DISARMAMENT AND INTERNATIONAL SECURITY COMMITTEE

Study Guide for Zurich Model United Nations

Written by Kim Studenski and Irina Lehner

May 4th to 7th, 2017

Zurich, Switzerland

CONTENTS

SUBMISSION DEADLINE

Delegates are requested to submit a position paper
A guide on how to write a position paper is available on
http://zumun.ch/preparation/

* * *

Saturday 29th of April 2017

* * *

disec@zumun.ch

YOUR CHAIRS

Honorable Delegates,

We feel more than honored to be welcoming you to the 3rd session of this conference. Organized under the framework of Model United Nations it is eager to reach a wide range of attendants from high schools and universities which are deeply interested in diplomacy, international relations, politics and the United Nations itself while constituting a unique experience of debating and socializing at the same time.

During the three days of ZuMUN you will simulate the First Committee of the General Assembly. Both topics address the pressing topic of terrorism, an issue that has sadly occupied the media over the last couple of years - be it the attack in Berlin, Tel Aviv, Kairo, Kabul, Mogadishu, Brussels, Paris or London.

Topic A looks at international and in particular illicit arms trade in order to help prevent especially the continuous rise of groups like ISIS who occupy territory and terrorize the population. Topic B addresses the issue of how terrorist groups are using social media and ICT in general to create fear, spread their message and recruit individuals for their cause with the same goals, scaring people and spreading their ideology.

This Background Guide serves as an introduction to the topics for this committee. However, it is not intended to replace individual research. We encourage you to explore your Member State's policies in depth and use the Annotated Bibliography and Bibliography to further your knowledge on these topics. For any further questions, please do not hesitate to contact us via president@mun-uzh.org.

We wish you all the best in your preparations and look forward to seeing you at the Conference!

Sincerely,

Kim Studenski, *Chair*

Irina Lehner, *Vice-Chair*

ABOUT THE COMMITTEE: DISEC

The First Committee of the General Assembly is one of the six main committees of the GA and is concerned with disarmament and related international security questions. It looks at global challenges and threats to peace that affect the international community and seeks out solutions to those challenges.

Key considerations include national capabilities and limitations, mitigation of conflict, and oversight and monitoring mechanisms. Because of the nature of the topics discussed, research and resolution writing must be very detailed in nature and focus on the operationalization of ideas. Additionally, due to the divisive nature of many of the discussions, the most effective ideas will be inclusive and focus on international cooperation.

TOPIC A - REGULATING ARMS TRADE IN THE WAR AGAINST TERROR

Introduction

Since the 9/11 attacks in 2001, terrorism has been a key concern worldwide with continued attacks around the world by religious extremists. Are the terrorists simply fanatics to be defeated, or is terrorism a consequence of real global injustices? Can we prevent terrorism without undermining civil liberties?

Political violence has always been a feature of human society, but terrorism as we know it has its roots in the politics of the nineteenth and especially twentieth centuries, as typically small groups of radicals sought to unsettle states and rally support by bombing buildings, assassinating politicians and carrying out other acts of violence. This would not be feasible if it were not for the large amounts of arms that these groups are able to acquire.

Arms dealers sell power—the power to back a regime, the authority to challenge the status quo, and the legitimacy that a gun can lend to an idea. All that an arms dealer asks for in return is money. At such a price, it is no wonder the industry enjoys annual revenues larger than the GDP of some small countries. Guns become highly-prized symbols of power and legitimacy; businesses, aware of their product's enormous influence, will often sell as indiscriminately as possible, even going so far as to arm both sides of a conflict. As a result, arms traders have been implicated in supporting an ever-growing list of violent coups, armed juntas, and terrorist plots.

International Terrorism

Definition(s) of Terrorism

The definition of the word "terrorism" is a very sensitive matter. Thus, there is no universally accepted definition of it, and it is very doubtful that it will ever be found. Attempts and negotiations about a legally binding Comprehensive Convention on International Terrorism by the UN have been under way for decades, with no result to show yet.

Three main sectoral protocols have been drafted: International Convention for the Suppression of Terrorist Bombings (1997); International Convention for the Suppression of the Financing of Terrorism (1999); and International Convention for the Suppression of Acts of Nuclear Terrorism (2005). There is multiple other sectoral conventions, but as stated above there is no comprehensive convention on terrorism.

In most of the common definitions of terrorism, four characteristics are defined:

1. The use or threat of violence aiming at political, religious or ideological change.
2. It can only be committed by non-state actors.

3. It is not aimed at individual target victims but the terror is aimed to influence a government or spread fear among the people.
4. It is a crime both made illegal by legislation and inherently immoral or wrong.

The Global Terrorism Database defines terrorist incidents in a slightly different way:

1. The incident must be intentional, the result of a conscious calculation on the part of the perpetrator.
2. The incident must entail some level of violence or immediate threat of violence.
3. The perpetrators of the incident must be sub-national actors.
4. At least two of the following three criteria must be fulfilled as well:
    a. The act must be aimed at attaining a political, economic, religious or social change.
    b. There must be evidence of an intention to coerce, intimidate, or convey some other message to a larger audience (or audiences) than the immediate victims.
    c. The action must be outside the context of legitimate warfare activities (outside of what is permitted by international humanitarian law).

Additionally, two ways of terrorist behavior can be distinguished: terrorist attacks (e.g. car bombings, shootings; in the “Western world”, Brussels, Paris etc. as well as in any other country) and terrorist so-called states such as ISIS, which have the capability of occupying big territories and have a state-like organization. But these two kinds are often unified in one organization behind them.

A terrorist group is therefore conventionally defined as a non-state actor which resorts to terrorism (see above) in order to achieve its goals. So, not only groups like ISIS or Al-Qaeda which are often called “terrorist groups” by the media etc. can fall under the definition of a terrorist group.

All of these criteria are subject to doubts and debate. One of the most-debated points is if the use of force should be allowed in the context of national liberation and self-determination. In many conflicts, one side considers a group a violent but nonetheless legitimate group of freedom fighters and the other side simply considers this same group terrorist.

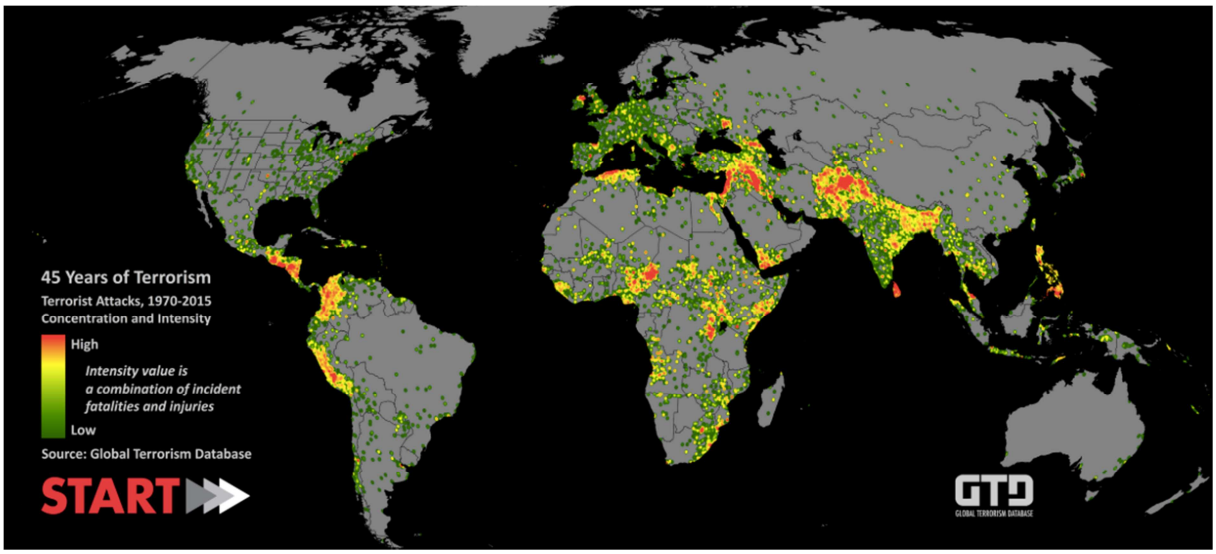
Especially in the 19th and 20th century when colonized countries started to rebel against their oppressing colonial powers, most of them were considered terrorist movements. Due to this the former colonial powers and the formerly colonized nations are not able to find common ground on the definition of terrorism.

Some states may consider a group a legitimate “freedom fighter group”, while other states consider the same group a terrorist rebel group, it is simply a matter of perception.

Overview

The number of incidents labelled as terrorism by the Global Terrorism Database has been rising since the first collection of data in 1970, but it has seen a more significant rise since the beginning of this century.

According to the Global Terrorism Index, the countries with the most terrorist incidents in 2015 were Iraq, Afghanistan, Pakistan, India, Philippines, Yemen, Ukraine, Nigeria, Egypt, Libya and Syria – most of them subject to ongoing conflict.



International Arms Trade

Definitions

Arms

The Cambridge dictionary defines arms as any kind of device used to injure, defeat or destroy in a war or a fight. To the United Nations, arms include most forms of military weaponry such as tanks, armored vehicles, submarines, aircraft carriers, missiles, battleships or gun boats, landmines, machine guns or self-propelled guns, but also small arms such as revolvers and pistols, rifles and carbines.

Armed Conflict

According to the Stockholm International Peace Research Institute, “conflict” is understood as physical confrontation between two or more parties with a clear political incompatibility.

In international humanitarian law, the distinction between “international armed conflicts” and “non-international armed conflicts” is much emphasized. But what both kind of armed conflicts have in common is that they are considered an armed conflict as soon as one or more State or non-governmental group have resorted to armed force against one or several other States or non-governmental groups. This definition applies regardless of the reasons or in-

tensity of the confrontation, even in the absence of open hostilities. No formal declaration of war or recognition of the conflict is needed. In short, defining a situation as an “armed conflict” should be based solely on factual conditions.

However, states are hesitant to admit that they are in fact in a situation of armed conflict. They try to avoid appearing weak and fear to lose influence and importance on an international level. Opposition coming from non-state actors might lead to a government denying the existence of “conflict” altogether; governments might easily choose to ignore such groups on the outside and repress them strongly on the inside.

Facts and Figures

The volume of international arms trade greatly increased during the 20th century and during the Cold War era it was used as a political tool. In the arms race between the USA and the USSR, both nations supplied weapons to their proxies across the world, particularly so-called third world countries, in order to strengthen military and political influence worldwide.

After the Cold War international arms trade declined and reached its low point in 2000. Ever since then – one can’t help but think of 9/11 as a factor contributing greatly to this – international arms trade has been increasing steadily once again. Transfers of major weapons have in the years 2012-16 reached their highest volume since the end of the cold war.

According to estimates, international arms trade amounted to 72 Billion USD in 2010. Recent reports estimate that since then, it has risen to around 100 Billion USD per year.

The five biggest exporters – USA, Russia, China, France, Germany – together account for about three quarters of the total volume of trade exports. 43% of the global imports go to Asia and Oceania, the position of the biggest importer of the world currently being held by India (13% of all arms trade). Other Asian nations such as Vietnam have been greatly increasing (202% increase) their import of arms over the last five years.

Along with Asia and Oceania, the Middle East is the second biggest importing region – 29% of global imports have been made by them in 2012-2016. Saudi Arabia ranks second in the list of biggest arms importers. Qatar increased its imports by 245% over the course of the last five years. Middle Eastern arms imports mainly come from Europe and the USA. Despite lower oil prices, the nations of the Middle East continued to increase their import of weapons due to rising regional tensions and conflicts in the region. This increase in arms import is also viewed as a contributing factor to the instabilities of the region.

On the African continent, Algeria was the largest arms importer (46% of all imports to the region). In sub-Saharan Africa, the largest importers are Nigeria, Sudan and Ethiopia – all currently in the midst of a conflict.

Imports by nations in Europe and the Americas have been decreasing in 2012-2016.

Largest importers of arms (2016)			
		Mio. US$	ATT
1	India	2629	no
2	Saudi Arabia	1550	no
3	China	1357	no
4	Indonesia	1200	no
5	Vietnam	1058	no
6	Taiwan	1039	no
7	UAE	1031	signed
8	Australia	842	ratified
9	Oman	738	no
10	Singapore	717	signed

Largest exporters of arms (2015)			
		Mio. US$	ATT
1	USA	10484	signed
2	Russia	5483	no
3	Germany	2049	ratified
4	France	2013	ratified
5	China	1966	no
6	UK	1214	ratified
7	Spain	1279	ratified
8	Israel	710	signed
9	Italy	570	ratified
10	Netherlands	444	ratified

International action

Arms Trade Treaty

The Arms Trade Treaty is an agreement which was adopted by the United Nations General Assembly. It entered force in 2014 and was ratified by 92 states, as well as signed by another 42. In the final vote of the General Assembly only the Democratic People's Republic of Korea, Iran and Syria voted against it while 23 states abstained (prominent nations amongst those abstaining were China, Russia, India and Saudi Arabia).

The ATT attempts to regulate the international trade of conventional weapons. It aims to contribute to international as well as regional peace, reducing human suffering and promoting co-operation, transparency and responsible action by and among states.

The ATT only regulated international arms trade. It is not meant to restrict domestic arms trade or the right of individuals to carry a gun, in order to respect national sovereignty and legislative power of member states to its full extent.

The ATT requires member states of the UN to supervise their arms exports. They are obliged to ensure that arms embargoes are respected and that no arms are being exported which could be used in violations of human rights or humanitarian law. This includes acts of terrorism. Therefore, the ATT is not only targeting arms trade between nations, but also those nations supplying non-state actors with weapons.

Member states accomplish this goal by imposing and enforcing standardized arms import and export regulations. Furthermore, member states are expected to track the destination of exports, in order for them not to reach destinations where they might be used to commit human rights abuses – neither directly nor via states of transit.

Experts criticize that many nations who are signatories of the ATT or similar agreements do not actually follow the rules they formally accepted.

Examples are:

- China has supplied ammunition and small arms to Sudan, where they are used by security forces and militia in Darfur, as well as to South Sudan and to the DRC.

- France has supplied arms to Libya under al-Gaddafi, Egypt, Israel and Chad, and Syria between 2005 and 2009.
- 10% of all Russian arms exports are believed to go to Syria, making it Syria's largest arms supplier. It has also supplied helicopter gunships to Sudan and is set to be a major exporter of military equipment to Egypt.
- The UK has supplied arms to countries with high-risk behavior when it comes to human rights abuses, such as Sri Lanka.
- The USA has supplied arms to more than 170 countries. It hasn't taken sufficient precautions against Iraq, Israel, Sri Lanka, Bahrain, Egypt and Yemen.

This is partly due to political reasons, since some states similar as in the Cold War era want to support a specific group, philosophy or government. But on the other hand arms producing companies are private companies that are looking for the financial gain no matter what the consequences and find ways to evade regulations.

Programme of Action

The "United Nations Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects" was adopted by the UN in 2001.

The PoA aims to combat illicit arms trade: illegal, clandestine arms trade, which is even more difficult to supervise and regulate than "normal" arms trade – but the harder it may be, the more important it is to try and regulate it.

In contrast to the ATT, the PoA concerns itself only with small arms (which can be used by a single person; e.g. revolvers, pistols, rifles and carabiners etc.) and light weapons (which can be used by one to three people; e.g. machine guns, rifle grenades, portable anti-tank and –aircraft guns etc.). This focus was chosen due to the importance of small arms in illicit trade and the potential danger they pose at the end of a conflict. Then after an armed conflict has ended, many small arms are still around and thus facilitate outbursts of violence even after a conflict has ended.

The PoA requires member states to regulate arms trade and manufacturing within their countries as well as to monitor and regulate export across state borders. Member states must supervise and track such actions, especially in order to enforce existing UN embargoes on a national as well as international level.

Furthermore, member states are called upon to be very attentive to illegal activity related to arms trade. Strict laws and stringent sanctions must be established to punish illegal arms trade and any kind of associated action.

Embargos

An embargo is the prohibition of the trade of certain goods with certain states. It can be imposed by the UN as well as by single states or other entities of states (OSCE, EU).

Some – but rather few – embargoes by the UN are declared mandatory for all member states. They are rarely directed against states – at the moment, only the DRC, Libya, Iran,

Sudan and Belarus are subject to a mandatory UN arms embargo. More often, mandatory UN arms embargoes are directed at non-governmental forces. Sometimes, simply all the non-governmental forces in a nation's territory are concerned (e.g. Iraq, Lebanon, Yemen, Central African Republic, Democratic Republic of the Congo). Other times, groups are directly indicated, for example ISIS, Al-Qaeda or the Taliban.

Other arms embargoes are only imposed by certain states (since usually, not all UN member states agree with embargoes against other states). Often, the "Western world" works together in embargoes. For instance, the EU and USA have about 10 arms embargoes which they uphold jointly. In many cases, some of the other Veto powers such as Russia or China strongly disagree with these embargoes – this for example concerns the embargos against Syria or Iran. But Russia as well as China are themselves subjected to sectional arms embargoes by the EU and the US.

Not all of the mentioned arms embargoes include all arms – for example, the UN embargo on Iran is limited to items that can be used in the context of nuclear weaponry.

Problems and Criticism

Several loop-holes in the regulations on arms trade, more explicitly concerning embargoes, can be named.

First of all often only components of weapons are sold. So a client only buys parts of arms from several countries. Thus, no nation takes the full responsibility.

Furthermore, many national arms companies outsource and produce arms in factories overseas - in countries whose laws are not as strict. And since the law of the factoring nation applies and not the law in country with the seat of the company, they can avoid strict regulations.

Moreover, 20% of all international arms trade is illicit. Therefore, it is hard to supervise or apply restrictions of any kind. Additionally, weapons are often transferred across several borders of neighboring countries. There is a lack of border and port security, especially international control of those. There needs to be a better transboundary approach which holistically attempts to solve the aforementioned issues.

Fueling Terrorism by Trading Arms

Over the past decades, we have experienced major changes both in the dynamics and the understanding of conflicts. Non-state actors have become much more prominent and involved in conflicts of all sorts. The sometimes long-developed, established mechanisms for managing and responding to conflicts by the international community are challenged. The international community only has a limited capacity to hold non-state actors accountable for their actions. The current security governance system, as well as most of the general problem-solving solutions, are by nature a framework for transactions between states – just think about the UN Security Council, which plays a very important role in the discussion of international security and stability issues.

Difficulties in regulating arms trade with non-state actors (including, but not limited to) are:

- Blurred, changing hierarchies within non-governmental groups which leads to unpredictability of these and to difficulties for even starting negotiations, if that is even an option at all.
- Difficulty in communication with the non-state actors as there only exist non-binding contacts which leads to a big unreliability on their statements.
- Missing continuity (in goals, group membership, power levels, …).
- Continued unrest, no distinct phases of conflict or post-conflict; continuation of non-state violence despite formally established peace (e.g. Iraq, Afghanistan).
- Indistinguishable interest ties amongst non-state actors as well as between non-state actors and nations which leads to an unpredictable mixture of economical and geopolitical interests.
- Newest development: The distinction between a state and a non-state actor gets increasingly difficult as former non-state actors start to develop state-like organizations and structure (ISIS, Al-Nusra) and unstable governments seem to lose control of their territory.

Terrorist attacks would not be possible without these groups having access to great quantities of arms. But it is not necessary that they are newly bought. Reports by Amnesty International have shown that as ISIS captured the city of Mosul in Iraq, it suddenly gained access to a large arsenal of weaponry stored there, result of the numerous arms trade actions to Iraq by various international partners (esp. US and ex-Soviet Union). As a result, ISIS uses weapons and munition originating from over 25 countries in the world, manufactured mainly in the years between 1970 and 1990, come to Iraq during the Iran-Iraq war (in which at least 28 nations have supplied weapons to both sides according to AI) and then again during the US-led invasion of Iraq after 2003. Corruption in the military and its control instruments contributed to easing the access to weapons for ISIS. Thus, Arms trade deals done today might as well have an impact on terrorist actions decades from now.

However, access to older weaponry is only one side of the problem. Many nations provide monetary and arms funding to non-state actors which are considered terrorist groups (by other nations). Like ISIS, other groups commonly referred to as terrorist (such as Boko Haram, Al-Nusra or Al-Qaeda) recover a lot of their arms stock from conquered cities and their enemies.

Moreover, the Mafia and similar criminal organizations recover and/or buy arms (often left behind at the end of armed conflicts in unstable regions) and sell them to terrorist organizations.

Finally, some nations openly supply rebel groups – considered terrorist groups by other nations – with weapons to support their local geopolitical interests (e.g. Turkey, Saudi Arabia or the United Arab Emirates to various groups in Syria).

Another issue nowadays is the supply of lone-wolf terrorists. EU officials have confirmed a suspicion that illegal weapons are flowing freely through Europe's 26-country Schengen zone, which allows near frictionless travel across borders, and that European leaders are lagging behind in cracking down on the trade. There are clear links between organized crime and terrorists, and a route that goes from the Balkans. It is an issue which poses new challenges to the international community and urgently needs to be addressed.

Issues a Resolution could/should address

- A universally agreed definition on terrorism has seemed impossible to be reached, but a more concrete definition should be helpful in constructing stricter regulation on terrorism.
- There exist a multitude of sectoral treaties that all partially cover certain problematic areas but often do not get properly implemented and enforced.
- The loop-holes that exist in arms trade make the current international agreements and embargoes seem toothless at times. Closing the loop-holes that get used by big exporters and importers of arms to circumvent international agreements and existing embargoes.
- The outsourcing of the factoring of arms to states with a troubling security leads to arms reaching the black market easier.
- The trade of arms often also happens illicitly and a more restrictive control on trade and shipments might lead to a reduction of arms trade. How can it be prevented that terrorists get their hands on weaponry?
- Terrorists often gain access to weapons by gaining control of stored arms from states. It would be in the interest of most states to reduce this line of access of terrorists to arms.
- Even though the direct support of terrorist groups is something states cannot afford to do there has been evidence in recent years that terrorist groups get directly supplied with arms and/or combat training.

Sources and Further Reading

- https://www.amnesty.org/en/latest/news/2013/03/global-arms-trade-treaty-a-beginners-guide/
- https://www.amnesty.org/en/latest/news/2012/06/big-six-arms-exporters/
- https://www.amnesty.org.uk/how-isis-islamic-state-ISIS-got-its-weapons-iraq-syria
- http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Conflict-Analysis-Tools.pdf
- http://www.start.umd.edu/gtd/
- http://www.start.umd.edu/gtd/downloads/Codebook.pdf
- https://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf

- https://www.sipri.org/commentary/blog/2017/state-major-arms-transfers-8-graphics
- https://www.sipri.org/commentary/essay/2011/global-security-governance-system-meeting-tomorrows-challenges-yesterdays-tools
- https://www.sipri.org/databases/armstransfers

TOPIC B - COMBATING INTERNATIONAL TERRORISM IN THE DIGITAL REALM

Introduction

Since the late 1990s, as global connectivity has increased, terrorist and violent extremist groups have become more sophisticated in their use of information and communications technologies (ICT), in particular the internet and social media, to radicalize and recruit terrorist fighters and supporters, spread propaganda and transfer knowledge and funds or to generate funds in support of their ideas and operations. These developments have important implications for the private sector, in particular those technologies and social media companies whose products and services are used by millions, if not billions of people across the globe.

Terrorist organizations depend on the open media systems of democratic countries to further spread their message and goals. In order to garner publicity towards their cause, terrorist organizations resort to acts of violence and aggression that deliberately target civilians. This method has proven to be effective in gathering attention.

It cannot be denied that although terrorism has proven to be remarkably ineffective as the major weapon for taking down governments and capturing political power, it has been a remarkably successful means of publicizing a political cause and relaying the terrorist threat to a wider audience, particularly in the open and pluralistic countries of the West.

While a media organization may not support the goals of terrorist organizations, it is their job to report current events and issues. In the fiercely competitive media environment, when a terrorist attack occurs, media outlets scramble to cover the event. In doing so the media help to further spread the message of terrorist organizations.

It is the responsibility of all states and the international community to ensure an appropriate balance between national security und civil liberties. Regulations and measures against the spreading of terrorist ideas and ideology are necessary but at what cost? And can terrorists even be stopped in the fast-paced world of social media?

Use of social media

Illicit power is not new. Illicit power structures' use of the Internet is not new. However, illicit power structures' use of social media and video game technology, to the extent that ISIS is using them, is new. And it is dangerous. ISIS's radicalization and recruitment efforts via social media and cyber technology have been very successful in gaining sympathizers worldwide. Terrorists and other illicit organizations understand that the young generation spends a huge amount of its time online, and they target that population for this reason. They realize how vitally important it is to have the young generation in their ranks.

In a study by Gabriel Weimann from the University of Haifa, Weimann found that nearly 90% of organized terrorism on the internet takes place via social media. Terror groups use social

media platforms like Twitter, Facebook, YouTube, and internet forums to spread their messages, recruit members and gather intelligence.

Social media tools are cheap and accessible, facilitate quick, broad dissemination of messages, and allow for unfettered communication with an audience without the filter or "selectivity" of mainstream news outlets. Whereas previously terror groups would release messages via intermediaries, social media platforms allow terror groups to release messages directly to their intended audience and converse with their audience in real time.

Media is ideal to reinforce Westerners' perception of the Islamic State and its devotees as ruthless beyond comprehension. All terrorist groups seek to cultivate this kind of image, of course, because their power derives from their ability to inspire dread out of proportion to the threats they actually pose. But the Islamic State has been singularly successful at that task, thanks to its mastery of modern digital tools, which have transformed the dark arts of making and disseminating propaganda. Never before in history have terrorists had such easy access to the minds and eyeballs of millions.

The Islamic State maximized its reach by exploiting a variety of platforms: social media networks such as Twitter and Facebook, peer-to-peer messaging apps like Telegram and Surespot, and content sharing systems like JustPaste.it. More important, it decentralized its media operations, keeping its feeds flush with content made by autonomous production units from West Africa to the Caucasus. As it established the rudiments of a functioning state, ISIS also was building a decentralized media syndicate. Each wilayat, or province, now runs its own media office, staffed by camera operators and editors who churn out localized content from Nigeria to Afghanistan.

Only a fraction of the Islamic State's online output depicts the kind of sadism for which the group is notorious: Far more common are portrayals of public-works projects, economic development, and military triumphs, frequently aimed at specific Muslim enclaves throughout the world. So far, digital propaganda of this sort has helped motivate more than 30,000 people to turn their backs on everything they have ever known and journey thousands of miles into dangerous lands, where they've been told a paradise awaits.

But the most significant way in which the Islamic State has exhibited its media savviness has been through its embrace of openness. The Islamic State is content to crowdsource its social media activity—and its violence—out to individuals with whom it has no concrete ties. And the organization does not make this happen in the shadows; it does so openly in the West's most beloved precincts of the Internet, co-opting the digital services that have become woven into our daily lives. As a result, the Islamic State's brand has permeated our cultural atmosphere to an outsize degree.

This has allowed the Islamic State to rouse followers that Al-Qaeda never was able to reach. To persuade foreigners to emigrate to the caliphate, the Islamic State produces—in addition to martyrdom videos—literature and videos that emphasize its alleged utopian aspects, particularly the freedom from any trace of religious persecution.

The cockroachlike resilience of the Islamic State's social media cheerleaders has bewildered law enforcement. And even the cleverest algorithms are unlikely to foil the majority of the Islamic State's online acolytes, who are highly incentivized to route around countermeasures. However, the Islamic State has clearly taken risks by opting for openness. Because its supporters are so visible on social media networks, they often attract law-enforcement scrutiny.

But the drawbacks to the Islamic State's online strategy have been outweighed by the advantages. On the most pragmatic level, social media has lowered the bar of entry for recruits, the curious have no problem finding the Islamic State's propaganda in numerous languages, and they can easily connect with intermediaries who will facilitate their travel to the caliphate. Furthermore, the Islamic State's aggressive approach to social media may be most valuable to the organization as a tool to stoke a particular kind of paranoia in the West.

Cyberterrorism

"The electronic war has not yet begun." That was one message released in a video on Monday, May 11, 2015, from a hacker group that claimed to be affiliated with the Islamic State.

These young hackers have tremendous cyber capabilities, which can help the terrorists not only radicalize and recruit new blood but also conduct cyber-attacks on their enemies. Attacks on electrical systems, transportation systems, and the financial sector can be devastating. We have seen such attacks in the past, and we will continue to see this method of warfare in the future. Extremist groups know that they must adapt and change to survive on the changing landscape of war. They will continue to use the Internet to maintain their current methods and will also try to eclipse those methods with new, more effective ones.

"I don't think anyone has any proof that there's an imminent attack or that ISIS has acquired the manpower or the resources to launch an attack on the infrastructure of the United States," said Craig Guiliano, senior threat specialist at security firm TSC Advantage and a former counterterrorism officer with the US Department of Defense. Cyber threats coming from China and Russia were much more advanced currently, but the FBI is concerned about these new organizations recruiting or buying the people and technology with more advanced cyberattack capabilities.

So far, these ISIS-affiliated groups have only been able to deface websites and make headlines in more minor hacking cases. Let's hope it stays that way. Nevertheless, the public and private sector need to prepare for the worst.

Terrorist groups using social media

Since ISIS is the most prominent example using social media it will be described throughout this study guide. However, they are not the only group using it.

ISIS

Isis has proven to be fluent in YouTube, Twitter, Instagram, Tumblr, internet memes and other social media.

Its posting activity has ramped up reaching an all-time high of almost 40,000 tweets in one day as they marched into the northern Iraqi city of Mosul. Twitter has tried to counter ISIS, suspending more than 1,000 accounts it suspected of terrorist links. Amateur videos and images are being uploaded daily by its foot soldiers, which are then globally shared both by ordinary users and mainstream news organizations.

Social-media monitor Recorded Future found that ISIS had succeeded in creating hype with a total of 700,000 accounts discussing the terrorist group.

Al-Qaeda

Al-Qaeda is a militant Sunni Islamist multi-national organization founded in 1988 by Osama bin Laden, Abdullah Azzam, and several other Arab volunteers who fought against the Soviet invasion of Afghanistan in the 1980s.It operates as a network made up of Islamic extremist, Salafist jihadists. Al-Qaeda has an Internet presence spanning nearly two decades.

The Czech Military Intelligence Service commented that Al-Qaeda are spreading its ideology among the Muslim community in Europe, mainly through the means of social media.

The difference between Al-Qaeda and ISIS is, that Al-Qaeda terrorists use the internet to distribute material anonymously or 'meet in dark spaces'. ISIS has taken a direct approach especially when uploading videos of them attacking towns and firing weapons.

Taliban

Taliban is a Sunni Islamic fundamentalist political movement in Afghanistan currently waging war (an insurgency, or jihad) within that country.

Before the Taliban were toppled from power in the US-led invasion of 2001, the Islamist group banned television, cinemas and photography as un-Islamic. Only an abrupt but brutal defeat by Western militaries in 2001 caused the Taliban to embrace technology. Much like Al-Qaeda in Iraq (which would later fracture to become the Islamic State or ISIS), Taliban militants filmed their attacks and posted them to the Internet, hoping to convince local audiences of the group’s impending return to power and foreign ones of the war in Afghanistan’s ultimate futility.

Now, the Taliban are active on a variety of media platforms. They recently began releasing audio files with songs and news updates, and launched a smartphone app for their Voice of Jihad website, available in multiple languages. Their videos, once grainy, are sleek and widely shared. From their hide-outs on both sides of the Afghan-Pakistani border, Taliban have started accounts on open platforms that often stayed below the radar of the companies that operate them. In late 2015, the group began using Telegram Messenger for official communications, following a similar move early in the year by Islamic State, whose technical

experts had determined the messaging app was among the most secure encrypted platforms. The complexity of the Taliban's presence on social media is startling in its scope.

When social networking services ban terrorist-linked accounts, channels, and pages, the Taliban will tell its supporters through available means of communication where to find the latest outlets of its news agency, rebuilt through fresh numbers and usernames.

ISIS has used social media to recruit thousands of non-Arab foreigners and strengthen the legitimacy of its global caliphate in the Muslim world. The Taliban, meanwhile, only has ambitions to rule Afghanistan, a country with 31% literacy where the computers and smartphones needed to access social media are scarce. Public relations have been a separate disaster, with the Taliban's popularity declining from 56% in 2009 to 29% in 2011. Its tiny audience therefore has little reach and less hope of growing.

However, the Taliban is using social media not for the instant gains on which ISIS thrives but as an example of soft power to achieve long-term goals. The Taliban's limited but targeted broadcasts to audiences in the Muslim and Western worlds can help it achieve its long-held goal of expelling foreign soldiers from Afghanistan as military adventures in the country lose more popularity.

However, social media could prove a mixed blessing for the Taliban in the short term. On the one hand, smartphones give American combat drones flying over Afghanistan and Pakistan an excellent opportunity to monitor and target Taliban members, perhaps including the militants' leader killed earlier this year. On the other, application software with end-to-end encryption such as Telegram, Viber, and WhatsApp has made the CIA's job of surveilling the militants much more difficult.

For now, the Taliban forms part of a wider trend in which local revolutionaries and terrorists, maybe inspired by ISIS, use social media to brand themselves and plot their agendas. Throughout the failed coup d'état in Turkey, the military putschists schemed over WhatsApp. In a similar fashion, Shia militias in Iraq are pushing their narratives over broadcasting satellite services.

Boko Haram

Boko Haram is an Islamic extremist group based in northeastern Nigeria, also active in Chad, Niger and northern Cameroon.

On 18 January 2015, an Arabic-language Twitter account purporting to be the official outlet for a new Boko Haram media group called Al-Urwah al-Wuthqa was launched and immediately promoted by key pro-IS media operatives.

Since then, the group has used the feed to publish a stream of propaganda, including several new videos, although there has been some disruption to its media activities following the suspension of the original account by Twitter.

The increased sophistication and organization of the propaganda that followed the launch of the Twitter account bore signs of the influence of ISIS, which has honed its social media

exploitation over the past year. It appears that the group may have been assisted by ISIS media operatives, or influenced by ISIS in an indirect way. But despite the marked improvements in quality, Boko Haram's overall media package remains some way off the sophistication of IS' output.

Since the launch of the Boko Haram Twitter account, there have been inconsistencies in the group's media operation, suggesting that a lack of professionalism may persist among those responsible for publishing the group's propaganda.

Attempts to thwart the use of social media by terror groups

So far, most attempts to neutralize the Islamic State's media juggernaut have proven ineffective. That is because the architects of the countermeasures fail to grasp what makes the organizations content and distribution method so distinctive. ISIS got that way by diligently analyzing how the West manufactures and consumes information and doing the same. To chip away at what they've created, the international community must learn from them.

One approach is to make social media companies responsible for what is posted on their sites, for example some US government officials have urged social media companies to stop hosting content from terror groups and social media providers have repeatedly shut down accounts affiliated with extremists. But as described in the next chapter, there is some issues with that even though Facebook and others have policies concerning terrorist content.

Moreover, there is many people who say that if the media spreads these news they support and legitimize terrorist groups. However, there is no proof how important social media actually is in drawing members to them since most people would never do something violent (join a terrorist group when seeing their content). Furthermore, locating terrorists via their social media accounts has helped law enforcement in the past tremendously.

Some believe the answer is that no new laws are needed, or justifiable, any more than it would be tolerable to enact laws restricting speech over the telephone, in a newspaper or a book, on a street corner, or in a church, mosque or synagogue.

Even if YouTube pulled down every video, radical groups could post the same videos on their own Web sites. Trying to restrain the Internet is a game of "whack-a-mole" that cannot be won. Having the videos on YouTube may even be a good thing, because it makes it easier for law enforcement officials, the media and the public to monitor the groups and their messages.

Social Media sites encourage the exchange of information even though that is exactly what we would like to prevent with terrorist messages. We need to realize several things in order to learn from this trend and combat it effectively:

- Understand social media's role and process as an accelerator/ multiplier.
- Develop open and agile public and private market sector cyberterrorism strategies and practices – governments must work together with industry in order to ideally

align national policy – the challenge is to find the balance between the right to privacy and the use of social media vs. the security capabilities available to law enforcement.

- Continue educating the public with appropriate messages – communication, the public needs to understand all sides of social media.

Terrorism is a real concern. But if we give up our fundamental rights, the terrorists win. If people use speech to engage in criminal acts, they should be prosecuted. Cutting off free speech is never the right answer. Online social media is not only a potent way to promote terrorism, but also a necessary tool in preventing it. It is the emerging challenge for the West: to regain the cyber territory it has long ceded to extremists.

Private Sector

Companies feel a business incentive to create a digital environment where their users feel safe and are increasingly compelled by governments to cooperate in blocking, filtering, countering or removing content or accounts on the grounds of public safety or national security concerns. In addition, users expect the companies to be transparent, accountable, respect privacy and freedom of opinion and expression and guarantee remedy while also ensuring an open, free and secure internet.

Unlike other sectors such as the telecommunications sectors which are highly regulated and formal requirements and obligations have already been established, regulation concerning the internet remains largely voluntary, due in in large part to the trans-border complexities of the domain itself.

There is a growing trend of self-regulation efforts among industry actors in response to online terrorist content and activity. Driven by business, user and government prerogatives, major technology and social media companies are investing significant resources in developing voluntary measures to respond to terrorist use of their products and services and involve:

- Adapting terms of use and community guidelines to prohibit certain content, activity and shape norms of behavior
- Guidance and systems for content flagging etc. incl. law enforcement
- Transparency for government requests
- Cooperation such as image hashing between private cooperation and also between companies and governments
- Tools against narratives of terrorists and similar.

A suiting example is the in late March 2016 by the Taliban created app which was released on Google's Play store. Short after the release the company quickly deleted it. It appeared soon after on Amazon.com Inc.'s Appstore, where it was also taken down. The two companies said they prohibit apps that contain illegal or offensive content.

Amazon says on its website that it reviews all apps submitted to its store to ensure they comply with its protocols and don't include offensive material, violate copyright or contain malicious code, among other things.

A spokesman for Alphabet Inc.'s Google said that the company previously relied on automated scans of apps for policy violations and on users to flag potential problem apps. In March 2015, the company launched a new system in which employees review every app that is submitted. The spokesman said Google made the change to expedite app approvals but didn't say how humans would approve apps faster than software.

The Taliban app continues to be available elsewhere, however. The Taliban media team has promoted the link to download it through their accounts on messaging services and social media platforms.

Twitter that has similar problems says that violent threats and the promotion of terrorism deserve no place on Twitter and their rules make that clear. They have teams around the world actively investigating reports of rule violations, and they work with law enforcement entities around the world when appropriate. Twitter's policies specifically state that users may not make threats of violence or promote violence, including threatening or promoting terrorism.

In December 2010, in response to growing demands that YouTube pull video content from terrorist groups from its servers, the company added a "promotes terrorism" option under the "violent or repulsive content" category that viewers can select to "flag" offensive content.

Similarly, Facebook states on its website that it removes content that expresses support for groups that are involved in the violent or criminal behavior related to terrorist activity or organized criminal activity. Facebook has managed to block ISIS-related accounts and posts more effectively than other sites, of all the companies, they are the leader and the best at removing content.

The regulations and guidelines created by social media companies are definitely a step into the right direction, but we have to ask ourselves, how we can make this process more effective and efficient. For the international community it is important to continue to work together with the private sector in order to fight this effectively. However, ISIS and its supporters continually create new IDs which they then use to resurge back with new accounts and sites for propaganda. As stated above banning this content permanently and continuously from social media is simply impossible, there needs to be a multilateral approach.

UN efforts

The UN has already started in 2005 to address the issue and asked in Security Council Resolution 1624 to prevent the abusive use of ICT by terrorists. In SC Resolution 2129 the Counter-Terrorism Committee Executive Directorate (CTED) was tasked with addressing this issue in consultation with Member States, international, regional, and sub regional or-

ganizations, the private sector, and civil society, and to advise the Committee on further approaches.

In September 2014, Resolution 2178 was passed which included the following clause:

7. Expresses its strong determination to consider listing pursuant to resolution 2161 (2014) individuals, groups, undertakings and entities associated with Al-Qaida who are financing, arming, planning, or recruiting for them, or otherwise supporting their acts or activities, including through information and communications technologies, such as the internet, social media, or any other means;

With this Resolution the position and work of the CTED was further strengthened and the necessity of fighting this threat recognized.

Nowadays, CTED's work focuses on four pillars:

- Mainstreaming ICT in its assessment of Member States' implementation of the aforementioned resolutions
- The promotion of industry-self-regulation
- Strengthening mutual legal assistance regarding digital content
- Promoting counter-messaging techniques

In a meeting in May 2016 the CTED was tasked to submit a comprehensive international framework (in May 2017) to effectively counter the ways that terrorist groups use their narrative to encourage, motivate and recruit other to commit terrorist acts. Furthermore, the UN has met in several Special meetings, organized by CTED, on this topic.

The common issue expressed by a number of participants in a special meeting of the Counter-Terrorism Committee, held at the United Nations in New York on 1 December 2016 was that exploitation of the Internet and social media for terrorist purposes can only be defeated through sustained and comprehensive action involving the active participation and collaboration of Member States, international and regional organizations, civil society, and the private sector. Thereby representatives of the private sector underscored their commitment to preventing the exploitation of ICT for terrorist purposes.

Participants in the special meeting and the accompanying technical sessions included Member States, international and regional organizations, United Nations entities, the private sector, academia, faith-based leaders, and civil society representatives. Having relevant actors from various sectors gathered in the same room provided an opportunity for dialogue and for a frank discussion about challenges and ways forward. The CTED plans to continue this holistic approach, however, it is only a subcommittee of the Security Council and their approaches need to be more applicable for everyone.

Catching terrorists via social media

Greater online visibility also carries greater risks for jihadists. By using social media they become more vulnerable to tracking systems and several members of Taliban have been tracked down with the help of the aforementioned.

However, law enforcement agencies are still not aware enough of how much social media could help in not only tracking terrorists but also preventing attacks by lone-wolf terrorists that operate without concrete support but have been radicalized through the internet. Furthermore, there is now also the problem that crimes are being live-streamed over the internet.

For example the gunman who committed a massacre at a popular gay nightclub in Orlando Omar Mateen, extensively used social media, posted several articles on Facebook and even during the crime he continues using social media. A couple of days later two French police men were killed by a terrorist who posted a video to FB. There is several more of these examples especially since ISIS has declared war on the West.

Facebook said in response that they are trying to remove content as quickly as possible however they are struggling to remove content and stopping crimes from being live-streamed. CloudFlare, which provides a content delivery network and Internet security services said that they work closely with government authorities to counter extremist activity online. “When we get notice that there is a site that is using us that may be illegal or involving content that may be problematic, we reach out to our contacts in law enforcement,” the head of CloudFare said.

Almost every major terrorist attack on Western soil in the past fifteen years has been committed by people who were already known to law enforcement.

In each of these cases, the authorities were not missing the data. But what they failed to do was appreciate the significance of the data they already had. The N.S.A. vacuums up Internet searches, social-media content, and, most controversially, the records (known as metadata) of United States phone calls—who called whom, for how long, and from where. The agency stores the metadata for five years, possibly longer. But there is only really one example of a case where, but for the use of bulk phone-records collection, terrorist activity was stopped.

In the thirteen years that have passed since 9/11, the N.S.A. has used Section 215 of the Patriot Act to take in records from hundreds of billions of domestic phone calls. Congress was explicit about why it passed the Patriot Act—despite concerns about potential effects on civil liberties, it believed that the law was necessary to prevent another attack on the scale of 9/11. The government has not shown any instance besides one in which the law’s metadata provision has directly led to a conviction in a terrorism case. Is it worth it?

The question that comes up is, how feasible is it to evaluate posts on Facebook or Twitter as part of a screening process - especially if people aren't posting under their real names? It is possible, but complicated. Individual investigations would slow down the visa process,

potentially hurting business and tourism. And the tech industry has pushed back against past efforts to enlist it in reporting users' content to the government, citing privacy concerns.

But policing online activity is tricky because a company like Facebook faces legal, technical, and ethical considerations in flagging such content. From a technical point of view, analytics, natural language artificial intelligence, and sentiment analysis software have all reached the stage that given a body of information (like Facebook postings), it is reasonable to expect them to be able to identify threatening communication. That said, it's far from 100% and there would also be false positives.

From the legal point of view, there are regulations that "require or compel" companies to participate in criminal investigations with the government. But ethically, companies do face some murky waters.

How do you separate a high-vitriol comment in the heat of an election season from legitimate threats? And is it right for all of us to be watched and potentially flagged to the government? Would we then use or trust these services?

Several problems pose:

- A solution might be to adjust the parameters more specifically, but especially lone-wolf terrorists have complicated this, since everyone could have been radicalized.
- What makes this more difficult is that these posts are published under an alias account. Facebook does its best to generate accurate identity information but it’s far from perfect.
- At the moment there are just not the right protocols or practices or maybe even policies that allow for the look at social media, as part of the vetting process. We should be looking at any and all information tied to an individual applicant. It is kind of worrisome that the private sector can identify your needs, desires and interest by analyzing your behavior, what you like etc. but governments struggle with finding and analyzing individuals that pose a threat to society.

Tech giants like Twitter, Yahoo. Facebook, and Google recently pushed back against a US Senate proposal that called for the companies to alert federal authorities about suspicions of terrorist activities. All of these sites have policies banning terrorist threats or content like video of beheadings, but they expressed concern that such legislation could get companies in hot water for missing a post or a tweet -- which are sometimes vague -- that could signal an impending terror attack.

Beyond company concerns, users have expressed doubts over whether their own online privacy could be compromised by a more thorough review of social media posts. Finding and fighting terrorists is very difficult and we do need all the advantages we can get in that fight. But from a sociological perspective, we need privacy and from a purely practical point of view, if someone thinks you are going to blab everything you post to the government, they are just not going to use your service.

Questions a Resolution should address

To defeat the new homegrown terrorist threat, the UN must carefully develop and implement the cohesive and comprehensive approach and apply it to an effective outreach and communications strategy. We must isolate and discredit the violent Islamist ideology as a cause worth supporting, let alone a cause worth advancing by attacking and killing one's neighbors and fellow citizens. In developing such a strategy, the international community must address several key questions including:

- How can the international community effectively work together to stop this transborder issue?
- How can the future threat of cyberterrorism already be prevented now?
- What are the tools and strategies needed to continue to thwart the use of social media and the radicalization of individuals?
- What role should the private sector play and what are the responsibilities who help spread this message?
- Freedom of expression vs. threat to (inter)national security
- How can we use social media to catch terrorists or individuals with terrorist intentions?
- What, if any, new laws, resources and tactics other than those already employed by intelligence and law enforcement should be used to prevent the spread of the ideology?
- What should a communications strategy, both on and off the Internet, look like, and what role, if any, should governments have in carrying out that strategy? What role must community and religious leaders play?
- What is the purpose of current outreach efforts, and how can those efforts improve, especially with increased coordination at all levels?
- What role should local officials and local law enforcement play given their longstanding relationships with the communities they serve and the fact that they are better positioned to recognize and intervene, if and when it is necessary to do so?

These are just a few of the pivotal questions that must be answered if the threat of homegrown terrorism inspired by violent Islamist ideology on the Internet is to be defeated.

Conclusion

Illicit power structures will continue to use the Internet and new technology—to spread their extremist message, to execute attacks, and to recruit women to their cause. The importance of women within these groups worldwide must not be discounted. If counterterrorism officials can work with other women and focus on changing the hearts and minds of females within these groups, perhaps these mothers at home will begin to teach their sons

and daughters to fight with their words and counter the extremists' distortion of the Quran, instead of taking up arms.

As the above sections demonstrate, the use of the Internet by Al-Qaeda and other violent Islamist extremist groups has expanded the terrorist threat to the world. No longer is the threat just from abroad, as was the case with the attacks of September 11, 2001; the threat is now increasingly from within, from homegrown terrorists who are inspired by violent Islamist ideology to plan and execute attacks where they live. One of the primary drivers of this new threat is the use of the Internet to enlist individuals or groups of individuals to join the cause without ever affiliating with a terrorist organization.

As this homegrown terrorist threat evolves, so too must our response. It must go beyond classified intelligence and law enforcement programs. Current efforts that rely on relatively uncoordinated outreach to Muslim communities and fragmented communications strategies must be improved. Indeed, the most credible voices in isolating and rejecting violent Islamist ideology are those of Muslim community leaders, religious leaders, and other non-governmental actors who must play a more visible and vocal role in discrediting and providing alternatives to violent Islamist ideology.

Over the past year, the law enforcement and intelligence communities have made it clear that they expect this threat to grow, especially as the Internet continues to be used to spread the terrorists' message, to enlist followers, and to provide more ways to pursue the terrorists' destructive goals. Member states must stay ahead of this threat by pursuing national strategies to counter the influence of the ideology. This is a critical challenge and they must work quickly and aggressively to overcome it.

If we're serious about winning this media game, time is of the essence. To offset some losses in the Middle East, the Islamic State is now moving to strengthen its North African wilayats. The group is already on the verge of turning Libya into its newest stronghold, which is why it's so important right now to dissuade young men and women around the globe from pledging their futures to the caliphate.

Sources

- http://www.nytimes.com/2008/05/25/opinion/25sun1.html?_r=2
- http://www.bbc.com/news/world-africa-31522469
- https://www.offiziere.ch/wp-content/uploads-001/2016/11/Afghanistans-Taliban-Push-Into-New-Media-WSJ.pdf
- http://thediplomat.com/2016/09/the-talibans-latest-battlefield-social-media/
- http://www.cbsnews.com/news/could-policing-social-media-prevent-terrorist-attacks/
- http://www.telegraph.co.uk/news/worldnews/islamic-state/11207681/How-terrorists-are-using-social-media.html
- https://en.wikipedia.org/wiki/Terrorism_and_social_media

- http://www.cnbc.com/2016/10/05/most-young-terrorist-recruitment-is-linked-to-social-media-said-doj-official.html
- https://www.un.org/sc/ctc/focus-areas/information-and-communication-technologies/
- https://www.un.org/press/en/2014/sc11580.doc.htm
- http://www.un.org/apps/news/story.asp?NewsID=52850#.WMZomKIo82w
- http://www.govtech.com/em/safety/Terrorists-And-Social-Media.html
- https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/
- http://www.un.org/en/sc/ctc/news/2015-11-18_CTED_SpecialMeeting_ICT.html
- https://www.un.org/sc/ctc/blog/event/special-meeting-of-the-security-council-counter-terrorism-committee-on-preventing-the-exploitation-of-information-and-communication-technologies-ict-for-terrorist-purposes-while-respecting-human-ri/
- http://foreignpolicy.com/2011/12/08/somalias-al-shabab-militants-rebrand/
- http://www.un.org/en/ga/first/
- http://www.govtech.com/em/safety/Terrorists-And-Social-Media.html
- http://www.telegraph.co.uk/news/worldnews/islamic-state/11207681/How-terrorists-are-using-social-media.html
- https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/
- http://www.govtech.com/em/safety/Cyber-Terrorism-ISIS-Cyber-Caliphate-Threat.html
- https://townhall.com/tipsheet/cortneyobrien/2016/06/16/cnn-cias-terror-report-didnt-inspire-much-hope-n2179302
- http://www.newyorker.com/magazine/2015/01/26/whole-haystack

Further Reading

- http://www.cfr.org/terrorism-and-technology/violent-islamist-extremism-internet-homegrown-terrorist-threat/p16216
- http://www.hsgac.senate.gov//imo/media/doc/IslamistReport.pdf?attempt=2
- http://cco.ndu.edu/Portals/96/Documents/books/Impunity/CHAP_13%20Recruitment%20and%20Radicalization.pdf?ver=2017-01-19-102815-587
- http://ict4peace.org/wp-content/uploads/2016/12/Private-Sector-Engagement-in-Responding-to-the-Use-of-the-Internet-and-ICT-for-Terrorist-Purposes-2.pdf
- https://www.oig.dhs.gov/assets/Mgmt/2017/OIG-17-40-Feb17.pdf