Impossible to Regulate: Social Media, Terrorists, and the Role for the U.N.

Paulina Wu

Recommended Citation
Available at: http://chicagounbound.uchicago.edu/cjil/vol16/iss1/11
Impossible to Regulate? Social Media, Terrorists, and the Role for the U.N.

Paulina Wu*

Abstract

The posting of journalist beheadings online and the arrests of numerous nationals attempting to join terrorist organizations have shown that terrorists are increasingly using social media to spread ideology and recruit members. The popularity of social media around the world provides a huge potential audience for terrorist content. Unfortunately, because of states’ inability to cooperate, previous attempts to govern and police the Internet have failed. Any regulation of the Internet or social media also raises collective action problems and baseline definition issues. The U.N. is not in the position to pass a binding treaty or convention because use of social media by terrorists is harder to identify than other regulated areas of internet use. Disagreement among U.N. members on whether internet governance should be implemented by the international community also makes a treaty unlikely. Despite these problems, this Comment suggests that the U.N. still has an important role to play in the regulation of terrorist content in social media. By taking a role as a coordinator between states, the U.N. can create an effective monitoring regime that reduces the costs of internet governance and promotes coordination between states.

Table of Contents

I. Introduction ............................................................................................................. 283
II. Terrorism and Social Media: A Recent Phenomenon ....................................... 285
   A. Social Media and Its Advantages ..................................................................... 286
   B. Terrorists’ Use of Social Media ...................................................................... 288
III. The U.N. and Internet Governance .................................................................. 289
   A. Social Media and the Right to Freedom of Expression ................................. 290

* J.D. Candidate, 2016, The University of Chicago Law School. The author would like to thank the Chicago Journal of International Law staff and Professor Adam Chilton for their guidance during the research and writing process. She would also like to thank her parents, Judy and Kevin Wu.
B. The U.N.'s Stance on Terrorists' Use of the Internet .................. 291

IV. The Challenges of Regulating the Internet and Social Media .......... 292
   A. Collective Action Problems: The Internet as a Commons ............ 292
   B. The Definition of Terrorism: A Baseline Issue ..................... 293
   C. The Failed Convention on Internet Governance: The World Conference on International Telecommunications ................................. 294
   D. The Implausibility of a Limited Treaty: Cyberterrorism and Social Media, an Imperfect Analogy ................................................. 297
      2. Fundamental differences between cyberterrorism and social media.. 298

V. The U.N.'s Role in Social Media Governance: An Ideal Facilitator ...... 299
   A. The Insufficiency of Private Regulation .................................. 300
   B. Solving the Collective Action Problem: Principles of Effective Monitoring and Their Application to the U.N. ................................. 301
   C. A Preliminary First Step: Identifying the Best Definition of Terrorism .............................................................. 304
      1. The U.S. ............................................................................. 304
      2. The U.K. ............................................................................. 305
      3. France .............................................................................. 306
      4. Russia .............................................................................. 306
      5. China .............................................................................. 307
      6. Who has it best? France. ...................................................... 308
   D. The U.N. Must Also Coordinate with Private Actors .................. 309

VI. Conclusion ............................................................................. 310
I. INTRODUCTION

Terrorists have increasingly used social media as a recruiting and publicity tool.\(^1\) Social media is a recent innovation that allows individuals to "share information, ideas, personal messages, and other content ([such] as videos)" around the world.\(^2\) It has several features advantageous to dissemination of content: open access to users, the ability to reproduce and transmit information quickly, and easy-to-use interfaces.\(^3\) But these advantages also make social media a useful tool for terrorists. In the last year, teenagers from the U.S., Europe, Asia, and Australia joined terrorist organizations, recruited by social media platforms.\(^4\) The Islamic State of Iraq and Syria (ISIS) also used social media to post the beheadings of journalists.\(^5\) Due to the growing terrorist presence on social media, regulation to limit and remove harmful content has the potential to save lives.\(^6\)

Since the 1990s, the U.N. has recognized the threat of terrorists using the Internet.\(^7\) However, regulation raises complicated questions of balancing an

---


\(^3\) See generally Weimann, New Terrorism, supra note 1.


individual’s right to freedom of expression with the need to reduce terrorism’s toll on human life. Because social media transcends borders, commentators have questioned whether the U.N. is the proper body to regulate internet and social media abuse. In response, the U.N. has agreed that limiting terrorist social media use is a pressing issue. However, the U.N. is not in a position to pass a convention or treaty covering internet or social media governance.

Two examples reflect the U.N.’s inability to regulate. In 2012, the U.N. hosted the World Conference of International Telecommunications (WCIT) in Dubai to discuss the issue of internet governance. Specifically, the Final Acts recognized that “all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security, and continuity of the existing Internet and its future development and of the future internet.” Despite the U.N.’s efforts, disagreement between members resulted in only 89 out of 144 total countries signing the nonbinding Final Acts. Countries such as the U.S., Canada, France, the U.K., and Germany did not sign the treaty. With so many countries refusing to sign the Final Acts, the conference shows how an international body is unlikely to resolve internet governance. Another example is the Convention on Cybercrime, which regulates cyberterrorism. In contrast to the WCIT, various states signed the Convention on Cybercrime. As a result, there is a plausible argument that the U.N. could pass a limited convention that only covers social media. However, cyberterrorism and social media have fundamental differences in the harms they create and the ability to identify violations. Cyberterrorism is easier to identify because any intrusion into a private or public server is a violation. In contrast, social media violations are at the most general level, only speech, which raises the need to balance whether the individual speech is harmful enough to warrant censorship or removal. These differences make a limited treaty on social media implausible.

This Comment addresses the issues surrounding regulation of terrorism in social media. Section II discusses the history of social media, its advantages, and

---

its use by terrorists. Section III details the U.N.’s attempts to govern the Internet in various ways, mostly through passing resolutions. The section also discusses the right to freedom of speech and its tension with speech regulation. Section IV then raises two of the predominant issues concerning regulation of internet social media: collective action problems and a baseline definition of terrorism. The inability of states to cooperate and agree on a definition for terrorism contributes to why internet governance has failed in the past. Finally, Section V argues that, despite the U.N.’s inability to enact formal regulations, it should still take a role in regulating terrorist use of social media by acting as a coordinator between states. As the largest and most legitimate international body, the U.N. can use its resources to minimize transaction costs, which would make it easier for states to cooperate. Furthermore, the U.N. could suggest the best methods of combatting terrorist content. This Comment takes a preliminary step in this direction by analyzing which definition of terrorism employed by Security Council nations is best suited for an institutionalized international governance regime. This Comment also notes that private actors cannot be completely removed from the governance process. Instead, there must be coordination between the U.N., member states, and private actors in order to successfully curb terrorists’ use of social media.

II. TERRORISM AND SOCIAL MEDIA: A RECENT PHENOMENON

Terrorism is rapidly increasing in frequency and magnitude around the world.12 In five years, the Terrorist Identities Datamart Environment (TIDE) database grew from 540,000 names to 875,000.13 Since 2000, the number of deaths from terrorism has grown from 3,361 in 2000 to 17,958 in 2013.14 Within that period, there were over 48,000 terrorist incidents that claimed over 107,000 lives.15 Technology and terrorism are closely related because technology helps terrorists reach more potential recruits, elevates the scale of destruction, and

13 Mark Hosenball, Number of Names on U.S. Counter-terrorism Database Jumps, REUTERs (May 2, 2013), http://www.reuters.com/article/2013/05/03/us-usa-security-database-idUSBRE94200720130503 (listing numbers from 2008 and 2013, respectively). The TIDE database is maintained by the National Counterterrorism Center and lists the names and information of people whom U.S. authorities see as known, suspected, or potential terrorists. See id.
15 Id. at 12.
increases the vulnerability of terrorist targets. In the past few years, more terrorist groups have started to use social media to recruit and proselytize, harnessing terrorists' ability to quickly connect individuals from around the world.

A. Social Media and Its Advantages

Social media is a modern innovation that allows users to communicate around the world in real time. Specifically, social media includes "forms of electronic communication (such as Websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos)." For the purposes of this Comment, social media includes any internet platform that allows communication through images, videos, or messages. The images, videos, and messages are not only targeted towards specific individuals, but also open to the public. Typical social media platforms include, but are not limited to, Facebook, Twitter, YouTube, and Instagram.

Initially, social media was limited to online services that allowed users to share files and access news and events. After 2002, social media grew into online communities where users could connect through photos, online chatting, and videos. When Facebook and Twitter launched, social media boomed because suddenly people could quickly post statuses or "tweet" messages as soon as something happened. As of 2014 in the U.S., 71 percent of adult internet users use Facebook; 23 percent use Twitter; and 26 percent use 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. By 2017, it is estimated the global social network audience will rise to 2.55

17 Merriam-Webster, supra note 2.
18 Targeting the public as an audience is essential in a definition for social media because stating otherwise would include private forms of communication, such as e-mail.
20 See id.
21 See id.
In little more than a decade, social media has become a dominant form of communication that continues to grow worldwide.

Social media provides numerous advantages for communication, one of which is its "overwhelming scope and generally open access." Most social media platforms are free and accessible to anyone with an internet connection. A person in the U.S. can post a message viewable almost instantaneously to someone in Africa or Asia. In comparison to traditional online communities where a user had to register in a forum with a particular subject matter, the general audience for social media is vast. A tweet on Twitter can be seen by millions of users from around the world. If an individual has a public Facebook page, one wall post is available for everyone to see.

Because social media is electronic and practically instantaneous, it is "often used for breaking news or sharing information of immediate importance." Social media can bring attention to global issues, keep actors accountable, and facilitate greater scrutiny of the battlefield. For example, social media brought considerable attention to the civil war in Libya in 2011. Local rebels and reporters used social media to disseminate news to the outside world and show the extent of the war and the government’s atrocities. In the case of Syria, citizens have used social media to document government actions. Social media also provided a means to acquire aid, as local villagers often raised awareness of their villages’ plight by posting on various online social media platforms. In the 2009 Iranian presidential elections, protestors turned to social media when the government cracked down on traditional forms of expression. Social media enabled protestors to coordinate peaceful demonstrations or give accounts of

24 Id.
25 Anne Herzberg & Gerald M. Steinberg, THL 2.0: Is There a Role for Social Media in Monitoring and Enforcement?, 45 ISR. L. REV. 493, 496 (2012).
26 Id.
27 See id. (describing how social media played a large part in providing transparency throughout Gaddafi’s capture in Libya).
29 See id.
30 See, for example, Stephen Dinan., Syrians Use Social Media to Tell World: See Atrocities for Yourself, WASH. TIMUS (Sept. 2, 2013), http://www.washingtontimes.com/news/2013/sep/2/syrians-use-social-media-to-tell-world-see-atrocit/?page=all (last visited May 1, 2015) (noting how, weeks after an attack by the government, over 200 videos were posted online showing everything from victims to munitions that were apparently used).
violent clashes between protestors and police. In contrast to traditional news websites where only reporters can post, social media provides a grassroots mechanism for everyone to participate.

Finally, social media is effective because it is easy to use. Social media requires “little effort on the part of followers or activists to engage with others and share information.” In the case of reporting human rights violations, social media minimizes the costs associated with documenting them: all it takes to post is an internet connection and perhaps a camera. By providing a low-cost and easy-to-use communication mechanism, social media enables users around the world to connect and spread information.

B. Terrorists’ Use of Social Media

The most recent example of a terrorist group spreading its message on social media is the release by ISIS of videos showing beheadings of foreign journalists. Today, “about 90 [percent] of organized terrorism on the Internet is being carried out through social media.” Al-Qaeda and other terrorist organizations have “moved their online presence to YouTube, Twitter, Facebook, Instagram, and other social media outlets.” Because at least one in four people in the world use social media, terrorists’ potential audiences are vast.

Terrorists use social media for many of the same reasons that anyone else does. It is “user-friendly, reliable, and free.” Consequently, terrorists use social media platforms because “these channels are by far the most popular with their intended audience, which allows terrorist organizations to be part of the mainstream.” When a terrorist account is shut down, the cost of establishing a

33 See id.
34 Herzberg & Steinberg, supra note 25, at 496.
35 See Isis Releases Video, supra note 5.
37 Weimann, supra note 1, at 1. For a detailed study on how terrorists use the Internet, see GABRIEL WEIMANN, TERROR ON THE INTERNET: THE NEW ARENA, THE NEW CHALLENGES (2006).
38 See Worldwide Social Network Users, supra note 23.
39 Weimann, supra note 1, at 3.
40 Id.
new one is minimal. Furthermore, "social networking allows terrorists to reach out to their target audiences and virtually ‘knock on their doors’—in contrast to older models of websites in which terrorists had to wait for visitors to come to them." The U.S. State Department estimates there are about 12,000 foreigners who have traveled to Syria from at least fifty different countries to fight with insurgent groups, including ISIS. Terrorists use Facebook as a "gateway to extremist sites and other online radical content"; it acts as a "media outlet for terrorist propaganda and extremist ideological messaging" and provides a mechanism to "share operational and tactical information." Twitter's real-time functionality also allows terrorists to exchange urgent communications. The U.S. Army has reported concerns that Twitter could become an effective coordination tool for terrorists trying to launch militant attacks. YouTube is used as a forum to post propaganda videos and recruit new individuals. Finally, terrorists have used Instagram and Flickr to glorify Osama Bin Laden, for example, or document the execution of hostages. In each of these cases, social media's advantages are abused to help terrorists advance their illegal aims.

III. THE U.N. AND INTERNET GOVERNANCE

Any attempt to regulate social media implicates the right to freedom of expression. Regulations must balance both the individual right to free speech and the public interest in restricting terrorist activity. Because terrorism falls into one of the exceptions to the general right to freedom of speech, the U.N. has recognized that terrorists' social media use is an issue that requires addressing.

---


42 Weimann, supra note 1, at 3.


45 See Weimann, supra note 1, at 8–9 (emphasizing how Syrian jihadists used Twitter to communicate during the August 2013 U.S. airstrikes).


47 An example is the case of Anwar al-Awlaki, a radical Islamic terrorist who posted 1,910 videos, one of which had been viewed 164,420 times. See Weimann, supra note 1, at 11.

48 Weimann, supra note 1, at 13.

49 See UNODC, supra note 9, at 3.
A. Social Media and the Right to Freedom of Expression

As a preliminary matter, Article 9 of the Universal Declaration of Human Rights (UDHR) recognizes the right to freedom of expression. Specifically, "everyone has the right to freedom of opinion; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." The U.N. recognizes that all individuals should express their thoughts and ideas in an open and unrestricted environment. As a result, when anyone posts something on social media, there is an expectation that this is protected speech. When speech is protected, there is a high standard the government must meet in order to justify censorship. Especially in countries like the U.S., where freedom of speech is domestically protected, screening and removal of offensive social media raises complicated issues over what should and should not be censored. For example, even speech that expressly encourages violence is protected under the U.S. Constitution unless it is likely that violence will imminently result. A further complication of applying established free speech law to terrorist recruitment is the concept of "imminent harm." If an individual is recruited into a terrorist organization, is there an imminent harm that will result? This would seem difficult to prove, because the foreseeability and certainty of harm could be too remote to satisfy the imminence test.

While most of its member nations accord broad protection for free expression, the U.N. recognizes that the right is not absolute. In Article 29(2) of the UDHR, the exercise of freedom of expression is subject "to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order, and the general welfare in a democratic society." As a result, speech that would call for the end of freedom of religion, one of the other rights emphasized in the UDHR, would not be permitted. This could be interpreted to apply to terrorist religious propaganda, but other than restricting speech that contradicts UDHR rights, Article 29 is not clear on when and how speech may be censored. The International Covenant on Civil and Political Rights (ICCPR) has a stricter standard, under which state parties must prohibit by law "any advocacy of national, racial, or religious hatred that
constitutes incitement to discrimination, hostility, or violence."\textsuperscript{54} By requiring states to take domestic action, the ICCPR has a stronger emphasis on curbing harmful speech. Whereas the UDHR is not a binding treaty but a "common standard of achievement for all peoples and all nations,"\textsuperscript{55} the ICCPR is binding and has 74 signatories and 168 parties.\textsuperscript{56} But since the ICCPR delegates most of the rulemaking to its signatories, the general vagueness present in both documents reflects the discretion given to states to implement and protect freedom of speech.

B. The U.N.'s Stance on Terrorists' Use of the Internet

The U.N. has recognized the dangers of terrorists using the Internet. In the 1990s, the U.N. called upon its member states to "note the risk of terrorists using electronic or wire communications systems and networks to carry out criminal acts and ... to find means ... to prevent such criminality and to promote cooperation where appropriate."\textsuperscript{57} The Security Council then asked member states to increase international cooperation by exchanging information regarding "use of communications technology by terrorist groups."\textsuperscript{58} In practice, this has been harder to achieve than envisioned.\textsuperscript{59} Nevertheless, in 2005 the U.N. recognized the specific issue of terrorists exploiting the Internet:

> Particularly in the age of popular social networking media, such as Facebook, Twitter, YouTube, Flickr and blogging platforms, individuals ... publish, voluntarily or inadvertently, an unprecedented amount of sensitive information on the Internet .... [S]ome of this information may be misappropriated and used for the benefit of criminal activity.\textsuperscript{60}

Although social media regulation raises difficult questions of individual rights and state sovereignty, the U.N. has recognized that terrorist abuse of

\textsuperscript{55} UDHR, supra note 50, pmbl.
\textsuperscript{57} G.A. Res. 51/210, supra note 7.
\textsuperscript{59} The U.S. and E.U. have generally agreed to share telecommunications to monitor terrorist activity, but in the negotiation of several U.S.-E.U. information-sharing agreements, some E.U. officials have expressed concern about whether the U.S. can guarantee a sufficient level of protection for European citizens' personal data. In comparison to the U.S., the E.U. considers the privacy of personal data a basic right and prohibits the transfer of such data to countries where legal protections are deemed inadequate. See Kristin Archick, U.S.-E.U. Cooperation Against Terrorism, CRS (Dec. 1, 2014).
\textsuperscript{60} UNODC, supra note 9, at 11.
social media requires attention. Unfortunately, there are fundamental issues with governing social media that make the U.N. unlikely to pass a successful governance treaty.

IV. THE CHALLENGES OF REGULATING THE INTERNET AND SOCIAL MEDIA

Despite its status as the foremost international legal body, the U.N. cannot pass a convention that regulates the Internet, or even one that only regulates social media. Besides free expression concerns, regulation of the Internet raises collective action and baseline definition problems. The inability of the U.N. to pass an efficacious convention was exemplified at the WCIT, where countries were unable to agree on an international regulatory regime. Furthermore, although a limited international convention worked in the case of cyberterrorism, there are fundamental differences between social media and cyberterrorism that make regulation of social media unlikely.

A. Collective Action Problems: The Internet as a Commons

One obstacle facing a treaty that regulates the Internet is the fact that the Internet is a global commons. On the international level, commons are areas that “do not fall within the jurisdiction of any one country”; these areas “are termed international commons or global commons.” Because they do not fall into any one jurisdiction, commons are difficult to regulate. Commons are governed through a “mixture of regulations at multiple levels, including multilateral treaty regimes, regional accords, and national regulations.” In general, the global commons consists of “international waters and airspace, space, and cyberspace,” which includes the Internet. The fact that private actors own parts of the Internet is a further wrinkle. Indeed, some argue that this makes the Internet a “pseudocommons.” Regardless, even proponents of the “pseudocommons” view concede that regulating the Internet raises collective action problems.

Collective action problems arise in regards to resources held in common, making it costly and difficult for diffuse actors to cooperate. Specifically, collective action problems occur when multiple individuals are required to

---

64 See Shackelford, supra note 62, at 1292.
65 See id.
contribute to achieving a joint outcome, but it is difficult to exclude free-riders who do not contribute but still enjoy the benefits. Because each actor wants to incur the least cost, the result is for everyone to try to free-ride; eventually, no one contributes even though it would be in their collective best interest to do so. Every country would benefit from less harmful content posted by terrorists. But because the Internet is a commons, no one country would want to contribute to the cost of regulating. Instead, each country is incentivized to free-ride.

B. The Definition of Terrorism: A Baseline Issue

Another obstacle to regulating the Internet is difficulty in defining the types of content subject to censorship. Although the U.N. recognizes that the fundamental right of freedom of expression is limited when used to promote violence or discrimination, much internet content is not clearly classified as one or the other. Historically, attempts to define terrorism in international law have failed, despite the fact that the U.N. has called for a comprehensive international definition. The issue stems from determining what exactly is "illegal" versus simply "objectionable" content. In many cases, there is tension between defining actors as individuals acting for the sake of self-determination and those acting as terrorists. Self-determination is the proposition that "every people should freely determine its own political status and freely pursue its economic, social, and cultural development." It is recognized in the ICCPR, which emphasizes that "[a]ll peoples have the right of self-determination." However, states differ on whether there are any circumstances where self-determination justifies use of violence. In an unresolved U.N. debate between

---

68 See generally Ben Saul, Attempts to Define Terrorism in International Law, 52 NETHERLANDS INT'L. L. REV. 57 (2005).
69 See, for example, As Sixth Committee Commences Session, Delegates Once Again Call for Clear Definition of Terrorism, Consensus on Draft Comprehensive Convention, UNITED NATIONS, GA/L/3453 (Oct. 7, 2013).
70 See generally Ben Saul, Defending Terrorism: Justifications and Excuses for Terrorism in International Criminal Law, 25 AUSTL. Y.B. OF INT'L L. 177 (2006) (discussing the issues with defining terrorism and whether there should be any justifications for using terrorism).
72 ICCPR, supra note 54, art. 1.1.
Pakistan and Morocco, Pakistan argued that self-determination constitutes the most fundamental human right, while Morocco argued that self-determination was obsolete.\(^73\) The debate is also relevant today, with Israel arguing that only countries should determine the peace negotiation process, in contrast to the State of Palestine’s contention that “[t]he right of self-determination belongs to all, and doesn’t come after negotiations.”\(^74\) If self-determination is a fundamental right, then use of violence is justified. But if it is obsolete, then use of violence can be defined as terrorism. Since both sides refuse to concede to the other, the question of self-determination’s primacy is unresolved.

Not only does resolving this dichotomy present a broad challenge for a U.N. convention regulating terrorist use of social media, but the search for a definition of terrorism also raises the issue of who should decide the definition of illegal content. Should it be the U.N. Security Council? Should the definition be subject to a vote in the General Assembly? What kind of consent is required in order to agree on a definition? Should it be a majority or a supermajority? The coordination and negotiation costs alone might explain the absence of a general definition of terrorism in the more than seventy years since the U.N.’s creation. This creates a dilemma: for there to be effective regulation to curb terrorists’ use of social media, there needs to be a definition of terrorism, but it is extremely difficult to arrive at such a definition. If a government cannot easily identify the illegal content, then the costs associated with determining whether the content should be removed are too high to make regulation effective. There is also the possibility of abuse of discretion—when the government is given the right to punish terrorist activity, there is a risk that the government will punish critics instead. Suggesting a baseline definition and analyzing the U.N.’s potential to reduce coordination costs, Section V seeks to help resolve many of these problems. By using its resources to monitor different governments, for example, the U.N. might reduce the risk of abuse of discretion.

C. The Failed Convention on Internet Governance: The World Conference on International Telecommunications

The U.N.’s most recent attempt to regulate the Internet failed. As a threshold matter, social media falls under the realm of “telecommunications” and thus is monitored by the U.N. International Telecommunications Union


\(^74\) Self-Determination Integral to Basic Human Rights, Fundamental Freedoms, Third Committee Told as it Concludes General Discussion, UNITED NATIONS, GA/SHC/4085 (Nov. 5, 2013).
Established in 1865, the ITU is an impartial organization that coordinates the operation of telecommunication networks. In 1989, the ITU developed the International Telecommunications Regulations “to facilitate global interconnection and interoperability of telecommunication facilities and to promote the harmonious development and efficient operation of technical facilities, as well as the efficiency, usefulness and availability to the public of international telecommunication services.” There were few subsequent developments until 2012, when the ITU came together in Dubai to pass a new set of regulations.

The World Conference on International Telecommunications (WCIT), held in Dubai from December 3 to 14, 2012, resulted in the ITU Final Acts, which focused on providing an international network for telecommunications. Specifically, the conference split into two sides—Russia, China, and developing countries such as the Ivory Coast and Kazakhstan signed the Final Acts, while Western countries such as the U.S., Canada, France, the U.K., and Germany did not.

The biggest point of contention was Resolution Plen/3, which recognized that all governments should have an “equal role and responsibility for international internet governance and for ensuring the stability, security and continuity of the existing internet and its future development.” Although it was not explicitly mentioned in the talks, this notion of equal responsibility poses issues about the costs of monitoring terrorist activity. If all governments should have an equal role, does that mean all governments must equally share the costs to maintain an adequate internet platform? What about Western countries, which use social media more than other developing countries? Should countries that have a greater terrorist presence, such as countries in the Middle East, pay more for the costs of regulation? Even without addressing these concerns, the U.S. perceived the resolution as a threat to the open internet:

The United States has consistently maintained that the Internet should not have been mentioned in the proposed treaty, which dealt with technical matters like connecting international telephone calls, because doing so could

78 See ITU, Signatories of the Final Acts, supra note 11.
79 Id.
lead to curbs on free speech and replace the existing, bottom-up form of Internet oversight with a government-led model.\textsuperscript{81}

This view contrasted with that of Russia, who "proposed \ldots that the treaty be revised to give each country control over the Internet within its borders, including domain names, addresses, and other key engineering resources."\textsuperscript{82} The polarization at the conference between the U.S. and Russia, therefore, seems to stem from disagreement over freedom of expression. Historically, the U.S. has taken a strong view of the need to protect free speech, even in cases of speech that promote violence or make false statements of fact.\textsuperscript{83} By contrast, Russia has consistently minimized the importance of freedom of speech, and recent reports from Russia have highlighted an erosion of free speech rights, particularly with respect to speech against the government.\textsuperscript{84}

Because fifty-five countries did not sign the ITU Final Acts, many have criticized the treaty as a failure. Specifically, one scholar has called the WCIT the "beginning of a devolution that ultimately leads to multiple Internets, with varying degrees of freedom of speech and other human rights respected."\textsuperscript{85} Some voices criticize the ITU itself, noting that the "ITU is the chosen vehicle for regimes for whom the free and open Internet is seen as an existential threat" and the "past and future role of the ITU has traditionally been to foster corruption, monopoly, to facilitate surveillance and censorship."\textsuperscript{86} Although it is unclear whether the ITU is a vehicle for authoritarian regimes, the WCIT does show that the fundamental differences between member states likely make any comprehensive treaty impossible.

\begin{itemize}
  \item[^83] See generally Brandenburg, 395 U.S. at 1828–31 (holding that speech can be restricted when it meets three prongs: express advocacy of law violation, the advocacy calls for immediate law violation, and the immediate law violation is likely to occur); New York Times v. Sullivan, 376 U.S. 254 (1964) (holding that false statements about a public official related to his official conduct are protected by the First Amendment).
  \item[^84] For a general discussion about freedom of speech in Russia, see Tatyana Beschastna, \textit{Freedom of Expression in Russia As It Relates to Criticism of the Government}, 27 \textit{Emory Int'l L. Rev.} 1105 (2013).
  \item[^85] Downes, supra note 82.
  \item[^86] Grant Gross, \textit{UN’s ITU Should Be Dismantled, Former White House Official Says}, \textit{Network World} (Nov. 29, 2012), http://www.networkworld.com/article/2161774/data-center/un-s-itu-should-be-dismantled--former-white-house-official-says.html. Arguably, this criticism has merit when the signatories of the ITU Final Acts are considered. Russia and China, countries historically criticized for their authoritative regimes, both signed the Acts, while the U.S. and Western European countries did not.
\end{itemize}
D. The Implausibility of a Limited Treaty: Cyberterrorism and Social Media, an Imperfect Analogy


Cyberterrorism is a "premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub national groups or clandestine agents." Independent hackers or government-sanctioned hackers use cyberterrorism to attack governments or private entities. Throughout the years, numerous cyberterrorism regulations have passed in various international forums. As early as 1990, the Eighth U.N. Congress on the Prevention of Crime and the Treatment of Offenders called for member states "to intensify efforts to combat computer crime by modernizing their national criminal laws and procedures, improving computer security and prevention measures, and promoting the development of a comprehensive international framework of guidelines and standards for preventing, prosecuting, and punishing computer-related crime in the future." By 2002, the Organization for Economic Cooperation and Development (OECD) passed the Guidelines for Security Systems, recognizing the need for greater cybersecurity protections.

In 2004, the Council of Europe enacted the Convention on Cybercrime, the most important international regulation of cyberterrorism to date. The Convention requires parties to enact substantive and procedural legislation to criminalize certain computer crimes. The U.S. was one of many countries that signed the Convention. Signatories agreed to adopt legislative measures that made hacking a criminal offense and to "co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal

matters. In 2011, NATO adopted the New Strategic Concept, which focuses on the threat of cyberterrorism. The New Strategic Concept aims to bring all of NATO's members under a centralized cyber-protection system to defend and recover from cyberattacks.

Even though countries faced similar issues of collective action, the fight against cyberterrorism resulted in international consensus. The Convention required members to cooperate "to the widest extent possible" and extended "not only to crimes established in the treaty, but also to the collection of electronic evidence whenever it relates to a criminal offense." An important provision mandated that parties to the Convention participate in the Cybercrime Convention Committee, which meant that countries not involved in the drafting of the original treaty would still be involved in the development of future international cybercrime standards. Countries were also given the option to refuse certain requests, provided that the request interfered with a country's "sovereignty, security, ordre public or other essential interests." Although the ability to opt out weakens the applicability of the Convention, countries are more likely to sign an international framework when they reserve their own sovereignty. Accordingly, there is a plausible argument that a limited treaty on social media could gain more momentum than a comprehensive treaty on internet governance.

2. Fundamental differences between cyberterrorism and social media.

The similarities between cyberterrorism and terrorists' use of social media give hope to the idea that an international treaty regulating social media is possible. Even though the WCIT failed to govern the Internet, the U.N. could possibly pass a limited treaty on social media. Cyberterrorism and social media are similar because both use the Internet in a harmful way: cyberterrorists steal information, while terrorists recruit and spread terror. Both require monitoring and coordination, and implicate concerns about internet regulation as a whole.

92 Id. art. 23.
94 See id.
98 Convention on Cybercrime, supra note 91, art. 29(5).
However, the fundamental differences between social media and cyberterrorism make a limited treaty on social media unlikely. Cyberterrorism is easier to identify—when anyone hacks or threatens to hack into a computer or network, it falls under widely accepted definitions of cyberterrorism. As a result, cyberterrorism is inherently illegal while general use of social media is not. This is to say that the costs of identifying cyberterrorism are much lower; there is no question when cyberterrorism is committed. On the other hand, there are grey areas when individuals use social media to promote terrorist causes. An individual’s right to post on social media raises freedom of speech issues, perhaps more directly than the typical instance of cyberterrorism does. If an individual posts that he or she thinks the government should be overthrown by Al Qaeda, does that constitute promotion of terrorism? If an individual posts on Twitter that he supports ISIS, is he a terrorist? It is much harder to determine who is a terrorist in the social media context than in the cyberterrorism context.

Furthermore, cyberterrorists tend to be sophisticated hackers with advanced understandings of technology, whereas almost anyone can use social media. The number of potential violators in the social media realm is much higher than in cyberterrorism. Finally, the link between the harm and the activity in cyberterrorism is much more direct. A cyberterrorist violates the privacy of a government or private entity, which creates a clear and imminent harm to the organization or individual. In the context of social media, this is less clear. There is no question that social media can lead to harmful consequences: people joining terrorist organizations, beheading others, and then posting shocking images or videos. But the strength of causation is weaker. Can social media be blamed for someone wanting to join ISIS? It is possible the person would have joined regardless from seeing stories about the organization on the news. The same could be said about beheading videos; instead of posting the video on social media, ISIS could send the video to news agencies. Due to these differences, a limited treaty on social media would not likely encounter the broad support the Convention on Cybercrime enjoyed.

V. THE U.N.’S ROLE IN SOCIAL MEDIA GOVERNANCE: AN IDEAL FACILITATOR

The U.N. may not be able to pass a treaty, but it can coordinate regulatory efforts between states and provide valuable information. With its resources and legitimacy as the leading international body, the U.N. can foster cooperation to hinder terrorists’ social media use. By spreading more widely the costs regulatory

initiatives would impose on private actors, the U.N. can identify the best methods to resolve this issue.

A. The Insufficiency of Private Regulation

Although private actors play an important role in monitoring the Internet, successful monitoring requires the presence of state actors. Some argue that private regulation is sufficient, because companies like Facebook or YouTube can regulate the Internet by using filtering techniques and allowing users to flag objectionable content.\(^\text{100}\) However, there are issues with private regulation that make monitoring of internet content particularly difficult.

First, the practical difficulties of filtering and zoning internet information make it extremely tedious for private actors to monitor the Internet. Facebook and YouTube are large companies, but the resources required to monitor the Internet are enormous.\(^\text{101}\) In these cases, the financial costs associated with monitoring are extremely high, disincentivizing voluntary monitoring of user content.

In addition, there are social costs to monitoring the Internet. An anonymous senior official at a social media company noted that “[o]ne person’s terrorist is another person’s freedom fighter,” thus making regulation of content “not something we’d want to do.”\(^\text{102}\) Although social media companies recognize that terrorist content should be removed, stricter regulation could “ruin” social media platforms by deterring normal users from posting objectionable but non-extremist content.\(^\text{103}\) This type of “chilling effect” prevents speakers from exercising their rights to expression, which, although objectionable, may provide valuable contributions to public discourse and debate.\(^\text{104}\) In these cases, social media companies fear that they will “create a standard for everyone that is in response to [a] small minority, [where] by creating that standard [the companies] then ruin the thing that [they have]…

\(^{100}\) See, for example, Rachel Weintraub-Reiter, Note, *Hate Speech Over the Internet: A Traditional Analysis or a New Cyber Constitution*, 8 B.U. PUB. INT'L. L. J. 145, 168–69 (1998) (noting that private corporations can use filtering techniques in order to remove hate speech).


\(^{102}\) Farrow, supra note 6.


Further, when internet monitoring is completely in the hands of a private market, there may be a gap between private interests and the public interest of promoting free discourse. Specifically, the private actor may prioritize its own interests over those of the public. Another complication is the fact that private actors face a legitimacy issue in regulating internet content. In the face of terrorist content, which raises security and free speech issues, are private actors competent to decide which content should be removed? The combination of financial and social costs makes it unfeasible to depend solely on private actors to regulate terrorist content.

B. Solving the Collective Action Problem: Principles of Effective Monitoring and Their Application to the U.N.

The U.N. is in the best position to coordinate between state governments to monitor the use of social media by terrorists. With its resources and legitimacy as an international body, the U.N. can best solve the collective action problem internet regulation poses. It can also oversee state governments and ensure that there are no abuses of discretion. The U.N. can solve the collective action problem in five ways: creating well-defined boundaries, ensuring proportional equivalence between benefits and costs, making collective choice arrangements, monitoring for violations, and implementing a system of graduated sanctions.

To solve a collective action problem, there must first be well-articulated boundaries that define who is and is not in the group. If a group can determine its own membership—including those who agree to use the resource according to their agreed-upon rules and excluding those who do not agree to these rules—then it makes an important first step toward limiting access and

---

105 Flanagan and Airoudi, supra note 103 (quoting Richard Allen, Facebook’s vice president for public policy in Europe, the Middle East, and Africa).
106 See generally Alexander Tsesis, Prohibiting Incitement on the Internet, 7 V.A. J. L. & TECH. 5 (2002) (detailing the failure of the private market to address regulation of racist content); CASS SUNSTEIN, FREE MARKETS AND SOCIAL JUSTICE 151–55 (1997) (articulating the inability of the market to address discrimination).
107 See Bailey, supra note 101101, at 95–96.
108 The basis of this argument is Elinor Ostrom’s paper on polycentric systems, which outlines principles to solve collective action problems on a small scale (for example, farms, villages, etc.). These principles provide a helpful framework for explaining why the U.N. remains the best actor to govern terrorists’ use of social media. See Elinor Ostrom, Polycentric Systems as One Approach for Solving Collective-Action Problems 12–15 (Ind. Univ. Vincent & Elinor Ostrom Workshop in Pol. Theory & Pol’y Analysis Working Paper No. W08-6, 2008), available at http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf?sequence=1.
developing greater trust and reciprocity. In the case of the U.N., membership is clearly established, and members "confer on the Security Council primary responsibility for the maintenance of international peace and security."

Thus, when the U.N. coordinates between states, clear boundaries demonstrate which states are obligated to listen to its suggestions.

The second important principle for overcoming collective action problems is consistency between distribution of costs and benefits, something the U.N. is well-placed to ensure. The benefits of a coordinated effort to regulate social media would be less terrorist propaganda and recruiting. The costs would be those associated with monitoring and participating in the governance of social media. The U.N. has stressed the importance of limiting terrorists’ internet use, which facially suggests its willingness to ensure a proportional distribution of benefits and costs. By coordinating across borders and offering its resources to monitor violations, the U.N. could help members enjoy the benefits of a safer internet environment.

An effective system would also require collective choice arrangements, where “most of the individuals affected by a resource regime may participate in enacting their rules. This enables regimes to tailor rules to local circumstances and to devise rules considered fair by participants.” For instance, the General Assembly is the “main deliberative, policymaking and representative organ of the U.N.” Because every country has one vote, every member has a voice in deliberating on social media regulations. If one country is abusing its discretion, either by curbing dissent or favoring certain countries’ content over others, the General Assembly can collectively debate the issue. Not only does this take advantage of the wealth of expertise each country can provide, but it also makes regulation more legitimate. Particularly in this area, the U.N. is more effective

109 See id. at 12–13.
112 See UNODC, supra note 9, at 134.
116 An example of this type of risk would be Western countries advocating removal of tweets that threaten Israel but ignoring similar threats against unipolar governments such as China.
than the ITU. By allowing each member to deliberate, the U.N. quells concerns that any regulatory regime is being abused by countries aiming to curb free speech.

Overcoming the collective action problem also requires monitoring. In order to minimize the risk of free-riding, an effective monitoring system must identify violations and violators. In the case of the U.N., a special committee could be created to monitor social media use. U.N. members can also file complaints, which would create an effective system to supplement government and private efforts to regulate harmful content. An independent expert could also be appointed to identify violations and act on individual cases.

Finally, the U.N. is the ideal venue to implement a system of graduated sanctions. Graduated sanctions are helpful because the first punishment notifies the individual or nation of public scrutiny, but the capability to escalate sanctions allows the regime to warn members of the costs of failing to conform. In the case of regulating terrorists’ social media use, punishment would be directed towards countries that abuse their discretion by clamping down on legitimate criticism and expression or failing to screen terrorist content. Sanctions could range from warnings to economic sanctions and, in extreme cases, even to military intervention. The U.N. is particularly equipped at implementing sanctions because of its broad reach—international principles contained in treaties such as the U.N. Charter and in customary law can be applied to non-state actors, as well as to states, to maintain international peace and security and minimize the potential for international conflict. In comparison to other agencies or private actors, the U.N. is in a better position to coordinate an effort between countries to regulate terrorist social media.

118 An example would be the United Nations Human Rights Council, which monitors global human rights violations.
119 Special procedures, “special rapporteurs” (as individuals), or working groups are used to advise on human rights violations. Because regulation of terrorist expression raises free speech concerns, a special rapporteur could be created to specifically address these violations. For a discussion of the role of special procedures, see Office of the High Commissioner of Human Rights, Special Procedures of the Human Rights Council, UNITED NATIONS HUMAN RIGHTS, http://www.ohchr.org/EN/HRBodies/SP/Pages/Introduction.aspx (last visited April 6, 2015).
121 It is important to note that U.N. military intervention is rarely pursued, even in response to well-publicized violations of UDHR rights. Two examples include the Rwandan genocide and the atrocities committed in Serbia. For a discussion of the UN’s reluctance to intervene, see Max Boot, Paving the Road to Hell: The Failure of U.N. Peacekeeping, FOREIGN AFFAIRS (March/April 2000).
C. A Preliminary First Step: Identifying the Best Definition of Terrorism

The failure of the U.N. to pass a convention on point does not preclude the possibility of coordination efforts. Although each State has its own methods to deal with terrorist use of social media, some methods work better than others. Social media use by terrorists is a new phenomenon, and the U.N. can be a useful resource in creating and fostering an effective monitoring system. The first step the U.N. can take is to suggest the definition of terrorism best suited to differentiating between valuable free expression and terrorist recruiting. By providing a suggestion, not a requirement, each State's sovereignty is preserved. Although non-binding recommendations may not be as effective or enforceable as a binding obligation, this approach makes it more likely that states will be open to some form of internet governance.\(^{123}\) As a preliminary attempt at this approach, this Comment looks at the definitions of terrorism used by each member of the Security Council, and analyzes which definition is best suited to a social media regulatory regime.\(^{124}\)

1. The U.S.

Multiple U.S. statutes define terrorism. One definition describes terrorism as “premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents.”\(^{125}\) U.S. law defines international terrorist acts\(^{126}\) with reference to three characteristics:

- [1] violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State;
- [2] [an intention] (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
- [3] [acts] occurring primarily outside the territorial jurisdiction of the United States, or transcend national boundaries.

\(^{123}\) For an overview of the advantages and disadvantages of hard law (binding) versus soft law (non-binding), see generally Gregory C. Shaffer & Mark A. Pollack, *Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance*, 94 MINN. L. REV. 706 (2010). In general, soft-law instruments are easier and less costly to negotiate, impose lower sovereignty costs on states, provide greater flexibility, and respond better to diverse perspectives. In the area of social media regulation, which is relatively new and uncertain and where nations have contrasting views towards the best way to proceed, non-binding regulation is much more likely to succeed than binding law.

\(^{124}\) This Comment focuses on the five Security Council members as a starting point, as their practices are likely good proxies for countries that actively respond to terrorist attacks.

\(^{125}\) 22 U.S.C § 2656f(d)(2) (2005).

\(^{126}\) This is in contrast to domestic terrorism, which is defined in 18 U.S.C. § 2331(5) (2001).
in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum.[127]

Although having an under-inclusive definition of terrorism is a legitimate concern, the U.S.'s definition is fragmented. By defining terrorism differently in multiple statutes, it is unclear which definition is proper in different circumstances. The creation of binding but ambiguous obligations violates the notion that statutes should provide fair notice to citizens.[128] If this definition were adopted to determine what types of social media content are considered "terroristic," it would be too broad to implement effectively. In addition, by defining international terrorism to require three prongs, the definition risks being under-inclusive of terrorist behavior. Having separate prongs and a conjunctive test may address the concern that the definition is too broad, but the number of prongs must be balanced in order to be detailed but cover the conduct at issue.

2. The U.K.

The U.K. defines terrorism as the "use or threat of action . . . designed to influence the government or to intimidate the public, and the use or threat is made for the purposes of advancing a political, religious or ideological cause," and:

(a) involves serious violence against a person,
(b) involves serious damage to property,
(c) endangers a person's life, other than that of the person committing the action,
(d) creates a serious risk to the health or safety of the public or a section of the public, or
(e) is designed seriously to interfere with or seriously to disrupt an electronic system.[129]

The U.K.'s definition is more inclusive than the U.S.'s. Unlike the U.S. definition, which requires satisfaction of all three prongs, the U.K. only requires "use or threat of action" designed to "influence the government or intimidate the public," made for the purposes of "advancing political, religious or ideological cause," which involves or causes the listed harms.[130] The harms are

128 For a discussion of the fair notice doctrine, see City of Chicago v. Morales, 527 U.S. 41, 58 (1999) ("[T]he purpose of the fair notice requirement is to enable the ordinary citizen to conform his or her conduct to the law.").
129 Terrorism Act, 2000, sec. 1(2) (U.K.).
130 Id.
also defined broadly, including violence, threats, risks, and interference.\textsuperscript{131} As a result, the U.K. definition covers more harmful content. Although it is not under-inclusive, its breadth creates a risk of abuse of discretion.

3. France.

France defines terrorism as acts "intentionally committed by an individual entity or by a collective entity in order to seriously disturb law and order by intimidation or by terror."\textsuperscript{132} The French Criminal Code also lists specific terrorist acts, such as "[a]ttempted murder, assault, kidnapping, hostage-taking on . . . all means of transport, theft, extortion, destructions . . . the production, sale, import and export of explosives, [etc.]."\textsuperscript{133}

French law defines terrorism broadly, then lists specific acts that can be prosecuted. The specific acts prevent the definition from becoming over-inclusive. In comparison to the U.S. and U.K. definitions, the French definition seems to be less susceptible to abuse of discretion because it does not have language such as "threat" or "risk." Although there are many instances of terrorists threatening to use violence, including "threat" or "risk" in a definition raises freedom-of-speech concerns as applied to social media. An individual could voice a threat but not take any substantial steps toward acting on the threat. Having a list of specific acts limits the French government from prosecuting those that are voicing objectionable, albeit non-terroristic, opinions.

4. Russia.

Russia defines terrorism as "the ideology of violence and the practice of influencing the adoption of a decision by public authorities, local self-government bodies, or international organizations connected with frightening the population and (or) other forms of unlawful violent actions."\textsuperscript{134}

Without any other elaboration of the term "terrorism," Russia has the broadest definition of all the Security Council members. As an authoritarian government, Russia mainly depends on the Roskomnadzor, a federal agency

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{131} Id.
\item \textsuperscript{133} Id.
\item \textsuperscript{134} Federal Law of the Russian Federation No. 35-FZ of March 6, 2006 on Counteraction against Terrorism art. 3 (June 2006) (version published by the Council of Europe).
\end{itemize}
\end{footnotesize}
established to monitor the Internet and media activities. Consequently, Russia’s definition is likely too broad for other countries to adopt. The risk of abuse of discretion is much higher with Russia’s definition than with the French or U.K. definitions. There are numerous voices of concern over Russia’s definition already, making it implausible for the General Assembly ever to approve the definition, let alone to suggest it to any other countries without widespread objection.

5. China.

China does not have a statutory definition of terrorism. The only definition appears in a draft bill, under which terrorist acts were “defined as those acts which are intended to induce public fear or to coerce state organs or international organisations by means of violence, sabotage, threats or other tactics.” Since 2011, there has been no subsequent legislation to pass the bill. However, China did pass a resolution elaborating on guidelines to define terrorism. Terrorist activities are those that severely endanger society that have the goal of creating terror in society, endangering public security, or threatening state organs and international organizations and which, by the use of violence, sabotage, intimidation, and other methods, cause or are intended to cause human casualties, great loss to property, damage to public infrastructure, and chaos in the social order, as well as activities that incite, finance, or assist the implementation of the above activities through any other means.

Although China does not have a statutory definition, its guidelines elaborate details that make China’s definition less susceptible to abuse than Russia’s for the purposes of regulating social media. China’s definition is directed towards acts that “endanger society,” which could be construed very broadly. A narrower definition of terrorism is more likely to find support because it excludes more issues of contention, making abuse of discretion less problematic. The need for China’s government to focus on stability may

---


136 See id. at 14–15 (noting how Russia’s internet community, academics, and activists have all expressed concerns that the creation of an Internet “blacklist” could lead to widespread censorship).


138 Id.

139 Standing Committee of the National People’s Congress, Decision on Issues Related to Strengthening Anti-Terrorism Work art. 2 (Oct. 29, 2011) (China).

140 See Alex P. Schmid, Frameworks for Conceptualising Terrorism, 16 TERRORISM & POLITICAL VIOLENCE 197, 204 (2004).
explain the country’s focus on the dangers terrorists pose to society. Because most other countries do not have a one-party system, China’s definition would be difficult to apply to more politically pluralistic nations.


One of the greatest hurdles for regulating terrorist use of the Internet is arriving at an accepted definition of terrorism itself. Among the definitions of terrorism each Security Council country has adopted, the most effective is France’s definition. With a broad definition followed by detailed acts, it is the least likely to encounter resistance from other countries. To regulate social media, a broad definition is required in order to cover a variety of contexts. Although countries that particularly value freedom of speech like the U.S. would be wary of a broad definition, there are substantial checks that the U.N. can provide to help curtail abuses of discretion.

First, the U.N. provides a forum for debate where members can vote to determine whether a warning or economic sanctions are appropriate. Even if a country adopts the recommended definition, it may be subject to punishment if it does not use the definition appropriately. Second, the U.N. has vast resources to call on to solve the collective action problem, so it can spread the costs of monitoring social media violations and ensure that the definition is not misused. To determine misuses, the most plausible mechanism would be to create a Special Rapporteur or supervise a complaint system where U.N. members can vote to determine when punishments are appropriate. Third, since members are able to report to the U.N., there are adequate protections to keep governments from using the terrorist definition to punish dissenters. An effective monitoring regime and complaint system will allow countries most concerned with violations to keep an eye on and report possible violators. The complaint system can also be open to reports by citizens—although this may open the door to a huge influx of complaints, the sorting of which would be extremely expensive. Even though the U.N. lacks strict enforcement mechanisms, such as a police force, a naming-and-shaming system could at least raise the reputation costs of

141 See Gary King et al., How Censorship in China Allows Government Criticism but Silences Collective Expression, 107 AM. POL. SCI. REV. 1 (2013) (finding that the Chinese government tends to censor speech that endangers stability by proposing collective action, rather than speech that criticizes the government).

142 See generally Saul, supra note 68.

143 Limited definitions would raise the issue of whether a video is threatening but a photograph is not, whether a tweet directed to recruit individuals would technically be a means of violence, etc.
abusive behavior. If a State adopted the recommended definition but was using it to suppress dissent, the U.N. could raise a global outcry to shame it back into compliance.

D. The U.N. Must Also Coordinate with Private Actors

Although private actors alone are insufficient for successful regulation, they must be included in the regulatory process. Historically, the U.N. has worked with private companies in public-private partnerships (PPPs) in order to promote human rights, fair labor practices, environmental protection, and anticorruption. A significant example is the World Intellectual Property Organization (WIPO), one of the specialized agencies of the U.N. created to "encourage creative activity, to promote the protection of intellectual property throughout the world." WIPO has successfully negotiated treaties to protect patents, copyrights, and trademarks worldwide. In The Global Innovation Index, published by WIPO, the organization noted that PPPs help governments become more inventive by creating a space outside the government structure that allows innovation to flourish. PPPs help to inject a broader set of skills and talents, as well as a more diligent and responsive work culture into the government machinery and to create a solid foundation for innovative thinking and creativity.

WIPO's success in protecting intellectual property indicates that private companies are willing to participate and take a role in the regulation process.

In the context of social media regulation, outside groups can provide expertise, such as "corporations like Google; international nonprofit corporations; organizations like the Internet Society, the Internet Engineering Task Force, and the Internet Corporation for Assigned Names and Numbers..."

---

144 For a discussion of why states comply with international law due to a concern for their reputation, see Andrew T. Guzman, How International Law Works: A Rational Choice Theory (2010).

145 Human rights organizations have also used naming and shaming in order to invite international scrutiny of human rights abusers. See, for example, James Meernik et al., The Impact of Human Rights Organizations on Naming and Shaming Campaigns, 56 J. of Conflict Resolution 233 (2012).


Chicago Journal of International Law

States must be aware that any regulation of social media will directly affect private industry, risking infringement on free enterprise. However, private social media platforms are incentivized to cooperate with the U.N. because the U.N. can spread expensive monitoring costs. Furthermore, working with the U.N. to remove terrorist content might improve a company’s standing in the court of public opinion; private companies do not want to be blamed for allowing terrorists to use their platforms. Instead of removing content on their own, private companies will be legitimized by openly cooperating with state governments. Of course, the risk still exists that private actors will limit too much content or fail to limit content at all. But because the U.N. can spread the cost of monitoring, the increased availability of resources can mean more detailed review. This results in closer scrutiny of whether content should be removed.

VI. CONCLUSION

The purpose of this Comment has been to identify the proper role for the U.N. in the regulation of terrorist social media. Although unable to pass a convention on internet or social media governance, the U.N. could still coordinate a successful international response to terrorists proselytizing to disaffected youth on the Internet—a strategy that has recently become more effective and produced horrific consequences. Social media provides important advantages in the new age of technology; it allows broad access around the world, fast reproduction and transmission of information, and is low-cost and easy to use. The U.N.’s attempt to address this issue at the WCIT fostered disagreement between states and produced a treaty that did not bind some of the

150 Loutrione, supra note 122, at 843.

151 See Susan Crabtree, Twitter Pressed to Confront Terrorist Abuse, WASH. EXAMINER (Feb. 6, 2015, 5:00AM), http://www.washingtonexaminer.com/twitter-pressed-to-confront-terrorist-abuse/article/2559893 (last visited May 1, 2015) (“[Social media] companies ... cannot hide behind free-speech rights because they have a basic responsibility to ensure that their platforms are not vehicles for hate speech or worse by terrorists and criminals.”); Michael Isikoff, Twitter Under Pressure to Act More Aggressively Against Terrorists, YAHOO NEWS (Feb. 18, 2015, 4:10AM), http://news.yahoo.com/twitter-under-pressure-to-act-more-aggressively-against-terrorists-230347109.html (last visited May 1, 2015) (quoting Representative Ted Poe, who said “there is frustration with Twitter specifically” for having an insufficient response to removal terrorist content, as well as J.M Berger, who said that “Twitter is notoriously close-mouthed in how they handle suspensions and what goes on in the company”).

biggest actors in the international arena. To curb terrorist use of social media, there should be cooperation between countries, specifically those with the most advanced social media infrastructure and those most likely to be the targets of social-media recruitment. Any attempt to regulate social media must address collective action problems and provide a baseline definition of terrorism. Private actors cannot regulate terrorist content sufficiently on their own but have shown a willingness to cooperate with the U.N. in other aspects of domestic regulation. There are also risks that governments will use social media regulation to curb dissent, and any implementation of a governance structure risks favoring certain countries over others. To resolve these issues, the U.N. should take a role as a coordinator and facilitate cooperation between all of its member states. Although this does not eliminate the possibility of debate between countries, it improves the current situation where there is no coordination at all. Taking a role as a coordinator respects state sovereignty, but also reduces transaction costs. By using its resources to identify abuses of power and determine the best methods to regulate terrorist use, the U.N. can successfully help regulate terrorist use of social media.