law and:

> [T]he law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a “law” unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able—if need be with appropriate advice—to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.\(^{60}\)

Further down, Article 52 of the Charter allows for various limitations to be legally imposed, but it reiterates that those restrictions must be “provided for by law and respect the essence of those rights and freedoms.”\(^{61}\) According to the Treaty of Lisbon, the European Union accedes to the European Convention as an entity in its own right, making the Convention and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 222, available at http://www.echr.coe.int/Documents/Convention_ENG.pdf.

56. Úbeda de Torres, supra note 54, at 7.

57. See infra Section III.B.


binding not only on the governments of the member states but also on the supranational institutions of the EU.\footnote{62} Free speech standards in Europe are different than they are in the United States. Historically, the United States has been more tolerant of speech that would be considered unacceptable (or even unlawful) under European standards. In \textit{Brandenburg v. Ohio}, the U.S. Supreme Court articulated the modern American standard on free speech, reversing the conviction of a Ku Klux Klan leader under Ohio state law.\footnote{63} The Court used a two-pronged test to evaluate speech acts: (1) speech can be prohibited if it is “directed to inciting or producing imminent lawless action” and (2) it is “likely to incite or produce such action.”\footnote{64} The Court emphasized that there is a difference between mere advocacy of abstract concepts, and preparing and inciting a group to “imminent lawless action.”\footnote{65} The two-pronged test from \textit{Brandenburg} remains the standard used by American courts to evaluate inflammatory speech. As will be shown throughout this Note, European jurists and policymakers have grappled with the appropriate elements for free speech and have debated the usefulness of both European and American approaches.

\section*{B. The International Protection of Fundamental Rights}

Within the international context on incitement, states have an obligation to uphold the fundamental freedoms of their citizenry, including the freedom of expression. In addition to the Charter of the Fundamental Rights of the European Union and the ECHR, European Union member states are also subject to the International Covenant on Civil and Political Rights (ICCPR) when it comes to addressing the freedom of expression.

The ICCPR was passed in 1976.\footnote{66} The ICCPR contains provisions for both protecting freedom of speech and curtailing freedoms in the interest of national security.\footnote{67} The ICCPR states that maintaining national security and public order are legitimate grounds for limiting freedom of speech. Specifically, Article 19, paragraph 3 and Article 20, Paragraph 2 require States to prohibit national, religious, or racial hatred that constitutes incitement to violence.\footnote{68} Article 15 problematizes the enactment of “incitement” legislation; it requires that governments not hold individuals guilty for crimes that do not constitute crimes under national or international law.\footnote{69}

\begin{footnotesize}
\begin{enumerate}
\item \textit{Id.} at 447.
\item \textit{Id.} at 448.
\item \textit{Id.} at arts. 19–20.
\item \textit{Id.} at art. 15.
\item \textit{Id.}
\end{enumerate}
\end{footnotesize}
The language of Article 19 of the ICCPR and Article 10 of the Charter of the Fundamental Rights of the European Union leave room for ongoing debate. The UNODC notes that “in practice, striking the right balance between preserving the right to freedom of expression and enforcing criminal legislation targeting the incitement of terrorist acts continues to be a challenge for Governments.” Human rights groups have expressed strong skepticism that glorifying terrorism is “sufficiently narrow and precise” to violate the principle of legality and the right to freedom of expression, “as enshrined in articles 15 and 19 of the [ICCPR].”

These two principles, sufficient precision to enable a citizen to guide his or her behavior and the ability of a citizen to foresee the consequences of their speech, have proven problematic in the debate about incitement. To date, terrorism lacks a widely-accepted definition under international law. Sami Zeidan, a Lebanese scholar, has analyzed the obstacles to defining terrorism:

There is no general consensus on the definition of terrorism. The difficulty of defining terrorism lies in the risk it entails of taking positions. The political value of the term currently prevails over its legal one. Left to its political meaning, terrorism easily falls prey to change that suits the interests of particular states at particular times.

British professor Jason Burke echoes Zeidan’s sentiment:

There are multiple ways of defining terrorism, and all are subjective. Most define terrorism as ‘the use or threat of serious violence’ to advance some kind of ‘cause’. Some state clearly the kinds of group (‘sub-national’, ‘non-state’) or cause (political, ideological, religious) to which they refer. Others merely rely on the instinct of most people when confronted with an act that involves innocent civilians being killed or maimed by men armed with explosives, firearms or other weapons.

International groups have expressed an ongoing worry that the rush to criminalize incitement may result in the restriction of free speech. In the Joint Declaration on the Internet and Anti-Terrorism Measures, an interdisciplinary body, comprised of members of the United Nations (UN), Organization for Security and Economic Cooperation, and the Organization of American States, worried “that the standard of restricting expression which amounts to incitement, hitherto well-established in the areas of public order and national security, is being eroded in favour of vague and

70. UNODC Report, supra note 18, at 44.
71. Id. at 6.
72. Van Ginkel, supra note 35, at 12.
potentially very overbroad terms.”75 The UN Secretary General agreed, stating that “the adoption of any overly vague or broad definition of the term terrorism in domestic legislation could lead to criminalization of conduct that does not constitute terrorism as such.”76 The Secretary General further cautioned that there is a danger in definitions that hamper “the legitimate non-violent and peaceful exercise of fundamental rights and freedoms.”77

C. The Convention on Cybercrime

In 2001, the Council of Europe organized the Convention on Cybercrime, the first international treaty78 addressing Internet and computer crime, which entered into force in July 2004.79 The treaty sought to “harmonize national laws,” coordinate law enforcement, and align objectives among participating nations.80 It focused on some of the most widespread and problematic Internet crimes: copyright infringement, fraud, child pornography, hate crimes, and financial crime. To date, 44 states have ratified the convention, while another 9 states have signed the convention but have not ratified it.81

In 2006, the Additional Protocol to the Convention on Cybercrime came into force.82 States that ratified the Additional Protocol agreed to

77. Id.
80. UNODC REPORT, supra note 18, at 20–21. (“For example, the Council of Europe Convention on Cybercrime requires parties to adopt legislation requiring Internet service providers (ISPs) to preserve specified data stored on their servers for up to 90 days (renewable), if requested to do so by law enforcement during the course of a criminal investigation . . . [it] also requires parties to implement legislation relating to the production of stored subscriber data. Such information may be crucial during the investigative stage to establish the identity of a perpetrator of a terrorist act involving use of the Internet, and may include the physical location of such person, as well as other related communication services employed in the commission of the act. The Convention also requires signatory States to establish minimum standards to enable real-time collection of traffic data associated with specified communications and the interception of content data in relation to specified serious offences under domestic law.”).
81. Id.
criminalize the dissemination of racist and xenophobic material through computer systems, and any threats associated with this material. The Additional Protocol has tasked states with balancing the needs of law enforcement with the protection of civil liberties. Specifically, Article 5 of the Additional Protocol must be applied together with the basic provision of Article 12 of the Convention on Cybercrime itself, which states that criminalization must be carried out in a manner that respects human rights. This does not mean that individuals can use free speech to express hateful or violent messages. For instance, the Council of Europe’s Explanatory Report of the Additional Protocol to the Convention on Cybercrime stated the “European Court of Human Rights has made it clear that the denial or revision of ‘clearly established historical facts—such as the Holocaust—[. . .] would be removed from the protection of Article 10 by Article 17’ of the ECHR” when it ruled in the *Lehideux* and *Isorni v. France* case of September 23, 1998.

Advocates argue that the Convention deters cybercriminals from engaging in illicit behavior. The Convention mandates sanctions and makes cybercrimes extraditable offenses, thereby reducing the number of countries in which criminals can avoid prosecution. Critics have observed that transposing Convention provisions into domestic law is difficult. Civil liberties groups have criticized the Convention, arguing that it undermines individual privacy rights. The ACLU, for example, has argued that “US authorities will use the Convention to conduct surveillance . . . that would not be allowed under current US law.” Further, skeptics note that not enough states have signed the Convention for it to have an impact. Cybercriminals often use the Internet portals of Yemen or North Korea to launch attacks; neither country is part of the Convention.

Moreover, the Convention did not fix difficulties associated with international cooperation on incitement offenses. When authorities in one country recognize an instance of cyberterrorism and want to cooperate with another country, it is sometimes significant whether the alleged acts also constitute a crime in the country receiving the request. This can create problems for sharing Internet data and also extraditing individuals

83. *Id.* at arts. 3–4.
84. *Id.* at art. 5; Convention on Cybercrime, *supra* note 80, at art. 12.
87. *Id.* at 3.
88. *Id.*
89. *Id.*
90. *Id.*
91. UNODC REPORT, *supra* note 18, at 97.
accused of committing terroristic acts on the Internet. It is also possible for authorities in one country to encounter difficulties in trying to shut down websites from other jurisdictions due to differing laws about the freedom of expression. As we will see, the difference in national approaches is something that has deeply affected the criminalization of the incitement of terrorism.

III. EU Legal Standards on Incitement and the Challenges of Interpretation

The European Union has encouraged states to criminalize the incitement of terrorism through the passage of its Framework Decisions. But the EU has used uncertain language to describe acts that should be criminalized, leading to a wide divergence of member state approaches. As a result, national courts have restricted the scope of member state legislation criminalizing incitement. The European Court of Human Rights has offered similar guidance in cases balancing the national security concerns with the freedom of expression (enshrined in Article 10 of the ECHR).

Part A considers the growing area of EU criminal law enforcement and analyzes the language of the Framework Decisions. Part B examines the fractured member state approaches to criminalizing the incitement of terrorism, and the role of courts in narrowing broad legislative language. Part C examines ECtHR incitement cases and the multitude of factors that the court uses to guide its analysis.

A. EU Criminal Law and Framework Decisions on Terrorism

The European Union’s Third Pillar represents criminal justice and inter-state cooperation. The first traces of EU criminal law enforcement were found in the Maastricht Joint Actions on organized crime and racism and xenophobia. The Treaty of Amsterdam clarified EU objectives in the area of freedom, security and justice and sparked numerous EU efforts to harmonize substantive criminal law among its Member States. By the mid-2000s, the EU had passed a multitude of initiatives and Framework Decisions to encourage collective cooperation on matter relating to “trafficking in drugs and human beings, human smuggling, environmental crime and, post-9/11, terrorism.” The Tampere Council and the Hague

92. Id.
93. Id. at 96.
95. Id.
96. Id. ("The reasons for this renewed emphasis on the harmonisation of substantive criminal law are threefold. The first reason has to do with efforts to amend and expand existing Framework Decisions taking into account subsequent international developments in the field. The second reason relates to a similar amendment process, but this time linked also with efforts to constitutionally refresh the form of legal instrument used for third-pillar harmonisation (namely to replace the vague Maastricht Joint Actions by the expressly legally binding Amsterdam Framework Decisions). The third reason for new legislation also relates..."
Program adopted the internal market formula of mutual recognition in the third pillar. Extensive legislation accompanied this mutual recognition, especially “in the area of terrorism, organized crime, and illicit drug trafficking in accordance with the relevant provisions set out in of Articles 29–31 EU.”

The European Union has taken an active role in fighting cyberterrorism but cannot be said to have a unified and comprehensive approach. The EU has actively encouraged its Member States to criminalize the incitement of terrorism. To this end, the EU has promoted a legal standard through the adoption of Framework Decisions and the Council of Europe’s Convention on the Prevention of Terrorism.

In 2002, the European Union Council adopted Framework Decision 2002/475/JHA on combating terrorism. This Framework Decision harmonizes the definition of terrorist offenses in all EU countries by adopting a common definition of the term “terrorism.” Article 1 of the 2002 Framework Decision defines terrorism as extending to acts including extensive destruction of government or public facilities or infrastructures. The acts must seriously damage any country or any international organization. The acts must aim to seriously intimidate a population or “unduly compel[]” any government or international organization to perform or abstain from any act or seriously destabilize or destroy the fundamental structures of a country.

The Framework Decision also set forth jurisdictional rules to EU constitutional developments, and consists of the need to address ECJ case law and harmonise criminal law under the first pillar.


99. EU PARLIAMENT REPORT, supra note 21, at 3 (“The EU is very closely engaged in cyber-security but cannot be said to have a comprehensive approach to the problem: the EU’s responses are diverse, lack coherence and could at times conflict.”).

100. A Framework Decision is a legislative act of the EU used only within the EU’s competences in police and judicial co-operation in criminal justice matters. Framework Decisions were similar to directives in that they required member states to achieve particular results without dictating the means of achieving that result. However unlike directives, Framework Decisions were not capable of direct effect, they were only subject to the optional jurisdiction of the ECJ and enforcement proceedings could not be taken by the European Commission for any failure to transpose a Framework Decision into domestic law.

101. UNODC REPORT, supra note 18, at 41.


coordinate terrorism prosecutions and outlined measures to cope with victims of terrorism. The EU Council amended the Framework Decision in 2008. The new version included provisions on public provocation to commit a terrorist offense, recruitment for terrorism, and training for terrorism. The Council drew upon Security Council resolution 1624 (2005), which called upon States to criminalize incitement to commit terrorist acts. The amended Framework Decision creates a legal basis for prosecuting the distribution of terrorist propaganda. The Framework Decision offers precise definitions for terrorist offenses. The Council defines “public provocation to commit a terrorist offence” as the “distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of one of the [terrorist] offences . . . [previously mentioned], where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed.” The incitement of terrorist acts is situated within the larger context of aiding and abetting an offense. Even though the provisions of Framework Decision 2008/919/JHA are not Internet-specific, they cover activities conducted by means of the Internet.

EU member state representatives disagreed throughout the amendment process about how to define “incitement.” Spain and Italy already had laws punishing public incitement to terrorism. But Nordic countries had strong reservations about the restriction of fundamental rights. These countries, along with civil rights campaigners, brought pressure to leave not restrict the freedom of expression. As a result, concepts of incitement, complicity, and attempt were not defined—their definitions were left to the member states.

104. 2002 Framework Decision, supra note 7, at arts. 9–10.
106. Id. at art. 3.
107. Id. at art. 3.
108. Id.
109. See id.; see also OSCE Report, supra note 51, at 5. (“Each Member State shall take the necessary measures to ensure that inciting or aiding or abetting an offence referred to in Article 1(1), Articles 2 or 3 is made punishable.”).
110. UNODC Report, supra note 18, at 23.
111. See Lungescu, supra note 30.
112. Id.
113. Id.
114. Id.
115. Eugenia Dumitriu, The E.U.’s Definition of Terrorism: The Council Framework Decision on Combating Terrorism, 5 German L.J. 585, 599 (2002) (“Whereas terrorist offences and offences linked to terrorist activities are very precisely defined, the same can unfortunately not be said for the concepts of incitement, complicity and attempt, whose definitions are left to Member States.”). See ICJ Report, supra note 103, at 4. (“The ICJ is concerned at the recent trend in European states towards the criminalization of a wider
The compromise created more of a problem than it intended. The EU Network of Independent Experts on Fundamental Rights concluded that “the breadth of the definition of terrorism in the Framework Decision breached[d] the principle of legal certainty.”\textsuperscript{116} The definition of “public speech” and “danger” went unaddressed. The distinction between participation in the activities of a terrorist group and complicity was similarly unacknowledged in the text. The broad and amorphous standard created by the European Union urged member states to criminalize incitement, but provided few guidelines about how to define these complex terms.

B. Fractured Member State Approaches

The European Union’s Framework Decision essentially asked its member states the following question: “[A]t what point exactly does legitimate opinion or political speech about the root causes of terrorism become a justification of terrorism?”\textsuperscript{117} There is no easy answer to this question. Many of the concepts from the Framework Decision were difficult to pin down, putting legislatures at “risk of [using] excessively broad definitions.”\textsuperscript{118} As of 2004, only six EU countries had national legislation defining the “apologie” of terrorism and/or “incitement to terrorism” as a specific criminal offense: Bulgaria, Denmark, France, Hungary, Spain, and the UK.\textsuperscript{119} The rest of the EU member states chose not to enact legislation defining the “apologie” of terrorism and/or “incitement to terrorism” as specific criminal offenses.\textsuperscript{120} Instead, these states relied on their general criminal legislation—from criminal codes, penal codes, and constitutions—to make these offenses prosecutable.\textsuperscript{121} As a result of these different approaches, legislative language varied widely from country to country. Incitement to terrorism was variously described as inducement, incitement, instigation, furthering, motivating or counselling the commission of a crime, or publishing calls for violence.\textsuperscript{122} The issue was further complicated by the fact that some of the variation in language was due to transla-

\begin{itemize}
\item \textsuperscript{117} OSCE Report, supra note 51, at 10.
\item \textsuperscript{118} Id.
\item \textsuperscript{120} Id. at 22.
\item \textsuperscript{121} Id.
\item \textsuperscript{122} Id. at 23.
\end{itemize}
tion. National courts throughout the EU have reacted against the broad scope of these statutes, construing them narrowly to avoid restricting the freedom of expression.

Spain is one of the six countries that has legislation criminalizing the “apologie” or glorification of terrorism. The Spanish Penal Code criminalizes ‘apologia’ (justification) of terrorism and ‘enaltecimiento’ (glorification), including “acts that discredit or humiliate the victims of terrorism.” The law in Spain distinguishes between incitement and apologie; the latter is “understood as a phrase which follows provocation.” “Provocation exists when ‘direct incitement’ to commit a crime is made by means of printed material, radio broadcasting, or another effective method that facilitates publicity.” It does not concern “mere ideologically motivated statements, but the approval of criminal behavior.” To prosecute, the government must consider the incitement dangerous insofar as it may incite others to commit the offense. The offense of “justifying” terrorism is an inchoate offense, meaning that is independent of whether an act is actually committed. In Spain, the government may prosecute public incitement to commit an act of terrorism. Article 578 punishes the crime of praising terrorism, an offence that was incorporated in the Penal Code by Organic Law 7/2000 of 22 December 2000. This article provides that “Apologism or justification by means of public expression or diffusion of the felonies included in articles 571 to 577 of this Code [Crimes of Terrorism] or of anyone who has participated in commission thereof, or in perpetrating acts that involve discredit, disdain or humiliation of the victims of terrorist offences or of their relatives shall be punished with a sentence of imprisonment from one to two years.”

123. Id.
126. Id. at 39.
127. Id. at 44.
128. In Spain, Articles 18 and 579 of the Spanish Penal Code criminalize public incitement to commit an act of terrorism. Article 578 punishes the crime of praising terrorism, an offence that was incorporated in the Penal Code by Organic Law 7/2000 of 22 December 2000. This article provides that “Apologism or justification by means of public expression or diffusion of the felonies included in articles 571 to 577 of this Code [Crimes of Terrorism] or of anyone who has participated in commission thereof, or in perpetrating acts that involve discredit, disdain or humiliation of the victims of terrorist offences or of their relatives shall be punished with a sentence of imprisonment from one to two years.” Arts. 18, 578–79 C.P. (Spain).
130. S.T.S., July 17, 2007 (J.T.S., No. 656) (Spain).
131. Id. See also Briefing Paper, supra note 124, at 7.
risk of a ‘slippery slope,’ i.e. the gradual broadening of the notion of terrorism to acts that do not amount to, and do not have sufficient connection to, acts of serious violence against members of the general population.” 132

In more recent developments, the Court has devoted significant time to narrowing the scope of the Spanish statute. 133 In February 2014, a young Spanish woman was convicted of inciting terror over Twitter. 134 Ms. González Camacho, a student in southern Spain, claimed to be unaffiliated with any political organization. 135 But her tweets had invoked a political group called the Grapo, who had killed more than eighty people in the late 1970s and 1980s. 136 Even though Grapo never formally disbanded, security officials believe it to be no longer operative. 137 According to the New York Times, “[t]he group’s dormancy did not matter to the judge, who accepted the prosecution’s argument, which said that Ms. González Camacho had posted ‘messages with an ideological content that was highly radicalized and violent,’ violating an article in the Spanish Constitution that prohibits any apology for or glorification of terrorism.” 138 The decision was criticized by Spanish criminal attorney Carlos Sáiz Díaz, who claimed that “legislators are always a step behind the new technology . . . We’re moving on unclear ground . . . which runs against the principle of legal certainty.” 139 Ms. González Camacho was sentenced to one year in prison but will avoid jail time under a plea bargain. 140

In the United Kingdom, prosecutors have wide discretion to determine when to prosecute the crime of inciting terrorism. 141 They must take into account the right of freedom of speech, the context in which the statements were made, and the likelihood that they could effectively incite


133. For its most recent decision concerning this issue, see S.T.S., Jun. 5, 2009 (J.T.S. 4503) (Spain). See also Detenido un hombre por enaltecimiento del terrorismo a través de Internet, EUROPA PRESS, Dec. 1, 2009, http://www.europapress.es/portaltic/internet/noticia-detenido-hombre-inaltecimiento-terrorismo-traves-internet-20091201191800.html (describing a case in which a young man was prosecuted by Spanish authorities for ‘enaltecimiento’ [glorification] for posting comments that were disrespectful of two policemen that were killed in a terrorist attack in July 2009.).


135. Id.

136. Id.

137. Id.

138. Id.

139. Id.

140. Id.

141. UNODC REPORT, supra note 18, at 106 (“[Specifically, UK] prosecutors make these decisions in accordance with the Code for Crown Prosecutors, which provides a threshold for charging based on evidential sufficiency and public interest. Prosecutors must be satisfied that the evidence before them discloses a ‘realistic prospect of conviction’ before charging a suspect with a particular offence.”).
others to violence or hostility. In the wake of the 2005 London Bomb- 
ings, the UK developed new policy guidelines. Then-Prime 
Minister Tony Blair proposed a new offense criminalizing the act of glorifying terrorism 
in the UK. This proposal sought to broaden the scope of existing legislation, which only prohibited 
direct incitement to terrorism, by criminalizing glorification language. The initiative to criminalize indirect incitement 
faced withering criticism that the terms ‘glorification’ and ‘indirect encour-
agement’ of terrorism did not allow people to appropriately self-regulate their conduct. The 2006 Terrorism Bill ended up being a compromise 
since it dealt solely with the encouragement of terrorism, which “still re-
 mains wider than the existing law of criminal incitement.”

The UK Court of Appeal overturned the conviction of a group of students who had been convicted under the Section 57 of the UK Terrorism 
Act for inciting each other to terrorism. The students possessed CDs 
with extremist propaganda downloaded from the Internet. They were using 
the material to encourage each other to go to Pakistan to get military training that could be used in the Afghani jihad. The Court applied a 
narrow construction of the offense of incitement, holding that there was 
no clear connection between the possession of extremist propaganda and 
the incitement of an act of terrorism. The UN Policy Department later 
remarked that “the fact of the original conviction, however, shows the risk 
herent in legislation that is broadly drawn.”

Germany is one of the many European countries that does not have a 
specific statute criminalizing incitement. The German Penal Code covers “incitement” to terrorism under Section 130, Sub-Section 1, Paragraph 1. 
Specifically, a person must disturb the public peace by inciting “hatred against sections of the population or calls for violent or arbitrary measures

142. Id. at 39.
143. Minder, supra note 134.
146. R. v. Zafar, [2008] EWCA (Crim) 184, [49], [2008] Q.B. 810 (Eng.). At trial, Zafar and Iqbal were acquitted on one count, which charged them with possession of three “philosophy discs” containing material emanating from Raja; however, they, together with the other defendants, were found guilty in respect of all other charges. Malik was sentenced to three years of imprisonment. Zafar and Iqbal to three years of detention in a young offenders’ institution, Butt to 27 months of detention and Raja to two years of detention. Id. at [10], [11].
147. Id. at [1].
148. See id. at [48]; see also UNODC REPORT, supra note 18, at 33. (“On the facts of the case, noting that it raised difficult questions of interpretation about the scope of application of section 57, the Court held that the necessary connection was not present, and therefore the resulting convictions were unsound, and allowed the appeals.”).
against them.” A person has committed a criminal offense if they engage in the “dissemination, public display, posting, or presentation of such calls in writing or other forms of imaging.” This language was interpreted by the German Federal Court of Justice in 2007, which limited the offense of “campaigning” for a terrorist group. The defendant was prosecuted for distributing audio and video messages from Al Qaeda on the Internet. The messages called for jihad and justified terrorist attacks. The court held that the actual recruitment to a terrorist organization was required. It also reduced the possible sentence from ten to five years.

National courts have hemmed in legislation that criminalizes incitement to terrorism with overly broad language. Lurking in the background of the incitement debate is the possibility that domestic prosecutions might have a chilling effect on civil society’s exercise of free speech. Courts have sought to avoid this outcome, demonstrating that it is important to have a constructive discussion about minority rights and perceived acts of terrorism. During a terrorism-prevention meeting attended by the Organization on Security and Cooperation in Europe (OSCE), Russia, and Germany, the group discussed the criminalization of inciting terrorism. The group concluded that domestic courts and the European Court of Human Rights “can be instrumental” in helping “define the conditions” for criminalizing incitement, specifically by relying on the “principles of legality, necessity and proportionality found both in the regional and international human rights instruments.”

C. Lessons from the European Court of Human Rights

The European Court of Human Rights has been a leader in judging the balance between the governmental interest and individual rights in the context of terrorist incitement. The main guarantee for the freedom of

150. Strafgesetzbuch [StGB] [Penal Code], Nov. 13, 1998, BGBL. I at 3214, as amended, §130, para. 1, sentence 1 (Ger.).
153. See UNODC REPORT, supra note 18, at 135. (“The development and enforcement of laws criminalizing the incitement of acts of terrorism while fully protecting human rights (e.g. the right to freedom of expression) presents an ongoing challenge for policymakers, legislators, law enforcement agencies and prosecutors in all countries.”).
154. See id. at 145; HUMAN RIGHTS WATCH, WORLD REPORT 2008: EVENTS OF 2007 388 (2008) (discussing a case in Germany where two academics were arrested for being “intellectual supporters of a militant left-wing faction allegedly responsible for a series of arson attacks”).
155. Van Ginkel, supra note 35, at 11 (describing the debate over the scope of incitement speech covered by the Convention). Again, this impact is likely to be most strongly felt in “already alienated minority communities,” where discussion of issues related to terrorism “needs to be encouraged, rather than stifled.” Id. at 26.
156. ICJ Report, supra note 103, at 5.
157. Id. at 11.
expression is found in Article 10 of the European Convention on Human
Rights (ECHR). The Court has applied a balancing test in its considera-
tion of “incitement” cases, weighing the legal certainty, necessity, and pro-
portionality of a state’s response to speech associated with terrorism.
‘Legal certainty’ implies that legal standards are properly crafted to allow
individuals the ability to regulate their own conduct.159 ‘Necessary’ does
not mean indispensable; instead, it implies a “pressing social need” that
must accord with the requirements of a democratic society.160 Proportion-
ality means there must be a reasonable relationship between the means
employed and the aims achieved.161 The ECtHR’s inquiries are fact-spe-
cific and consider the totality of the circumstances.162 The OSCE claims
these inquiries have “never been simple.”163

Despite the difficulty of the ECtHR’s task, the European Union can
draw valuable insights from past cases.164 The Court has allowed states to
restrict freedom of expression on a national security basis, as well as other
grounds described in Article 10 (2). But Article 10 also provides the metric
by which the Court has found state violations of freedom of expression
where the definition of an offense was too vague.165 The following cases
have produced a series of factors that the Court has used to balance indi-
vidual rights with the governmental interest.

The ECtHR has expressed in numerous cases that the link between
incitement and the potentiality of violence was an important factor in their
balancing test. In Leroy v. France, the ECtHR did not find a violation of
Article 10 in the case of a journalist who had been convicted of publishing
a controversial cartoon in a Basque newspaper.166 On Sep. 13, 2001, the
newspaper published a cartoon depicting an attack on the World Trade
Centre with a parody of a famous advertising slogan: “We have all dreamt
of it . . . Hamas did it” (cf. “Sony did it”).167 The Court reasoned that the
drawing went further than merely criticizing the United States; it “sup-

159. OSCE Report, supra note 51, at 7.
(1976).
161. Factors to consider when assessing whether or not an action is disproportionate
are: “(1) Have relevant and sufficient reasons been advanced in support of it? (2) Was there a
less restrictive measure? (3) Has there been some measure of procedural fairness in the deci-
ision making process? (4) Do safeguards against abuse exist? (5) Does the restriction in ques-
tion destroy the ‘very essence’ of the right in question?” OSCE Report, supra note 51, at 7.
(2000). (“The Court must look at the impugned interference in the light of the case as a
whole. In particular, it must determine whether the interference in issue was ‘proportionate
to the legitimate aims pursued’ and whether the reasons adduced by the national authorities
to justify it are ‘relevant and sufficient.’”).
164. Id.
167. Id. ¶ 6; UNODC REPORT, supra note 18, at 42.
ported and glorified its violent destruction.”168 The Court stated that the caption indicated the cartoonists’ moral support for the perpetrators of the September 11 attacks.169 The Court took numerous factors into account, including the cartoonist’s choice of language, the sensitive date of the publication, and the politically sensitive nature of the region in which it was distributed.170 The UN Office on Drugs and Crime stated that “[t]he principles developed in this landmark case will apply equally to cases in which the alleged incitement to terrorism has occurred via the Internet.”171

In Hogefeld v. Germany, the ECtHR accepted that a measure limiting freedom of expression was justifiable in a case of indirect incitement, where the applicant’s previous statements could be understood by supporters as an appeal to continue the violent activities of the Red Army Faction (RAF) terrorist group, in light of her background as an RAF representative.172 In Sürek v. Turkey (No. 1), the owner of a Turkish newspaper was prosecuted for publishing two readers’ letters strongly criticizing the violence of Turkish military operations in the southeast corner of the country.173 The Court did not find that the state’s actions violated Article 10, holding, “the impugned letters amounted to an appeal to bloody revenge by stirring up base emotions and hardening already embedded prejudices which had manifested themselves in deadly violence.”174 The decision was hotly disputed, with seven of eighteen judges partly dissenting.175 The dissenting judges argued that the real and imminent risk of those letters inciting violence or hatred had not been proved. Some of the dissenters said the U.S. Supreme Court’s Brandenburg test should be used.176

Over time, the ECtHR has considered a number of factors to determine when free speech should be protected by the European Charter on Human Rights. Three cases from Turkey illustrate the application of these factors. In Ceylan v. Turkey, the Court considered an article written by a trade-union leader, which described the Turkish military operations in the South East as “State terrorism,” “genocide,” and “bloody massacres.”177 The letter called for a reaction from the democratic forces of the nation.178 The Court, pointing out the importance of political speech, found “that the article in question, despite its virulence, does not encourage the use of

168. UNODC REPORT, supra note 18, at 42.
170. UNODC REPORT, supra note 18, at 42.
171. Id.
174. Id. at 356.
175. Id. at 392–99.
176. Id. at 394.
178. Id. at 39.
violence or armed resistance or insurrection” and accordingly registered a violation of Article 10.179

In Karataş v. Turkey, the Court held that poetic expression (directed to a small audience) had a “limited impact” on national security, notwithstanding some lines calling for violence with quite aggressive tones.180 Considering the poems, the Court affirmed: “the fact that they [the poems] were artistic in nature and of limited impact made them less a call to an uprising than an expression of deep distress in the face of a difficult political situation.”181 Similarly, in Incal v. Turkey, the court held that criminal conviction for the dissemination of a pamphlet was in violation of Article 10 ECHR, considering the (1) severity of the sanction, (2) the fact that the applicant sought an authorization from the prefecture but was arrested the next day before he could circulate the leaflet, (3) the fact that the applicant is a member of one of the opposition’s political parties, and (4) because the document was not considered by the ECtHR as clearly inciting violence or hatred among Turkish citizens.182

These ECtHR cases illustrate that the Court is consistently trying to determine the degree to which certain statement are actually likely to incite violence. Other facts considered by the court are: the format of the expression and the audience (including its artistic merits), the general political situation in a country, the severity of the governmental sanction, “the status of the person (e.g. a member of a political party)” and the intent of the person.183 The Court has never set a rigid probability test, but it does weigh the credible nature of the danger, the author and the addressee of the message, and the context in which the offence is committed.

IV. THE NEED FOR AN INTEGRATED APPROACH IN THE EU

The decisions of the ECtHR and national courts should inform European Union policy on the “incitement” of terrorism. Even though the Lisbon Treaty abolished the passage of new Framework Decisions, they are still in effect. The analysis of European courts can help the EU to explore new legislative options, such as directives, to address the most ambiguous elements of the Framework Decision. These elements include the subjective intent to incite violence, the likelihood of future acts, and speech that is actually public. The EU can improve enforcement by dedicating resources to address the root causes of radicalization and violence. Part A offers a non-exhaustive list of legislative prescriptions to improve the Framework Decision. Part B argues that a change in the legal framework must be supported by stronger enforcement efforts, specifically engagement with at-risk communities throughout the Europe.

179. Id. at 40.
181. Id.
183. OSCE Report, supra note 51, at 21.
A. Legislative Prescriptions

A handful of scholars and international organizations have offered their prescriptions for defining the incitement of terrorism. There is a split in the debate between advocates who believe that legislative change is necessary and those who do not. Advocates who do not think legislative change is necessary believe that any changes the EU might undertake would be more likely to further restrict freedom of expression than clarify existing standards. Considering the trend of courts limiting overly broad legislation, I argue that a clarification of the legal standard on the incitement of terrorism is necessary. To uphold the principle of legal certainty—that is, that people can actually understand the legal limits of their conduct—the EU should consider a new set of directives on cyberterrorism with consideration paid to the factors used by the ECtHR and national courts. The EU should also consider the unique challenges posed by speech on the Internet, including distinctions between public and private communication.

Any legislative language dealing with the complicated areas of terrorism and free speech should be carefully targeted and proportionate. The European Union should strongly consider the following factors in clarifying the 2002 Framework Decision on Terrorism. First, the indirect incitement of terrorism should be criminalized when it evidences a subjective intent to incite violence. Second, there should be a direct causal connection between incitement and the likelihood of violence. Third, the criminalized speech must offer specific support for future terrorist acts. And fourth, the speech must be public in nature. Each one of these elements will be examined in turn. The analysis presented here is by no means an exhaustive list, but should serve to identify some of the most pressing concerns.

The first element that the EU should clarify is the intent to incite violence. Advocates have explained that mens rea should be carefully addressed in the description of incitement as a criminal offense. The intent to incite terrorism requires some purposeful knowledge of how the speech will impact a wider community and actually motivate violence. The distinction between an intent to incite and recklessness as to incitement is nota-


185. The Briefing Paper and the ICJ do not believe that further legislation is necessary. Van Ginkel argues that legislation must clearly define the following elements: (1) target conduct; (2) content of speech; (3) public/private distinction; (4) imminence/likelihood of causation; (5) intent to incite. Van Ginkel, supra note 35, at 2.

186. See Briefing Paper, supra note 124, at 8 (“[T]o introduce such legislation would have a disproportionate impact on the enjoyment of the right to freedom of expression in the European Union.”).

bly absent from the language of the Framework Decision. Similarly absent from the Framework Decision is the mention of violence. The Framework Decision merely refers to the danger of a terrorist act being committed. The European Union should take its cue from the ECtHR, which has held that inciting violence is a key factor in considering the criminality of terroristic incitement. The subjective intent element to incite violence is important to prevent the governmental imposition of objective penal responsibility, which is prohibited in international law.

The second element requiring EU clarification is the causal link between incitement and the likelihood of violence. There should be some direct link between an individual’s speech and the likelihood of a violent terrorist act being committed. The Johannesburg Principles on National Security, Freedom of Expression, and Access to Information (Johannesburg Principles) advocate that “expression may be punished as a threat to national security” if the government can demonstrate, among other elements that “there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.” The causal relationship between speech and violence helps to ensure that there is a concrete threat associated with a potential act of violence. It is problematic to characterize incitement as an inchoate offense, because speech is then completely divorced from the execution of terrorist act.

The third element requiring clarification is that the speech support a violent terrorist act that will occur in the future. This element is deeply intertwined with intent and causality. All acts must have requisite intent and a causal relationship to a potential act of violence. The ECtHR has held that criminalizing certain acts that denigrate victims but do not have any link to a future terrorist act risk non-compliance with Article 10 of the ECHR. In considering the past and future distinction, the ECtHR has debated the applicability of the Brandenburg standard. It is particularly useful in this context, since it provides that the First Amendment does not “permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or produc-

188. *ICJ Report,* supra note 103, at 10 (“A number of elements are not explicit in the Framework Decision and may vary in incitement offences in national law. These include: the level of intent that is required to incite to an act of terrorism, and whether the requirement is one of intent to incite, or recklessness as to incitement.”).


190. See Sürek v. Turkey (No. 1), 1999-IV Eur. Ct. H.R. 353, 356 (holding that prosecution of a newspaper for the publication of letters detailing torture by state agents was justified).

191. The Nuremberg Tribunal recognized members of three Nazi organizations to be guilty of particular offences, but rejected objective penal individual responsibility for membership of the group, unless the individual had participated voluntarily and acknowledged the criminal goals of the group. See U.N. Security General, *Report of the Secretary General pursuant to Paragraph 2 of Security Council Resolution 808* (1993), U.N. Doc S/2/25704 (May 3, 1993).

The focus of the *Brandenburg* standard is on future acts, precisely where it should be. The European Court of Human Rights—in dissent—has even considered adopting certain elements of the *Brandenburg* test. This logic has been echoed by the Johannesburg Principles discussed above, since causality implies some future action.

In the context of Internet expression, “public speech” must be carefully addressed. For example, is it a crime for people to incite terrorism on a closed forum or chatroom? To qualify as incitement, speech should be directed at a general audience in a place that is public. Instant messaging, Facebook posting, or members-only websites should not qualify. Public Twitter and Instagram accounts should qualify, since it is a truly public forum capable of reaching a wide public audience. Non-public incitement can be covered by general criminal law, especially if concrete planning of a terrorist event is involved. Nonetheless, it can be difficult to define exactly every public/private distinction as it occurs on the Internet. The EU should conduct context-specific inquiries that consider the number of people involved in an incitement case, as well as the accessibility of their dialogue about terrorist actions, past or present.

States must ensure that their actions targeting the incitement of terrorism fully conform with their international obligations under human rights law, refugee law and humanitarian law. Governments should formulate offenses in terms that are as close as possible to international instruments. Legislation should not be drafted in an unduly restrictive manner. This will allow legal authorities and judges to assess the substance of the unlawful conduct that is the subject of requests “rather than adopting an unduly narrow approach.”

### B. Enforcement Prescriptions

The European Union can play an active role in facilitating inter-governmental cooperation through its Third Pillar. The EU has created both strategic and operational initiatives. Beginning in 2004, the European Council agreed on a five-year plan called the Hague Programme to develop the areas of freedom, security, and justice. One of the primary areas for analysis and action was the fight against terrorism. In 2005 the EU Presidency and the Counter-Terrorism Coordinator presented the European Union Council with a comprehensive strategy containing four component parts: (1) to prevent, (2) to protect, (3) to pursue, and (4) to respond. Under the first component part, the EU’s main goal is “[t]o prevent people [from] turning to terrorism by tackling the factors or root

196. *Id.* at 14.
197. UNODC *REPORT*, *supra* note 18, at 135.
198. *Id.* at 95.
causes which can lead to radicalisation and recruitment.” Specifically, the EU has resolved to “[1] disrupt the activities of the networks and individuals that draw people into terrorism; [(2)] ensure that voices of mainstream opinion prevail over those of extremism; [and (3)] promote security, justice, democracy and opportunity for all even more forcefully.”

At the operational level, the European Police Office (EUROPOL) conducts Internet policing in a variety of capacities. The European Parliament has several standing committees that address cyberterrorism in some capacity. The Committee on Industry, Research and Technology (ITRE) concerns the information society and information technology, including the establishment and development of trans-European networks in the telecommunication infrastructure sector. The Committee on Civil Liberties, Justice and Home Affairs (LIBE) has oversight of legislation in the areas of transparency and of the protection of natural persons with regard to the processing of personal data. The Committee on Culture and Education (CULT) addresses audiovisual policy and the cultural and educational aspects of the information society.

Law enforcement in European countries can learn a great deal information about terrorist activities from websites and chat rooms. Authorities are able to compile electronic data for counter-terrorism purposes. Increasingly sophisticated tools, such as CleanIT, can detect terrorist activity. CleanIT is an information technology initiative used for flagging terrorist content. CleanIT administrators contact Internet providers to encourage them to block the flagged material. The European Commission originally funded CleanIT in 2010 with a grant of €400,000. The aim is to create “a non-legislative ‘framework’ that consists of general principles and best practices. . . to counter the illegal use of Internet,” according to the group.

For CleanIT to be truly effective, it must be part of a larger law enforcement effort to engage at-risk youth on websites and chat services. Shutting down extremist websites may not be enough. Removal or prohibition of websites might have a short-term positive effect, but will only encourage the republication of the web site under a different name.

201. Id.
203. Id.
204. Van Ginkel, supra note 35, at 8 (“In a policy brief of the Center on Global Counter-Terrorism Cooperation, Liat Shetret argues that it is sometimes better not to remove or ban websites on which extreme ideas are communicated.”).
205. See Internet Jihad, supra note 3.
removal or the prohibition can fail to counter the message itself.\textsuperscript{206} The Economist notes that, “attempts to close down extremist sites are little more than short-lived harassment. What is needed is a systematic campaign of counter-propaganda, not least in support of friendly Muslim governments and moderate Muslims, to try to reclaim the ground ceded to the jihadists.”\textsuperscript{207} By facilitating a constructive debate, law enforcement may discourage potential terrorists.\textsuperscript{208}

Yet replacing one form of propaganda with another must be coupled with other initiatives; it cannot be used as a stand-alone measure. The deep roots of discontent found in Europe’s disenfranchised populations require a multifaceted approach. Although CleanIT is a start, the European Union will need to devote more than €400,000 to effectively counter terroristic incitement on the Internet.\textsuperscript{209} The EU should make a concerted effort to hire translators and law enforcement officials that not only speak Arabic, but also understand the historical and contemporary dimensions of Islamic fundamentalism. In order to promote alternatives to radicalization, experts must be able to advance a compelling counter-narrative.\textsuperscript{210} By engaging at-risk populations on the Internet, these experts can “weaken cult personalities, challenge extremist doctrine, dispel the terrorist lifestyle, and offer a street-smart, locally developed and communicated answer.”\textsuperscript{211}

If the European Union is serious about its counter-terrorism goals—such as “community policing, and effective monitoring of the Internet”\textsuperscript{212}—it must prioritize an integrated strategy.

Academics and policymakers have advocated for a non-military approach to combating terrorism called the human security paradigm.\textsuperscript{213} This approach seeks to address the deep inequities and disenfranchisement that drives terrorist activity. Human security is “defined as freedom from violent conflict and physical want.”\textsuperscript{214} This can take many forms including proper access to food and water, education, public health programs, housing, and protection from violence, military or otherwise. Canada and Norway have led the charge by establishing a “human security

\begin{itemize}
\item \textsuperscript{206} Id.
\item \textsuperscript{207} Id.
\item \textsuperscript{208} UNODC \textit{Report, supra} note 18, at 12.
\item \textsuperscript{209} Farivar, \textit{supra} note 202.
\item \textsuperscript{210} \textit{Internet Jihad, supra} note 3.
\item \textsuperscript{211} Van Ginkel, \textit{supra} note 35, at 8.
\item \textsuperscript{212} Presidency, \textit{Report of the Presidency on the EU Strategy for Combating Radicalisation and Recruitment to Terrorism}, at 3, COREPER and the Council of the EU, Doc. No. 14781/1/05 REV 1 (Nov. 24, 2005).
\item \textsuperscript{214} America’s Climate Choices: Panel on Advancing the Scl. of Climate Change, Nat’l Research Council, Advancing the Science of Climate Change 300 (2010).
\end{itemize}
network” of states and NGOs that “endorse the concept” of human security.215 A number of EU states have joined the network, including Austria, Greece, Ireland, the Netherlands, and Switzerland. It is vital to involve a diverse group of actors such as governments, non-profits, citizens, and international organizations.

The EU can also bring religious and political groups into the fold in order to mitigate the radicalizing effects of violent rhetoric.216 Intercultural debates and educational initiatives can actively promote respect for human rights and individual liberties.217 To be truly effective in this context, EU law enforcement must build empathy within at-risk communities to demonstrate that violence is not a desired outcome in any context. The European Union is in a unique position to assume a coordinating function that brings together all of the relevant stakeholders: member states, NGOs, and officials from national and regional courts.218

CONCLUSION

Considerable uncertainty surrounds the current European Union and member state definitions on the incitement of terrorism. The Internet compounds these problems by creating open fora for the perpetuation of controversial speech. The EU should seek to clarify the old Framework Decisions by passing new directives to elucidate the principle of legal certainty. By clarifying the legal standard on incitement, the EU can encourage free speech within the boundaries of its Framework Decision. This kind of action will set an example for its member states, many of whom have passed overly broad legislation that has since been narrowed by national courts. These judgments, along with those from the European Court of Human Rights, provide a ready-made example of how to structure the language of a directive. The EU will address many of the Framework Decision’s most ambiguous elements by focusing on the subjective intent to incite violence, the likelihood of future acts, and speech that is actually public. Moreover, the EU can improve enforcement by dedicating resources to law enforcement that can engage with at-risk populations to mitigate against radicalization and violence.

216. Healey, supra note 186, at 175.
217. Id. (“To ensure that the European Union promotes justice, democracy, security, and opportunity for everyone, the European Union targets identified areas of discrimination and inequality within the European Union with intercultural debates; outside of the European Union, the European Union promotes human rights, education, good governance, and economic prosperity with assistance programs and political debates.”).
218. Van Ginkel, supra note 35, at 8.