

IIMUN 2018

**TRACKING NETWORK
COMMUNICATIONS WITHIN TERRORIST
GROUPS**

Forum: The Disarmament and International Security Committee (DISEC)

Issue: Tracking network communications within terrorist groups.

Student Officer: Öykü Özbirinci

Position: Deputy Chair

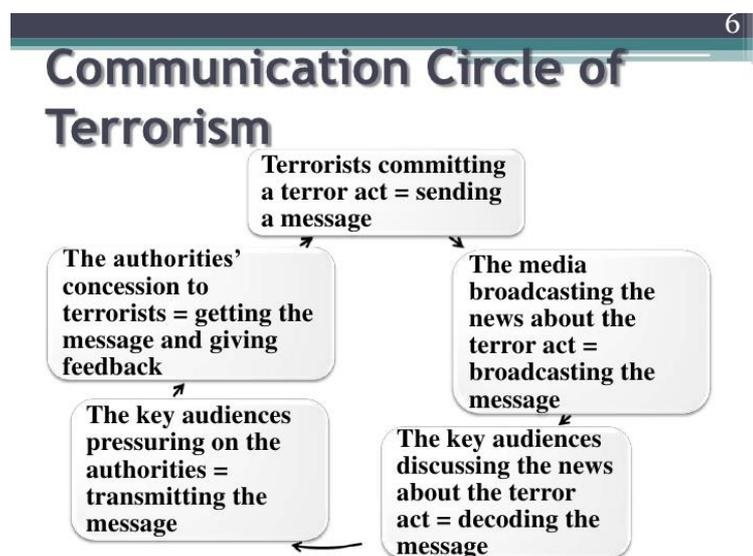
1) Introduction:

a) Introduction:

Terrorist use internet as a tool for communication both with each other and the rest of the world. The public is exposed to propaganda videos of certain terrorist groups on terrorist sites and rebroadcasts on news networks very often. A lot of effort is currently being put into intensifying the surveillance of such sites through which propaganda videos are released. Although the risks posed by the use Internet for communication purposes by terrorist groups are known, there is currently no universal instrument that addresses the pervasive facet of terrorist activity specifically.

There are many ways terrorists use the Internet. Terrorist share information in chat rooms, release propaganda videos, raise funds, plan and coordinate attacks through network communications in addition to their incitement, recruitment, radicalization purposes according to experts. Terrorist organizations also use terrorist websites as virtual training grounds to release tutorials through network services. These tutorials are mostly on topics such as but not limited to building bombs, firing missiles, sneaking through the borders, shooting weapons. When it comes to deciding what constitutes a terrorist website, a terrorist website can be defined simply as contentious as defining terrorism.

When it comes to media use of terrorist groups, there are three main purposes that lay behind the interaction of terrorist groups with media which are attention, recognition and legitimacy in addition to purposes such as demoralizing enemies and creating chaos.



b) Definition of Key Words:

Propaganda: Dissemination of propaganda is one of the many reasons why terrorists use internet as a tool for communication. Propaganda provides ideological or practical instruction, ideas, promotion of terrorist activities and takes the form of multimedia communications. Terrorist propaganda may include audio and video messages, virtual tutorials, presentations, treaties released by terrorist organizations. It is important to take note of the fact that dissemination of propaganda is generally not illegal as it can be justified by fundamental human rights.¹

Incitement: While propaganda per se is generally not prohibited by many Member States, the use of propaganda for incitement purposes is not considered to be legal in most cases. The Internet provides an abundance of materials that can be downloaded, edited and shared which might unlawfully provoke or glorify acts of terrorism. It should be noted that in order for an individual or a group to be held liable for incitement, the propaganda carried out by them must have a direct casual relation with an executed terrorist act.

Radicalization: The process of indoctrination that involves the transformation of recruits into extreme ideologists who are individuals who are determined to act with violence. Radicalization often involves the use of propaganda whether it is via Internet or in person.

Planning: Many criminal justice practitioners defended the fact that every prosecuted terrorist act involved some use of Internet technology. Specifically, the use of Internet technology facilitates remote communication of terrorists and thus, the planning process of acts of terrorism. A recent case from France, Public Prosecutor v. Hicheur ² is a great example that shows how Internet technology is used as a tool for communication among terrorists that facilitates the preparation process for acts of terrorism.

¹ See, International Covenant on Civil and Political Rights (General Assembly resolution 2200 A (XXI), annex), art. 19, para. 2

² Judgement of 4 May 2012, Case No. 0926639036 of the Tribunal de Grande Instance de Paris (14th Chamber/2), Paris.



An undated but verified image posted on a militant website on Jan. 14, 2014 showing fighters from the al-Qaida linked Islamic State of Iraq and the Levant (ISIL), now called the Islamic State group, marching in Raqqa, Syria.³

Militant Website—AP

2) Body:

a) General Overview:

i) Historical Background

Many companies previously made statements that show their effort toward blocking the communication between terrorist groups. For Trend Micro said that it's "cracking down on accounts that open support and spread terrorist propaganda by banning those accounts outright." (Reisinger) Similarly, "We condemn the use of Twitter to promote terrorism and the Twitter Rules make it clear that this type of behavior, or any violent threat, is not permitted on our service," the spokesperson of Twitter said. "As the nature of the terrorist threat has changed, so has our ongoing work in this area. Since the middle of 2015 alone, we've suspended over 125,000 accounts for threatening or promoting terrorist acts, primarily related to ISIS." (Reisinger) These are two examples of the efforts that were put into the prevention of different types of applications' use for terrorist purposes.

ii) Major Parties Involved and Their Views

UNODC: "The United Nations Office on Drugs and Crime (UNODC) plays a vital role in assisting Member States, in addition to its mandate to strengthen the capacity of national criminal justice systems to implement the provisions of the international legal instruments against terrorism and does so in compliance with the principles of rule of law and international human rights standards."⁴

³ Photo taken from <http://fortune.com/2016/05/03/terrorists-email-social-media/>

⁴ See, UNODC. The use of the Internet for terrorist purposes. New York, 2012.

UK: In the United Kingdom, most of the population support the prevention of terrorism: a survey proved that 9 in 10 people are okay with a proportionate loss of privacy that may result from security checks.

USA: A survey that was conducted in 2015 revealed that the number of American citizens that were concerned about violation of civil liberties was only half the number of American citizens that thought the government should do more to combat terrorism.⁵

b) Timeline of Events:

Date of the event	The Event
4 November 1987	South Asian Association for Regional Cooperation Regional Convention on Suppression of Terrorism’s main emphasis is on the principles of the SAARC Charter
22 April 1998	Arab Convention on the Suppression of Terrorism
4 June 1999	Treaty on Cooperation among States Members of the Commonwealth of Independent States in Combating Terrorism
1 July 1999	Convention of the Organization of the Islamic Conference on Combating International Terrorism
1 July 1999	Organization of African Unity Convention on the Prevention and Combating of Terrorism
3 June 2002	Inter-American Convention against Terrorism
2005	Security Council Resolution 1624 Adoption
2006	The United Nations Global Counter-Terrorism Strategy Resolution
11 January 2007	Association of Southeast Asian Nations Convention on Counter Terrorism
11 September 2017	Economic Community of West African States directive on Fighting Cybercrime

3) Conclusion:

a) Previous Attempts to Resolve the Issue

After 9/11 U.S. intelligence intercepts assisted the prevention of some al-Qa`ida plots, which included the 2006 transatlantic airplane plot, the 2007 plot by terrorists that are linked to al-Qaida to bomb U.S. soldiers in Germany, a plot by Najibullah Zazi to bomb New York two years later. National Security Agency’s (NSA) success at the time was widely reported on in the media at the time of the events, and this resulted in the group of terrorists, increasingly moving toward encrypted communications.⁶

⁵ See, Americans feel the tensions between privacy and security concerns, February 19, 2016

⁶ Paul Cruickshank, “Did NSA leaks help al Qaeda?” CNN, June 25, 2013.

In 2006, the General Assembly adopted The United Nations Global Counter-Terrorism Strategy Resolution unanimously which also highlighted certain points of the issue of the use of Internet for terrorist purposes.⁷

Another resolution which is a key resolution from 2005 addresses the glorification and incitement of terrorist acts. In the fourth perambulatory clause of the resolution, the UN Security Council condemns “in the strongest terms the incitement of terrorist acts “and disclaims “attempts at the justification or glorification (*apologia*) of terrorist acts that may incite further terrorist acts”.⁸ In addition, in the first paragraph, it calls upon all States to adopt measures as such which may be appropriate and needed, and parallel to their accountabilities under international law, in order to constrain by law and counter incitement to carry out act of terrorism.

b) Possible Solutions:

We live in an encrypted World in which means of communication is not limited to easy-to-intercept text messages and phone calls. However, although these easy-to-intercept means of communication are not the only ways used by terrorist groups, they can sometimes be great tools to track the communications within terrorist groups up to some point. For instance, mobile service providers keep record of every phone call, every movement, every text message as long as one is carrying a mobile phone. When officials have the required warrant, they are able to access these information that may or may not be classified. Certain applications (like WhatsApp and Telegram) require registering with a phone number and the applications cannot be used without this number. So, as long as officials know this number, they can track terrorist communication activity on these applications the same way that was previously mentioned. With today’s technology, monitoring chats is possible even if the chat is end-to-end encrypted and this is possible if the app used in the chat supports synchronizing conversations or group chats. Furthermore, in the presence of an internet address, the unique identifier of a phone could possibly be discovered by intelligence services (also known as the IMSI or International Mobile Subscriber Identifier).

c) Notes from the chair:

Dear Delegates,

It is honor to take part in IIMUN 2018 as the Deputy Chair of DISEC. DISEC deals with disarmament, global challenges regarding international security and threats to global peace that have an impact on the international community and its aim is to find solutions to the problems that challenge the international security regime. I genuinely hope that every delegate will come up with effective resolutions which will tackle the questions we will be discussing for the duration of the conference. However, in order to achieve this, each delegate

⁷ General Assembly resolution 60/288

⁸ See, UNSC Resolution 1624, 2005

should come up with solutions that is parallel with the view of the country they are representing and not bring in their subjective judgements.

To come to an understanding about this issue and have constructive debates upon it, you will need to comprehend the policies of your countries in addition to basic international law and certain resolutions. I tried my best to simplify and elaborate on some principles in this study guide, but if you still have questions you can feel free to send an inquiry. Our main expectation from you, is for you to find creative and reasonable solutions for this issue.

The things I would suggest using when doing research on your countries' policies prior to the conference are;

- CIA World Factbook Page: <https://www.cia.gov/library/publications/the-world-factbook/>
- Speeches at the UN: <http://research.un.org/en/docs/find/meetings>
- Official Government Websites
- UN Permanent Mission (some of which could be found from the link <https://www.un.int>)
- BBC Timeline (these timelines are very useful for learning what the most important events in your country's history are <http://www.bbc.co.uk/history/interactive/timelines/>)
- IMUNA Country Profile (The International Model United Nations Association has resources on each country <http://www.imuna.org/resources/country-profiles>)

For the delegates that will be representing NGO's, here is the link to a research guide that I find very helpful: <http://bestdelegate.com/ngoguide/>

The documents I would suggest going through once again for further research on the topic of "Tracking network communications within terrorist groups" are the ones listed in the citations at the end of this report.

If any of you have questions, please feel free to send your inquiries to oykuozbirinci@gmail.com

I am looking forward to meeting all of you.

Kind regards,

Oyku Ozbirinci

d) Bibliography:

Allison, Peter Ray. *Tracking terrorists online might invade your privacy*. 9 August 2017.

Field, Antony. "Tracking terrorist networks: problems of intelligence sharing within the UK intelligence community." *Review of International Studies* (2009): pp. 997-1009.

Graham, Robert. "How Terrorists Use Encryption." *CTC Sentinel* June 2016.

Kaplan, Eben. "Terrorists and the Internet." 8 January 2009. *Council on Foreign Relations*.

Reisinger, Don. "The Many Ways Terrorists Communicate Online." *Fortune* 3 May 2016.

Sarah Gordon, Richard Ford. *Cyberterrorism?* Symantec. n.d.

UNODC. *The use of the Internet for terrorist purposes*. New York, 2012.

UN. *Countering the Use of the Internet for Terrorist Purposes — Legal and Technical Aspects*. New York, May 2011.

UNSC. "Resolution 1624." 2005.

The United Nations Global Counter-Terrorism Strategy: Resolution. UN, 2006.