

**Forum:** General Assembly 3 (Social, Cultural, and Humanitarian)

**Issue:** Preventing terrorist groups from using the Internet for propaganda purposes

**Student Officer:** Alex Tai

**Position:** Head Chair

---

## Introduction

In the twenty-first century, technology has become an increasingly integral part of our everyday lives. The rapid spread of access to the Internet has taken communication to a whole new level, connecting us in unimaginable ways. It has the aptitude to pull distinct communities together, and empower billions of people, yet it has proven to be a double edged sword. The Internet enabled the instant anonymous delivery of information across the globe. The perks of the development of the Internet is certainly encouraging, but one must also take into consideration of the potential exploitations of these services by terrorist groups. The Internet serves as a platform for terrorist groups to advance their goals and coordinate acts of terror that might generate fear among the general public.

Instant communication may be used by terrorist groups to facilitate propaganda purposes such as recruitment, radicalization, and incitement. This research report will identify and go into detail of the numerous ways in which terrorists may use the Internet for propaganda purposes. It will also make an emphasis on the consideration of the rule of law when attempting to tackle the issue at hand.

## Definition of Key Terms

### Internet

The Internet is an abstract concept of a *network of networks*. It may be defined as a global system of computer networks that is used to connect billions of devices globally. It is the single relationship between all devices online. The internet serves as the primary method of communication to a massive audience with increasingly low entry barriers for access. As of such communication, massive amounts of data/information are carried through the Internet.

Ever since the late 1980s, the Internet has become one of the leading ways of highly dynamic communication. With an ever-increasing audience globally, terrorists exploit such communication to further their agendas.

## **Terrorism**

There are currently no official United Nations (UN) definition for terrorism as the defining process have proven to be controversial in its parameter setting. There has been a definitional hiatus ever since 2000 due to the standoff between the Organization of the Islamic Conference (OIC) and the member states. The OIC wanted to exclude “armed struggle for liberation and self-determination” from the definitional parameter. However, excluding such condition would allow multiple terrorist acts committed by Al Qaeda to avoid label/classification.

Even though there are no internationally agreed upon definition of terrorism, it is a general consensus that terrorism is a strategy of violent action. Terrorism’s purpose is not achieved by the violence itself, but rather by the message of intimidation disseminated to the public.

## **Cyberterrorism**

According to the Center for Strategic and International Studies (CSIS), cyberterrorism is defined as “the use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population.”

## **Censorship**

According to the Global Internet Liberty Campaign, censorship is defined as “the control of the information and ideas circulated within a society.” While censorship may be a threat to fundamental human right to free expression, appropriate censorship may be essential towards combatting terrorism. As stated previously, the purpose of terrorism is achieved only when the message of intimidation is disseminated to the public. With censorship of the message of intimidation, the act of terrorism loses its purpose. As of the current status of the United Nations, multiple resolutions have made it their position to call for global censorship. When drafting their resolutions, delegates should be aware of their country’s official stance on censorship and freedom of expression.

## **Propaganda**

Propaganda is essentially information. What sets propaganda apart from other types of information is its intent. Propaganda is typically dissemination of not only information but also arguments that attempt to influence the public’s opinion. It can be seen as a systematic attempt to manipulate beliefs, attitudes, and/or actions of others.

Propaganda in regards to the issue at hand is extremely important. Propaganda employed by terrorist organizations may be set out to radicalize, incite, and/or recruit potential terrorists. When discussing the issue regarding the preventing terrorist groups from using the Internet for propaganda purposes, one should definitely consider the information that may be put out by the subjects and their intended purpose.

## **Fear mongering**

Fear mongering refers to the use of fear deliberately to influence one's attitude and actions. Normally through the appeal of emotion, fear mongering is used extensively by terrorist organizations with massive publicity. Occasionally, terrorists use fear mongering as a method of negotiation with member states. Public emotions catalyze policy-making within a country and normally pressures the government into taking action.

## **Background Information**

### **Cyberterrorism: A Transnational Issue**

The exponential development of technologies has established an ever growing network with an incredibly global reach. The entry barriers for access to the Internet continue to lower and more and more global citizens connect. The merits of the Internet are abundant, with instant anonymous communication over borders being one of them. With that being said, it is equally important to recognize the potential malpractice of the Internet. With easy access for any and all, terrorist groups may exploit the convenient and elusive nature of the Internet and use it for terrorist purposes such as propaganda and funding.

With the nature of the Internet established, it is conceivable that terrorist use of the Internet and cyberterrorism is a transnational issue. It is a transnational issue that would call for an amalgamated response across member states and among local criminal justice systems.

### ***Role of the United Nations (UN)***

With the United Nations mandate to maintain international peace and security, the UN would logically play a key role in the issue of preventing terrorist groups from using the Internet for propaganda purposes. It addresses the issue at hand with the attitude of cooperation and decides to build consensus regarding common approaches to combating terrorist use of the Internet.

The UN generates relevant universal legal frameworks such as resolutions of the General Assembly (GA), resolutions of the Security Council, and treaties. Resolutions passed within the Security Council are legally binding on member states according to the Charter of the United Nations.

### ***Role of the international community***

Although resolutions of the Security Council are legally binding, the responsibility to carry out sanctions and bring terrorists to justice lies largely with the national/local authorities. In order

to prevent any violation of national sovereignty, international tribunals such as the United Nations generally lack jurisdiction over how punishments and justice are delivered.

## Key Issues

The “Key Issues” section will be separated into many subsections and sub-subsections. The following subsections will be organized based on the ways in which the Internet is utilized by terrorist groups.

### Propaganda

As stated previously, propaganda is information of biased nature spread deliberately to influence the public’s opinions, beliefs, attitudes, and actions. One of the primary functions of the Internet for terrorist purposes would be the dissemination of propaganda. Also previously stated, laws on censorship vary from country to country and the dissemination of propaganda may be considered perfectly legal in some cases. However, most countries have banned propaganda that are aimed towards inciting violence against groups or individuals. The United Nations Office on Drugs and Crime (UNODC) has identified three major intentions of the propaganda disseminated by terrorist organizations through social media and terrorist websites. These three major intentions are recruitment, incitement, and radicalization.

One of the most common theme in terrorist propaganda is the promotion of violence. Propaganda with intentions of incitement may include violent video footage or games designed by terrorist groups to encourage the audience to experience the role virtually. The second most common theme in terrorist propaganda is the usage of extremist rhetoric with the intention of radicalizing the general public. Many of the videos and games mentioned above may also serve to radicalize the intended audience.

A lot of the content within terrorist propaganda may overlap in theme and intention, but it is still necessary to identify the purpose behind these content in order to nullify its impact.

### Recruitment

The contents of terrorist propaganda may appeal to emotions in an attempt to establish relationships with the audience. Fear mongering may often times encourage radical behavior, while sympathetic content may solicit support from the audience to the terrorist group. By sympathizing with their cause, many of the audiences end up aligning their own beliefs and attitudes with terrorists.

It is important to note that these terrorist recruitment propaganda is generally tailored for the marginalized communities as it is easier to relate to groups that are different. The purpose behind this target is evident. Recruitment propaganda feeds off of the feeling of exclusion from these marginalized communities and offers a sense of belonging to the marginalized audience.

## **Incitement**

As previously stated, propaganda and censorship have proven to be a sensitive topic. However, there are no debates over propaganda that incite violence. Contents that encourage acts of terrorism is considered illegal by numerous Member States. Any media that glorifies acts of terrorism is considered an encouragement, and is deemed unlawful.

Censoring content that might incite acts of terrorism is considered legitimate due to one defining reason. According to the International Covenant on Civil and Political Rights (ICCPR) article 19, third paragraph, it is legitimate to deter mobilization of terrorism in the interest of protecting national security and public order.

The problem of incitement lies primarily with the classification of “glorification.” To what extent does a country consider specific contents glorifying? What prerequisites serve to differentiate between mere propaganda and incitement of violence? Without this classification, it will be extremely hard to determine when to apply sanction, and when to be lenient. As this line of acceptability varies from states to states, prosecution of incitement on the international level has proven to be a complex matter.

## **Radicalization**

According to the UNODC, radicalization refers to the “process of indoctrination that often accompanies the transformation of recruits into individuals determined to act with violence based on extremist ideologies.” With that being said, it is conceivable that radicalization involves a great amount of propaganda through the Internet.

The process of radicalization of the general public may be separated into three common levels of rhetoric used by terrorist groups. The United States Institute of Peace (USIP) have identified these distinct deliveries in almost all terrorist propaganda. The first rhetoric is the justification of violence, with the claim of having “no other choice.” This allows the terrorist groups to reason with the audience and present their actions as a necessity in face with an oppressive enemy. In order to make this delivery, terrorist groups attempt to portray themselves as the victim by associating governmental counter-terrorism acts with loaded language such as “murder”, “slaughter”, and “genocide”.

The second rhetoric used for radicalization is the justification of violence on the grounds of a merciless and oppressive enemy. By portraying the actions of the government as immoral, brutal, and inhuman, terrorist groups often times successfully demonize governments. The demonization of governments and the humanization of “freedom fighters” serve as a compelling fallacy for persuasion. Although irrelevant, attacking the opponent rhetorically, also called *ad hominem*, proves to be an extremely effective way of persuasion.

The third and last rhetoric identified by the USIP, is the use of anti-violence language in an attempt to negate the terrorist's violent public perception. Contrary to their actions, many terrorist groups claim to aim ultimately for peaceful negotiations and diplomatic settlements.

### Considerations for the rule-of-law

As previously stated in the censorship section, often times counter-terrorism measures may be controversial in regards to several human rights. Extra care must be given to international human rights standards when taking actions against terrorism. In order to do this, member states are highly encouraged to develop legislative frameworks on counter-terrorism and practices that protect the rule of law as well as the fundamental human rights.

#### *Freedom of expression*

Effective counter-terrorism tactics and the provision of fundamental human rights are not mutually exclusive and may even be complementary when being framed in a mutually reinforcing way. As noted in the second paragraph of the Incitement section, freedom of expression is a fluid right that may be restricted given the situation. When banning incitement to terrorism, restrictions on the freedom of expression is considered legitimate. Please refer to the Incitement section for more information regarding the classification of incitement.

#### *Right to privacy*

Preventing terrorist groups from using the Internet for terrorist purposes may often times involve collection of data relating to potential converts, and surveillance of citizen internet usage. Effective solutions should take extra care to protect persons from arbitrary surveillance. Inspection should not be used carelessly and reasonable doubt should be present when putting a surveillance team in action.

## Major Parties Involved and Their Views

### Counter-Terrorism Implementation Task Force (CTITF)

The Counter-Terrorism Implementation Task Force was established and adopted in a General Assembly resolution called The United Nations Global Counter-Terrorism Strategy. It was established in response to a general consensus between Member States that international cooperation is necessary in the process of countering terrorism. Combining a total of 38 international organizations and dividing the resources of those entities into so called "Working Groups". So in essence, the CTITF is an organization

with a synergistic nature. Its mandate is to “strengthen coordination and coherence of counter-terrorism efforts of the United Nations system.” With that mandate in mind, the CTITF aims to maximize each member organization’s comparative advantage by having specific organizations specialize on particular aspects of themes.

It is important to understand that the CTITF only aligns the agendas and resources of Member States, and that the responsibility of implementing the Global Counter-Terrorism Strategy still lies with the Member States. The CTITF ensures that the entire organization of UN programmes accommodate the needs of the Member States.

### United Nations Office on Drugs and Crime (UNODC)

The United Nations Office on Drugs and Crime was established as a result of an integration between the Centre for International Crime Prevention and the United Nations Drug Control Programme. The primary goals of the UNODC is to assist Member States of the UN in combatting illicit drugs, crime, and terrorism. In 2011, Resolution 66/178 reaffirmed the mandate of the UNODC and went into even greater detail regarding its assistance in combatting terrorism. The resolution made an emphasis on the use of the Internet for terrorist propaganda. Ever since then, the UNODC have been working cohesively together with the CTITF, to provide with legal frameworks and technical strategies for combatting terrorism on the Internet. While there is no single universal approach to combatting terrorism in regards to the use of the Internet, the Office has identified two aspects to work with in developing a comprehensive instrument for countering this type of terrorism: legal and technical. With these two aspects addressed, the UNODC believes that it will bring the international community one step close towards developing a comprehensive criminal justice system.

## Timeline of Relevant Resolutions, Treaties and Events

Date	Description of event
September 14, 2005	<p><b>Security Council Resolution 1624</b></p> <p>The Resolution of the Security Council #1624 is the first resolution to articulate the specific nature of terrorism with regards to the use of the Internet. It specifically addressed the incitement and pardoning of terrorist acts through propaganda.</p>
September 8, 2006	<p><b>United Nations Global Counter-Terrorism Strategy</b></p> <p>The United Nations Global Counter-Terrorism Strategy is General Assembly resolution adopted by the UNGA on 8 September 2006. This adoption established the United Nations Counter-Terrorism Implementation Task Force, a</p>

synergistic organization that aligns international resources for counter-terrorist purposes. The Global Counter-Terrorism Strategy identified four primary pillars of countering terrorism:

1. "Addressing the conditions conducive to the spread of terrorism"
2. "Measures to prevent and combat terrorism"
3. "Measures to build states' capacity to prevent and combat terrorism and to strengthen the role of the united Nations system in that regard;"

"Measures to ensure respect for human rights for all and the rule of law as the fundamental basis for the fight against terrorism"

### **Security Council Resolution 1963**

December 20, 2010

One of the more recent resolutions passed by the Security Council is Resolution 1963 in 2010. The resolution expressed "concern at the increased use, in a globalized society, by the terrorists of new information and communications technologies, in particular the Internet, for the purposes of the recruitment and incitement as well as for the financing, planning and preparation of their activities."

## **Relevant UN Treaties and Events**

- Security Council Resolution 1373, 28 September 2001 (**S/RES/1373**)
- Security Council Resolution 1566, 8 October 2004 (**S/RES/1566**)
- Security Council Resolution 1624, 14 September 2005 (**S/RES/1624**)
- Report of the Secretary-General - Uniting against terrorism: recommendations for a global counter-terrorism strategy, 27 April 2006 (**A/60/825**)
- The United Nations Global Counter-Terrorism Strategy, 8 September 2006 (**A/RES/60/288**)
- Security Council Resolution 1963, 20 December 2010 (**S/RES/1963**)

## **Evaluation of Previous Attempts to Resolve the Issue**

Although preventing terrorist groups from using the Internet for propaganda purposes is a relatively new issue, several attempts have been made by Member States to counter terrorism. According to the Council on Foreign Relations, there have been endless debates over the best way to counter terrorism. One of the main theme of discussion is short-term and long-term solutions. Often times, the situation calls for immediate relief of the consequences and some Member States believe that taking short-term solutions is the first step towards combatting terrorist's use of Internet. Evan Kohlmann,



an expert on terrorism with regards to Internet usage, describes these immediate relief solutions “the knee-jerk reaction is if you see a terrorist website you shut it down.” There are obviously several pros and cons to this type of solution. While it may offer immediate relief to sensitive times where fear is pervasive, it may also lower the chances of governmental investigators from attaining invaluable information regarding terrorist activities. By being discrete about the handling of terrorist websites, investigators may learn valuable information that may prove to be even more essential than shutting down the spread of propaganda.

Some member states have been extremely unforgiving to terrorist sympathizers hosting websites and have taken forceful actions to take down the website. However, in countries like these, numerous counts of freedom of expression charges were raised against the government. Without a clear, non-debatable legal framework, governments would not be able to avoid this problem.

In addition to thinking about these aspects of the solution, delegates should also focus on the development of legal and technical frameworks in order for a less ambiguous justice system and plan of action.

## Possible Solutions

The whole research report primarily focuses on the issues that arise from terrorist usage of the Internet as well as the potential issues that might arise from attempting to tackle the issue. It identified the numerous ways that the Internet may be exploited for recruitment, radicalization, and incitement. Emphasis should incontestably be placed on the implementation of the usage of the Internet as means to detect, deter, and prevent acts of terror. Usages may include gathering intelligence for the prevention of planned acts of terrorism and gathering evidences for the legal prosecution of these acts.

Obvious solutions to combatting radicalization are the use of counter-narrations and rhetoric. Implementing the same persuasive element within the counter-narrations may effectively impede the process of citizen radicalization to terrorist ideals and may also indirectly address the incitement issue. In the next few paragraphs, the report will go over several aspects to consider to construct a comprehensive solution. These aspects are emphasis on international cooperation, private sector cooperation, legal prosecutions, and investigation/ intelligence gathering.

As repeated stated in this present report, preventing terrorist groups from using the Internet for propaganda purposes is a transnational issue and must be solved through international cooperation. There is no exhaustive international treaty on combatting terrorism as of today and as stated in previous sections, there is no internationally agreed upon definition of terrorism. Without this definition, it is extremely hard to advance the cause. With that being said, delegates should aim to define terrorism, while at the same time be sensitive about the potential claims other organizations might have towards

the definition. Miniature terrorist acts that form into part of a crime carried over the Internet may raise complicated issues on jurisdiction. Delegates would need to put some thought into deciding which country's laws and judicial system to be used.

When addressing international cooperation, another creative solution to the issue is cooperation with private sectors. Engagement with private industries such as Internet service providers, website hosting companies, social media companies, and major technological companies such as Google, would facilitate the monitoring process of terrorist content.

As stated earlier, the development of a comprehensive legal instrument is essential for furthering the goal of prevention. With that being said, the implementation of these legal frameworks are also equal in terms of importance. Bringing justice to perpetrators of terrorism and providing safe haven for citizens is also one of the many obligations of Member States. In order to carry out these prosecutorial practices, evidences and intelligence must be collected.

## Bibliography

Barrett, Richard, and Jan Neutze, editors. "Countering the Use of the Internet for Terrorist Purposes - Legal and Technical Aspects." *CTITF Publication Series*, May 2011, <[http://www.un.org/en/terrorism/ctitf/pdfs/ctitf\\_interagency\\_wg\\_compendium\\_legal\\_technical\\_aspects\\_w eb.pdf](http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_w eb.pdf)>.

Brunst, Phillip W. "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet." *Terrorist Use of the Internet*, <[http://link.springer.com/10.1007/978-0-387-89291-7\\_3](http://link.springer.com/10.1007/978-0-387-89291-7_3)>.

"CTITF Office | About." *United Nations*, United Nations, <<https://www.un.org/counterterrorism/ctitf/en/ctitf-office>>.

Kaplan, Eben. "Terrorists and the Internet." *Council on Foreign Relations*, Council on Foreign Relations, 8 Jan. 2009, <<http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005#p7>>.

"Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes." *United Nations Counter-Terrorism Implementation Task Force*, <[http://www.un.org/en/terrorism/ctitf/pdfs/wg6-internet\\_rev1.pdf](http://www.un.org/en/terrorism/ctitf/pdfs/wg6-internet_rev1.pdf)>.

"Security Council Resolution 1373." *Security Council Resolution 1373*, 28 Sept. 2001, *UN Documents*, <[http://www.un.org/en/sc/ctc/specialmeetings/2012/docs/United%20Nations%20Security%20Council%20Resolution%201373%20\(2001\).pdf](http://www.un.org/en/sc/ctc/specialmeetings/2012/docs/United%20Nations%20Security%20Council%20Resolution%201373%20(2001).pdf)>.

"Security Council Resolution 1566." *Security Council Resolution 1566*, 8 Oct. 2004, *UN Documents*, <<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N04/542/82/PDF/N0454282.pdf?OpenElement>>.

"Security Council Resolution 1624." *Security Council Resolution 1624*, 14 Sept. 2005, *UN Documents*, <<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/510/52/PDF/N0551052.pdf?OpenElement>>.

"Security Council Resolution 1963 (S/RES/1963)." *Security Council Resolution 1963*, 20 Dec. 2010, *UN Documents*, <<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/702/23/PDF/N1070223.pdf?OpenElement>>.

Talbot, David. "Terror's Server." *Terror's Server*, MIT Technology Review, 1 Feb. 2005, <<https://www.technologyreview.com/s/403657/terrors-server/>>.

"The United Nations Global Counter-Terrorism Strategy (A/RES/60/288)." *General Assembly Resolution 288*, 8 Sept. 2006, *UN Documents*, <<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/504/88/PDF/N0550488.pdf?OpenElement>>.

"Uniting against Terrorism: Recommendations for a Global Counter-Terrorism Strategy." *Report of the Secretary-General*, 27 Apr. 2006, *UN Documents*, <<http://www.securitycouncilreport.org/atf/cf/%7B65BF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Terr%20A60%20825.pdf>>.

"The Use of the Internet for Terrorist Purposes." *United Nations Office on Drugs and Crime*, Sept. 2012, <[https://www.unodc.org/documents/frontpage/Use\\_of\\_Internet\\_for\\_Terrorist\\_Purposes.pdf](https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf)>.

Weimann, Gabriel. "Https://Www.usip.org/Sites/Default/Files/sr116.Pdf." *United State Institute of Peace USIP*, no. 116, Special Report, Mar. 2004, *Special Report*, <<https://www.usip.org/sites/default/files/sr116.pdf>>.