Forum: General Assembly 1

Issue: The question of having measures to guard against the use of internet for terrorist purposes

Student Officer: Joseph Whitehead

Position: Head Chair

Introduction

The internet, a modern tool for communication, has come under scrutiny in recent times. While it creates and consolidates global connections, it has also emerged as a powerful platform for terrorist organisations to propagate extremist ideologies, recruit followers, and coordinate attacks. This troubling phenomenon has sparked a significant debate regarding the necessity of measures aimed at preventing the misuse of the internet for terrorist purposes.

Proponents of stringent regulations argue that without effective oversight, the internet serves as an unregulated space where dangerous content can flourish, posing a substantial threat to national and global security. They argue that proactive measures are essential to preventing the radicalization of individuals and dismantling the online networks that facilitate terrorism. Conversely, critics raise concerns about the potential infringement on the right to free expression that such measures may result in. They argue that protective measures could interfere in legitimate discourse and drive extremist activities underground, making them harder to detect.

Recent statistics show the urgency of addressing this issue. In 2022, reports indicated a marked increase in online terrorist activity, with the number of extremist propaganda materials circulating on social media platforms rising by over 30%. This highlights the need for collaborative international efforts to develop strategies that protect both public safety and fundamental rights.

Background Information

With the rise of internet use over the past decades, there has been a proportional rise in extremist groups and ideologies being shared online along with the radicalization of vulnerable people. This is shown by reports from various organisations that have indicated that online extremist content has increased significantly, with some studies showing a rise of over 30% in extremist propaganda on social media platforms in recent years. On top of this, research by the Institute for Strategic Dialogue found that approximately 70% of individuals who joined terrorist organisations reported being influenced by online content, highlighting the internet's role in recruitment. Furthermore, a study by the Global Internet Forum to Counter Terrorism (GIFCT) revealed that 85% of terrorist groups actively use social media to disseminate their messages and recruit new members..

The importance of measures to counteract internet terrorism can be highlighted by these previous statistics, and evidence of them being implemented and taking effect are demonstrated because, according to the Global Counterterrorism Index, governments worldwide spent over $120 billion on counter-terrorism measures in 2021, with a growing portion allocated to online monitoring and countering extremist narratives. This can be further shown by a 2020 study by Facebook that found that its content moderation algorithms were able to identify and remove 94% of extremist content before it was reported, indicating the potential for technological solutions in combating online terrorism.

Major Countries and Organisations Involved

- **United Nations**: Creates worldwide structures to tackle online terrorist content, such as UN Security Council Resolution 2354.
- **Global Internet Forum to Counter Terrorism (GIFCT)**: A tech-industry collaboration (Facebook, Microsoft, Twitter, and YouTube) focused on combating online extremism through shared databases and technology.
- **European Union (EU)**: Carries out laws such as the Digital Services Act to hold internet companies responsible for damaging content, such as propaganda from extremists
- **Interpol**: International policing body that aids member countries in counter-terrorism by sharing intelligence on cyber activities linked to terrorism.
- **National Counterterrorism Center (NCTC)**: Analyses online extremist content as part of the coordination of U.S. counterterrorism activities.
- **Tech Against Terrorism**: A UN-backed organisation that helps tech companies, particularly smaller platforms, develop strategies to detect and prevent terrorist content.

- **Internet Referral Unit (IRU) - Europol**: Identifies and reports terrorist propaganda on digital platforms, working with tech companies to remove harmful content.
- **Digital Trust & Safety Partnership (DTSP)**: A coalition of online companies working to encourage safer online practices and prevent extremist groups from exploiting them.
- **Electronic Frontier Foundation (EFF)**: Advocates for protection of free speech and civil liberties online while calling for protection from online terrorist groups.
- **Europol:** Launches its counter-terrorism unit, which later expands to address threats from online extremist content

Timeline of Events

Date	Description of Event
September 28, 2001	**UN resolution 1373, The UN mandates preventive measures against terrorism post 9/11, including the monitoring of online activities to disrupt terrorist communications.**
January 1, 2006	**Europol launches its counter-terrorism unit, which later expands to address threats from online extremist content**
December 3, 2015	**EU Internet Forum Launched - The EU collaborates with tech companies to reduce the online spread of extremism, promoting voluntary removal of terrorist content from social media.**

May 24, 2017	The UN passes Resolution 2354 to strengthen global cooperation in countering terrorist propaganda online, advocating for coordinated strategies.
June 26, 2017	Facebook, Microsoft, Twitter, and YouTube join forces to create GIFCT, aimed at reducing terrorist content on their platforms through shared resources.
May 15, 2019	Christchurch Call to Action - Following the Christchurch attack, New Zealand and France lead a global pledge to prevent extremist use of social media, with support from governments and tech firms.
December 15, 2020	EU's Digital Services Act (DSA) Proposed The DSA introduces new responsibilities for tech companies to moderate illegal content, including extremism, with plans for implementation in 2024.
October 7, 2022	U.S. National Counterterrorism Strategy Updated The U.S. revises its counterterrorism strategy, with an increased focus on preventing online radicalization through enhanced monitoring

Challenges and Obstacles

- **Anonymous user profiles:** Prevention of extremist content online can be hindered by users profiles being anonymous and the inability of algorithms to detect differences between real and bot profiles.
- **Platform Migration:** Extremist groups can easily move to other social media platforms when banned meaning algorithms need to be constantly updated to look for these changes.

- **Data Sharing and Privacy Concerns:** Privacy regulations can result in companies being unable to send relevant data to governments resulting in an inability for effective implementation of counter-terrorism measures.
- **Resource Limitations for Smaller Platforms:** Smaller platforms can lack the resources needed to add algorithm updates that the large platforms can afford to do, resulting in extremist propaganda flourishing on these platforms.
- **Extremist group Tactics:** Terrorists have many methods to evade detection such as code language and disguised profiles which can result in their posts going untraced.
- **Global policy Differences:** Differing international policies can make it challenging to reach a consensus on counterterrorism measures, which complicates efforts to enact and implement regulations.
- **Limited Accountability for Encrypted Platforms:** Extremists may communicate without worrying about being watched due to encrypted messaging apps like Telegram, which makes it more difficult for law officials to keep tabs on activities and identify risks.
- **Balance Between Security and Free Expression:** Efforts to fight extremism online often raise concerns about free speech, as overly restrictive measures can infringe on genuine free expression, causing infringement on civil liberties.

Previous Attempts to Solve the Issue

United Nations security council resolution 1373, was passed in 200, following 9/11, and encourages countries to collaborate on counter-terrorism measures by requiring countries to criminalise the financing of terrorism, freezing terrorist linked assets, preventing terrorist recruitment, and increasing information sharing between nations to prevent terrorist activities. United Nations security council Resolution 2354 specifically addressed the spread of terrorist propaganda online, recommending cross-border information sharing and digital security measures.

The Global Internet Forum to Counter Terrorism (GIFCT) was created in 2017 by a coalition of online platforms such as facebook, Microsoft, twitter, and youtube to share databases and use machine learning to remove extremist content online. The GIFCT's efforts have set a standard among private sector platforms for content moderation.

The European Union (EU) has seen large involvement in regulation of online content. The EU internet forum enabled tech firms to cooperate with governmental organisations to voluntarily remove harmful online content. The Digital Services Act (DSA) was proposed in 2020 to enforce obligations on tech companies and platforms and make them legally liable for enabling content such as extremist propaganda to be spread on their platform.

The Christchurch Call, following the terrorist attack in Christchurch, New Zealand, enabled governments and tech companies to collaborate, aiming to prevent social media from being used to promote terrorism by establishing rules and standards to make monitoring online content more effective and efficient. These rules included but were not limited to preventing upload of violent content, immediate response and removal, allowing users to report content and promoting counter narratives.

Possible Solutions

- **Strengthen international legal frameworks:** This can be done by creating internationally recognised content moderation standards, by bridging differing national policies which in turn will allow countries to coordinate more effectively.
- **Enhance cooperation between governments and tech companies:** Creating relationships between tech companies and governments to identify and remove threatening or extremist content and creating shared databases to use machine learning algorithms to further enhance the efficiency of extremist content recognition.
- **Develop and implement national legislation on cybersecurity:** mandate reports from tech companies about potential terrorist activities and require transparency about how these threats are dealt with.
- **Promote digital literacy and counter-extremism programs:** helps individuals identify and report extremist propaganda and to understand the risk associated with this type of content, and working with educators to spread awareness of these issues.
- **Improve international information sharing and intelligence cooperation:** establish secure international communication in which member states can freely

exchange information on potential online threats, and develop standard protocols to deal with terrorist content when flagged.

- **Protect privacy and human rights:** implement safeguards that ensure radical terrorist content can be identified and dealt with efficiently while ensuring the private data of individuals is not at risk and their civil liberties and freedom of speech are not infringed by setting up organisations to review legislations in place to decide if they are too invasive or not protective enough.

- **Provide technical assistance and financial support:** providing aid to poorer countries and smaller social media platforms can give them the capital necessary to implement their own counter-terrorism measures which they would not have had the finance or knowledge to set up before.

- **Monitor emerging technologies:** Monitoring emerging technology such as Artificial Intelligence can help counter terrorist organisations understand the technology and know how it can be applied for terrorist purposes, allowing them to be better prepared for if it happens allowing them to deal with it swiftkey.

Questions for Considerations

1. What regulatory frameworks exist to counter online extremism, and how effective have they been?
2. How can social media algorithms and AI be improved to detect extremist content without violating privacy?
3. What role should governments and tech companies play in countering online extremism, and how can they collaborate more effectively?
4. How does the balance between free speech and security play into policies regulating online content?
5. What are the challenges and ethical considerations of using surveillance technologies to monitor extremist content online?
6. How can smaller platforms with limited resources address extremist content effectively?

7. What impact do extremist content regulations have on legitimate content and discourse?
8. What are the most common tactics used by extremists to evade detection on online platforms, and how can countermeasures be adapted?
9. How does the international legal landscape affect the enforcement of anti-extremist regulations?
10. What alternative measures, such as promoting counter-narratives, are available, and how effective are they compared to content removal?
11. How can law enforcement agencies track and prevent the use of encrypted communication platforms for terrorist activities?
12. What are the legal challenges associated with cross-border enforcement of anti-terrorism regulations on digital platforms?
13. How can tech companies better support researchers and NGOs in identifying emerging extremist trends without compromising user privacy?
14. What role do online gaming platforms and other non-traditional social spaces play in the spread of extremist ideologies?
15. How can content moderation policies be adjusted to respond to the evolving tactics of extremist groups in real-time?

Bibliography

Weimann, gabriel. “Generating Terror: The Risks of Generative AI Exploitation”. January 2024
https://ctc.westpoint.edu/generating-terror-the-risks-of-generative-ai-exploitation/

The UK parliament. “online extremism”. may 2020
\https://researchbriefings.files.parliament.uk/documents/POST-PN-0622/POST-PN-0622.pdf

Bickert, Monica. “hard questions: what are we doing to stay ahead of terrorists?” november 8 2018
https://about.fb.com/news/2018/11/staying-ahead-of-terrorists/

Fishman, Brian. “Dual-use regulation: Managing hate and terrorism online before and after section 230 reform”. March 14 2023 https://www.brookings.edu/articles/dual-use-regulation-managing-hate-and-terrorism-online-before-and-after-section-230-reform/

Afina, Yasmin. “Towards a global approach to digital platform regulation”. January 8 2024 https://www.chathamhouse.org/2024/01/towards-global-approach-digital-platform-regulation/summary

Binder, Jens. “Terrorism and the internet: How dangerous is online radicalization?”. october 13 2022 https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2022.997390/full

Baron, Quinn. “balancing free speech and social media regulation”. november 9 2022 https://www.law.uchicago.edu/news/balancing-free-speech-and-social-media-regulation

US supreme court. “Reno v. ACLU”. June 26 1997 https://supreme.justia.com/cases/federal/us/521/844/#:~:text=ACLU%2C%20521%20U.S.%20844%20(1997)&text=A%20law%20may%20violate%20the,as%20well%20as%20unprotected%20speech.&text=The%20federal%20government%20enacted%20the,access%20to%20explicit%20material%20online.

Samples. John. “Why the government should not regulate content moderation of social media”. April 9 2019 https://www.cato.org/policy-analysis/why-government-should-not-regulate-content-moderation-social-media

GIFTC. “Terrorist and violent extremist exploitation of the Internet threatens open societies everywhere.” https://gifct.org/about/#:~:text=The%20Global%20Internet%20Forum%20to,extremists%20from%20exploiting%20digital%20platforms.

Interpol. “INTERPOL and UN publish joint handbook for online counter-terrorism investigations” July 11 2019. https://www.interpol.int/en/News-and-Events/News/2019/INTERPOL-and-UN-publish-joint-handbook-for-online-counter-terrorism-investigations

the christchurch call. “Working together to eliminate terrorist and violent extremism content online.”

https://www.christchurchcall.org/

European commission. “the digital services act” https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

United Nations resolution 1373 https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf

United Nations resolution 2354 https://documents.un.org/doc/undoc/gen/n17/149/22/pdf/n1714922.pdf

Saltman, Erin. “challenges in combatting terrorism and extrimism online”. July 11 2021 https://www.lawfaremedia.org/article/challenges-combating-terrorism-and-extremism-online

Nicholson, Joanne. “Countering violent extremism online”. June 28 2023 https://www.rand.org/pubs/research_reports/RRA2773-1.html

Williams, Heather. “The Promise—and Pitfalls—of Researching Extremism Online” July 17 2023 https://www.rand.org/pubs/commentary/2023/07/the-promise-and-pitfalls-of-researching-extremism-online.html