Terorrism, Radicalization, and Extremism

Peter Carragher, adapted from Mariana Olaizola Rosenblat and Inga Kristina Trauthig

Terorrism, Radicalization, and Extremism

2026-04-18

Terorrism, Radicalization, and Extremism

Peter Carragher, adapted from Mariana Olaizola Rosenblat and Inga Kristina Trauthig

Learning Objectives

- Understand the concepts of terrorism, extremism and radicalization in relation to the online space.
- Explore existing and potential future ways of countering online extremism.
- Analyze the role online platforms play in facilitating extremist activity by examining two case studies: the January 6th insurrection at the US Capitol and in gaming sites.

Learning Objectives

Today we will:

- Understand the concepts of terrorism, extremism and radicalization in relation to the online space.
- Explore existing and potential future ways of countering online extremism.
- Analyze the role online platforms play in facilitating extremist activity by examining two case studies: the January 6th insurrection at the US Capitol and in gaming sites.

Framing questions

- How is extremism related to, and different from, online hate speech?
- Is the removal of extremist content from the Internet an effective measure to counter extremism?
- What are the benefits and drawbacks of using AI to counter extremism?
- How does extremists' use of encrypted messaging platforms impact the effectiveness of available counter-extremism tools?
- How can law shape online platforms' response to online extremism, and what are law's limitations?
- What should be the roles of the private and public sectors, respectively, in countering extremism and terrorism online?
- How will emerging technologies, such as "the DWeb" and "metaverse" change the ways that extremists exploit online platforms?

Framing questions

- How is extremism related to, and different from, online hate speech?
- Is the removal of extremist content from the Internet an effective measure to counter extremism?
- What are the benefits and drawbacks of using AI to counter extremism?
- How does extremists' use of encrypted messaging platforms impact the effectiveness of available counter-extremism tools?
- How can law shape online platforms' response to online extremism, and what are law's limitations?
- What should be the roles of the private and public sectors, respectively, in countering extremism and terrorism online?
- How will emerging technologies, such as "the DWeb" and "metaverse" change the ways that extremists exploit online platforms?

Defining “extremism”

Defining “extremism”

Relativistic definition: a belief system that lies outside the bounds of currently acceptable/mainstream norms of society. Context-dependent (Neumann)

vs.

Non-relativistic definition: a belief system held together by an unwavering hostility towards a specific “out-group.” Focused on inter-group hostility (Berger)

Bottom line: No universally accepted definition of extremism. Some convergence among academics (see Charlie Winter et al., “Online Extremism: Research”)

No internationally binding treaty or customary international norm defining extremism (https://www.uscirf.gov/sites/default/files/Legislation%20Factsheet%20-%20Extremism_0.pdf).

Defining “terrorism”

Defining “terrorism”

Behavior-focused definition: “premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents” (US Dept of State)

vs.

Belief-focused definition: “a doctrine about the presumed effectiveness of a special form or tactic of fear-generating, coercive political violence” (Schmid)

[Feel free to add others!]

National governments employ different definitions, some of them quite problematic. E.g.:

- US: Terrorism is defined in Title 22 Chapter 38 U.S. Code § 2656f(d), for purposes of the State Department’s annual country reports on terrorism, as “premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents.”
  - FBI differentiates between international and domestic terrorism;
  - USAID defines violent extremism as “advocating, engaging in, preparing, or otherwise supporting ideologically motivated or justified violence to further social, economic, and political objectives.”
- UK: Terrorism is an action or threat designed to influence the government or intimidate the public. Its purpose is to advance a political, religious or ideological cause (UK Terrorism Act 2006).
  - “Extremism is the vocal or active opposition to our fundamental values, including democracy, the rule of law, individual liberty, and respect and tolerance for different faiths and beliefs. We also regard calls for the death of members of our armed forces as extremist” (UK The Counter Extremism Strategy 2015)
- Russia: “terrorism shall mean the ideology of violence and the practice of influencing the adoption of a decision by public authorities, local self-government bodies or international organizations connected with frightening the population and (or) other forms of unlawful violent actions”.
  - A terrorism act can mean the “popularisation of terrorist ideas, dissemination of materials or information urging terrorist activities...” (Counteraction Against Terrorism Law of March 2006)
  - Any court may add texts to the Federal List of Extremist Materials. As of January 2019, there were over 4,000 items on this list, including many religious texts with no apparent connections to militancy. The list includes the translation of the Bible used by the Jehovah’s Witnesses, which in 2017 was the first centralized religious organization to be banned as an extremist organization in the country.

Defining “terrorism”

Defining “terrorism”

Behavior-focused definition: “premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents” (US Dept of State)

vs.

Belief-focused definition: “a doctrine about the presumed effectiveness of a special form or tactic of fear-generating, coercive political violence” (Schmid)

NOTE: duplicate slide to make space for notes

- Tajikistan: the extremism law punishes “extremist, terrorist, or revolutionary activities” without requiring acts that involve violence or incitement of imminent violence.
  - Trials under these charges lack due process and procedural safeguards. The Tajik government uses concerns over Islamist extremism to justify actions against participants in certain religious or political activities.
- Saudi Arabia: the 2014 counterterrorism law and related legislation criminalized as terrorism virtually all forms of peaceful dissent. Terrorism also included calling into question the fundamentals of Islam.
  - While the counterterrorism law was amended in 2017 to address some of the human rights concerns by referencing the use of violence as one possible aspect of terrorism, the law still contains overly broad definitions and continues to be applied against activists.
- China: Legislation applicable in Xinjiang province identifies 15 types of behavior the government views as extremist, such as wearing an “abnormal” beard, wearing a veil, or following halal practices (Muslim dietary laws).

***Counter-extremism measures taken by states must be consistent with international human rights standards on, e.g., freedom of religion or belief, freedom of opinion and expression, and the freedom of peaceful assembly and association. Under IHRL, each of these rights can be limited only in very narrow circumstances. Any restrictions need to conform with standards of legality, legitimacy, necessity and proportionality

https://www.uscirf.gov/sites/default/files/Legislation%20Factsheet%20-%20Extremism_0.pdf

Defining “radicalization”

Defining “radicalization”

“A process leading towards the increased use of political violence” (della Porta and La Free)

“Change in beliefs, feelings, and behaviors in directions that increasingly justify intergroup violence and demand sacrifice in defense of the group” (McCauley and Moskalenko)

“The set of processes that causes attitudinal change that leads towards the use of violence” (Neumann and Rogers)

See Charlie Winter et al., “Online Extremism: Research Trends in Internet Activism, Radicalization, and Counter-Strategies,” International Journal of Conflict and Violence, Vol. 14 (2020) https://www.ijcv.org/index.php/ijcv/article/view/3809

10-minute exercise

10-minute exercise

Turn to the person next to you. In pairs, draft workable definitions for (1) extremism and (2) terrorism for your fictional online platform's community standards.

Use examples to illustrate the types of content and behavior you are seeking to prohibit on the platform.

[Alternative exercise: have groups look up and critique Facebook's community guidelines on extremism and terrorism]

Dominant strains of extremism online

- Radical Islamists and Salafi-jihadis
- Far-right extremists, alt-right, white supremacists
- Manosphere, incelosphere
- Left-wing extremists, sometimes focused on environmental issues

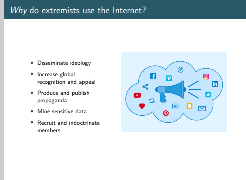
Dominant strains of extremism online

- Radical Islamists and Salafi-jihadis
- Far-right extremists, alt-right, white supremacists
- Manosphere, incelosphere
- Left-wing extremists, sometimes focused on environmental issues

(There is overlap as well as reciprocal radicalization between all of them)

Why do extremists use the Internet?

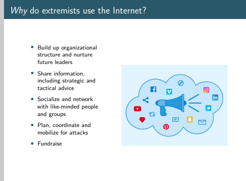
- Disseminate ideology
- Increase global recognition and appeal
- Produce and publish propaganda
- Mine sensitive data
- Recruit and indoctrinate members



Pic from google with creative commons license

Why do extremists use the Internet?

- Build up organizational structure and nurture future leaders
- Share information, including strategic and tactical advice
- Socialize and network with like-minded people and groups
- Plan, coordinate and mobilize for attacks
- Fundraise



Pic from google with creative commons license

How do extremists use the Internet?

- Extremists rely on different platforms (fringe, mainstream, encrypted) for different reasons (audience reach vs. security, for example), and platform migration is common.
- E.g., in early 2023, far-right actors migrated from Telegram to TamTam, and in 2016 ISIS supported moved from Twitter to Telegram.

How do extremists use the Internet?
- Extremists rely on different platforms (fringe, mainstream, encrypted) for different reasons (audience reach vs. security, for example), and platform migration is common.
- E.g., in early 2023, far-right actors migrated from Telegram to TamTam, and in 2016 ISIS supported moved from Twitter to Telegram.

Pic from this report: https://crestresearch.ac.uk/resources/how-telegram-disruption-impacts-jihadist-platform-migration/

Countering online extremism - the role of platforms

- Content removal
- Account suspensions
- Counter-speech / counter-activism

- Counter-messaging
- Awareness-raising / education

Countering online extremism - the role of platforms

Reactive/defensive measures:

- Content removal
- Account suspensions
- Counter-speech / counter-activism

Proactive/offensive measures:

- Counter-messaging
- Awareness-raising / education

Discuss pros and cons.

Technological approaches: AI

- Generative AI apps like Chat-GPT increase the speed and ease of generating extremist disinformation.
- Deepfakes and other synthetic media enable the creation of propaganda materials that can be used in social media disinformation campaigns to manipulate public opinion.

- AI models can be trained to spot AI-manipulated audio-visual content.
- Large hash (digital fingerprint) databases are used to scan online services for matching terrorist content in real time and a high scale.
- Artificial data produced by general adversarial networks (GANs) can also be used to train algorithms.
- Social network analysis (SNA) can be used for understanding and modelling network structures and identifying the main actors or groups therein.

Technological approaches: AI

Challenges:

- Generative AI apps like Chat-GPT increase the speed and ease of generating extremist disinformation.
- Deepfakes and other synthetic media enable the creation of propaganda materials that can be used in social media disinformation campaigns to manipulate public opinion.

Opportunities/solutions:

- AI models can be trained to spot AI-manipulated audio-visual content.
- Large hash (digital fingerprint) databases are used to scan online services for matching terrorist content in real time and a high scale.
- Artificial data produced by general adversarial networks (GANs) can also be used to train algorithms.
- Social network analysis (SNA) can be used for understanding and modelling network structures and identifying the main actors or groups therein.

Open-source databases on terrorism, such as the Global Terrorism Database and GIFCT hash database, can be used for the purposes of training algorithms.

In December 2016, Facebook, Twitter, Google and Microsoft announced plans to tackle extremist content such as terrorist recruitment videos and violent terrorist imagery using PhotoDNA (previously used to identify CSAM)

Human rights risks of AI deployment

- Privacy risks
- Infringement on freedom of thought and freedom of association
  - Especially when takedowns are mandated by public authorities.
  - Lack of clear and adequate definitions of extremism and terrorism in many legal systems allows these terms to be weaponized to crack down on political opponents.
- Discrimination
  - Bias in data fed to algorithms results in discriminatory AI.

- Lack of consensus definitions of extremism and terrorism, respectively, can lead to fragmented data collection.

Human rights risks of AI deployment
- Privacy risks
- Infringement on freedom of thought and freedom of association
  - Especially when takedowns are mandated by public authorities.
  - Lack of clear and adequate definitions of extremism and terrorism in many legal systems allows these terms to be weaponized to crack down on political opponents.
- Discrimination
  - Bias in data fed to algorithms results in discriminatory AI.

Other reminders / cautionary notes about AI:
- Lack of consensus definitions of extremism and terrorism, respectively, can lead to fragmented data collection.

The mass and indiscriminate collection of data online in order to gather intelligence carries inherent privacy risks. Need proper safeguards on storage and use.

Without a clear and narrow definition of illegal extremist and terrorist content, enforced takedowns and other punitive actions can infringe on freedom of expression and thought. (*"law enforcement and counter-terrorism agencies aiming to use AI-enabled technologies to direct users at risk of radicalization to counter-narrative content need to consider the possibility that these technologies could result in unlawful interference with the right to freedom of thought through the manipulation of the way that the targeted users think"*).

Targeting individuals for differential treatment based on protected characteristics contravenes right to non-discrimination. AI-enabled systems can discriminate against vulnerable groups by screening for indicators that act as proxies for protected characteristics.

Countering online extremism – The role of law/regulation

2021/784

- Since June 2022, all tech companies offering their services in the EU are required to take action against terrorist content found on their platforms.
- Hosting service providers must remove terrorist content within one hour of receiving a removal order issued by competent authorities.
- Internet platforms that do not systematically comply with the rules are liable to be fined up to 4
- Resources: Tech Against Terrorism Europe (TATE) provides a free, bespoke and comprehensive programme of support to hosting service providers to ensure to compliance with the regulations.

Countering online extremism – The role of law/regulation
EU Rules on Terrorist Content Online (2021/784)
- Since June 2022, all tech companies offering their services in the EU are required to take action against terrorist content found on their platforms.
- Hosting service providers must remove terrorist content within one hour of receiving a removal order issued by competent authorities.
- Internet platforms that do not systematically comply with the rules are liable to be fined up to 4
- Resources: Tech Against Terrorism Europe (TATE) provides a free, bespoke and comprehensive programme of support to hosting service providers to ensure to compliance with the regulations.

Europe has been a leader in advancing online platform regulation.

Countering online extremism – The role of law/regulation

- As of November 2022, online platforms are required to remove content that is illegal in any EU Member State, suspend accounts that disseminate illegal content—including hate speech, terrorist content, child sexual abuse material, and disinformation—and report criminal behavior.
- Very large online platforms need to produce an annual risk assessment and undergo an independent audit, have risk mitigation measures in place, and appoint a compliance officer for illegal content obligations.

Countering online extremism – The role of law/regulation

EU Digital Services Act

- As of November 2022, online platforms are required to remove content that is illegal in any EU Member State, suspend accounts that disseminate illegal content—including hate speech, terrorist content, child sexual abuse material, and disinformation—and report criminal behavior.
- Very large online platforms need to produce an annual risk assessment and undergo an independent audit, have risk mitigation measures in place, and appoint a compliance officer for illegal content obligations.

Europe has been a leader in advancing online platform regulation.

Countering online extremism – The role of law/regulation II

- *Gonzalez v. Google LLC*
- *Twitter, Inc. v. Taamneh*

Countering online extremism – The role of law/regulation II

US Anti-Terrorism Act (ATA)

Justice Against Sponsors of Terrorism Act (JASTA)

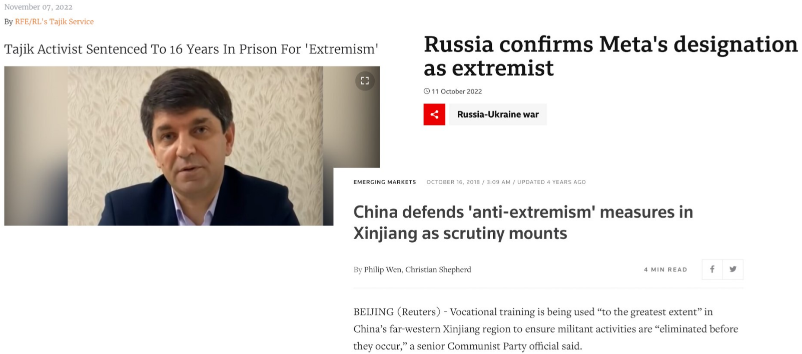
Does Section 230 of the Communications Decency Act exempt online platforms from liability when they algorithmically promote terrorist content?

Supreme Court cases (decision pending)

- *Gonzalez v. Google LLC*
- *Twitter, Inc. v. Taamneh*

The US federal govt doesn't (yet) regulate online platforms directly.

How anti-extremism laws can be weaponized *against* human rights



November 07, 2022

By RFE/RL's Tajik Service

Tajik Activist Sentenced To 16 Years In Prison For 'Extremism'

Russia confirms Meta's designation as extremist

11 October 2022

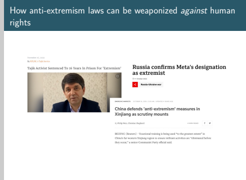
Russia-Ukraine war

EMERGING MARKETS OCTOBER 16, 2018 / 3:09 AM / UPDATED 4 YEARS AGO

China defends 'anti-extremism' measures in Xinjiang as scrutiny mounts

By Philip Wen, Christian Shepherd 4 MIN READ

BEIJING (Reuters) - Vocational training is being used "to the greatest extent" in China's far-western Xinjiang region to ensure militant activities are "eliminated before they occur," a senior Communist Party official said.

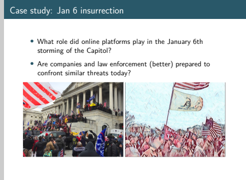


A few examples from Russia, Tajikistan, China.

- China: Legislation applicable in Xinjiang province identifies 15 types of behavior the government views as extremist, such as wearing an "abnormal" beard, wearing a veil, or following halal practices (Muslim dietary laws).
- Tajikistan: the extremism law punishes "extremist, terrorist, or revolutionary activities" without requiring acts that involve violence or incitement of imminent violence. Law has been used to punish political opposition.
- Russia: following its invasion of Ukraine, Russia designated Facebook as an extremist org because Facebook wouldn't comply with Russian gov commands.

Case study: Jan 6 insurrection

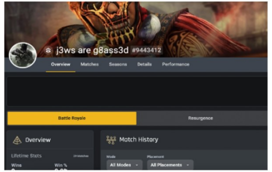
- What role did online platforms play in the January 6th storming of the Capitol?
- Are companies and law enforcement (better) prepared to confront similar threats today?

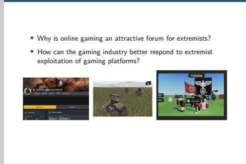


Right corner picture: Taken from report "The WOmen of Jan 6th" by the Program of Extremism in DC: https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Women-of-Jan6_Matfess-and-Margolin.pdf

Case study: Online gaming

- Why is online gaming an attractive forum for extremists?
- How can the gaming industry better respond to extremist exploitation of gaming platforms?





Screenshots taken by NYU Stern Center for Business and Human Rights.

Top left: screenshot of ISIS propaganda videos created by the 16-year-old Singaporean teenager using Roblox game footage.

Bottom left: neo-Nazi username in Call of Duty leaderboard.

Bottom right: Nazi village on Roblox.

What next?

- DWeb technology could be exploited for data storage and retrieval purposes. In that case, “[...] decentralized methods of data storage could make it difficult, if not practically impossible, for a single entity to censor content”
- Will this make it impossible for extremist content to be removed and will thus be accessible to anyone who knows where to find it?
- Are extremists already relying on Dweb technologies? Which ones and why?

- How will the metaverse enable new forms of extremist and terrorist recruitment, networking and coordination?
- How will existing counter-extremism measures fare in an immersive, always-on 3D virtual space?
- Who will be responsible for policing the metaverse?
- What proactive steps can industry and government take to prevent and mitigate extremist exploitation of this new expansive virtual realm?

2026-04-18

└What next?

What next?

DWeb (decentralized web)

- DWeb technology could be exploited for data storage and retrieval purposes. In that case, “[...] decentralized methods of data storage could make it difficult, if not practically impossible, for a single entity to censor content”
- Will this make it impossible for extremist content to be removed and will thus be accessible to anyone who knows where to find it?
- Are extremists already relying on Dweb technologies? Which ones and why?

Metaverse

- How will the metaverse enable new forms of extremist and terrorist recruitment, networking and coordination?
- How will existing counter-extremism measures fare in an immersive, always-on 3D virtual space?
- Who will be responsible for policing the metaverse?
- What proactive steps can industry and government take to prevent and mitigate extremist exploitation of this new expansive virtual realm?

Readings / References

1. Online extremism and potential countermeasures:
   Charlie Winter et al., "Online Extremism: Research Trends in Internet Activism, Radicalization, and Counter-Strategies," *International Journal of Conflict and Violence*, Vol. 14 (2020) https://www.ijcv.org/index.php/ijcv/article/view/3809

2. Overview of suggested solutions in academia:
   Correa, D., & Sureka, A. Solutions to detect and analyze online radicalization: a survey. *arXiv preprint arXiv:1301.4916 (2013)*. https://arxiv.org/abs/1301.4916

3. Countering Terrorism Online with Artificial Intelligence:
   An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia, United Nations Office of Counter-Terrorism and United Nations Counter-Terrorism Centre (2021), pp. 10-14, 23-34, 43-49. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/countering-terrorism-online-with-ai-uncct-unicri-report-web.pdf

4. Social media's role in the Jan 6th insurrection:
   Case study – Jen Patja Howell, The Lawfare Podcast: A Jan. 6 Committee Staffer on Social Media and the Insurrection (Feb. 8, 2023) https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/countering-terrorism-online-with-ai-uncct-unicri-report-web.pdf

5. Gaming sites and extremists:
   "Gaming the System: How Extremists Exploit Gaming Sites and What Can be Done to Stop Them," NYU Stern Center for Business and Human Rights (forthcoming Mar. 2023).

Readings / References

5 core readings (other formats like podcasts fine too):

1. Online extremism and potential countermeasures:
   Charlie Winter et al., "Online Extremism: Research Trends in Internet Activism, Radicalization, and Counter-Strategies," *International Journal of Conflict and Violence*, Vol. 14 (2020) https://www.ijcv.org/index.php/ijcv/article/view/3809
2. Overview of suggested solutions in academia:
   Correa, D., & Sureka, A. Solutions to detect and analyze online radicalization: a survey. *arXiv preprint arXiv:1301.4916 (2013)*. https://arxiv.org/abs/1301.4916
3. Countering Terrorism Online with Artificial Intelligence:
   An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia, United Nations Office of Counter-Terrorism and United Nations Counter-Terrorism Centre (2021), pp. 10-14, 23-34, 43-49. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/countering-terrorism-online-with-ai-uncct-unicri-report-web.pdf
4. Social media's role in the Jan 6th insurrection:
   Case study – Jen Patja Howell, The Lawfare Podcast: A Jan. 6 Committee Staffer on Social Media and the Insurrection (Feb. 8, 2023) https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/countering-terrorism-online-with-ai-uncct-unicri-report-web.pdf
5. Gaming sites and extremists:
   "Gaming the System: How Extremists Exploit Gaming Sites and What Can be Done to Stop Them," NYU Stern Center for Business and Human Rights (forthcoming Mar. 2023).

Readings / References

- Lorand Bodo and Inga Kristina Trauthig, “Emergent Technologies and Extremists: The DWeb as a New Internet Reality?” Global Network on Extremism and Technology (July 2022). https://gnet-research.org/wp-content/uploads/2022/07/GNET-Report-Emergent-Technologies-Extremists-Web.pdf
- Elson, Joel S, Doctor, Austin C and Sam Hunter. The metaverse offers a future full of potential - for terrorists and extremists, too. The Conversation (January 7, 2022). https://theconversation.com/the-metaverse-offers-a-future-full-of-potential-for-terrorists-and-extremists-too-173622

- Center for Countering Digital Hate: https://counterhate.com/
- GIFCT website: https://gifct.org/
- Global Network on Extremism and Technology: https://gnet-research.org/
- ISD Global toolkits: https://www.isdglobal.org/pub-types/toolkits/?fwp_language=english
- Tech Against Terrorism: https://www.techagainstterrorism.org/
- VOX-Pol Network of Excellence (NoE): https://www.voxpol.eu/

Readings / References

[Optional] Additional readings: Online extremism outside of main social media platforms/emerging challenges:

- Lorand Bodo and Inga Kristina Trauthig, “Emergent Technologies and Extremists: The DWeb as a New Internet Reality?” Global Network on Extremism and Technology (July 2022). https://gnet-research.org/wp-content/uploads/2022/07/GNET-Report-Emergent-Technologies-Extremists-Web.pdf
- Elson, Joel S, Doctor, Austin C and Sam Hunter. The metaverse offers a future full of potential - for terrorists and extremists, too. The Conversation (January 7, 2022). https://theconversation.com/the-metaverse-offers-a-future-full-of-potential-for-terrorists-and-extremists-too-173622

Additional resources for further readings:

- Center for Countering Digital Hate: https://counterhate.com/
- GIFCT website: https://gifct.org/
- Global Network on Extremism and Technology: https://gnet-research.org/
- ISD Global toolkits: https://www.isdglobal.org/pub-types/toolkits/?fwp_language=english
- Tech Against Terrorism: https://www.techagainstterrorism.org/
- VOX-Pol Network of Excellence (NoE): https://www.voxpol.eu/