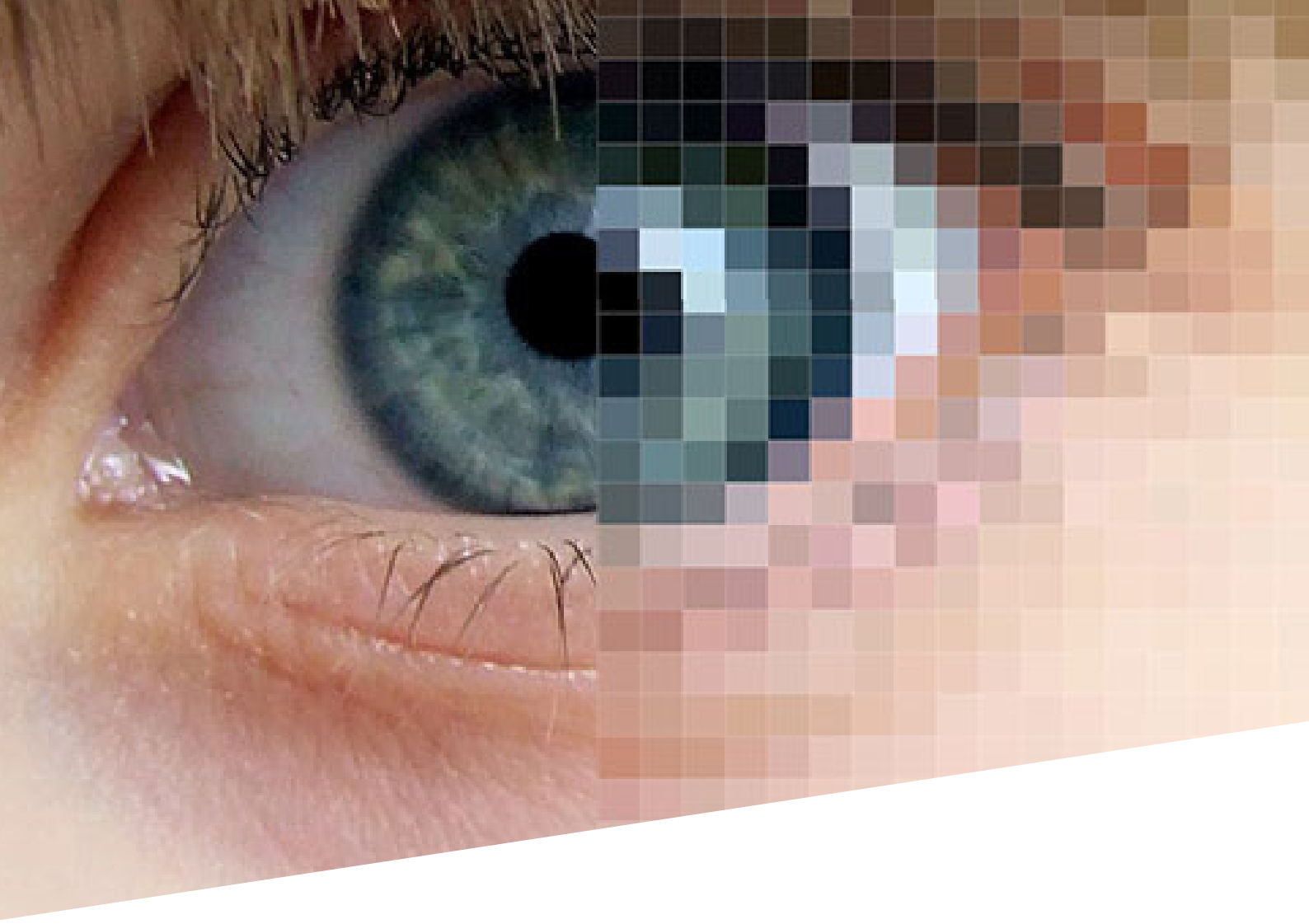

C R T G

Children Affected by the Foreign Fighter Phenomenon: Guidelines on the Prevention of Radicalization on Social Media and the Internet in this Digital Era

2023 VOL. I

/ Cecilia Polizzi

ABOUT CRTG WORKING GROUP

The CRTG Working Group is the world's first organization dedicated to addressing the involvement of children with terrorism and violent extremism. We help understand the nature of child involvement with terrorist and violent extremist actors, support prevention and mitigation efforts.

The CRTG Working Group recognizes that child exploitation in terrorism is an evolutionary outcome of terrorist tactics and strategy and one of the core elements enabling the long-term survival of terrorist organizations, spreading violent ideology, and fueling conflict. We acknowledge that addressing the complex and evolving nature of the terrorist threat, requires our own adaptation and therefore, we are intentionally forward-looking in our understanding of children´s role - as a factor that can exacerbate existing challenges, but also one that can, when effective intervention measures are implemented and sustained, provide new solutions to current threats that we confront and help prevent new ones from materializing.

Through a multi-tiered approach, the CRTG Working Group provides unique insights and cross-cutting analysis into this area, helps shape policies that accommodate both child protection and security concerns through direct, personal advocacy, and works to address context-specific needs, facilitating meaningful and sustainable solutions.

LICENSING AND DISTRIBUTION

Working Group on Children Recruited by Terrorist and Violent Extremist Groups
Web: crtgroup.org
Guidelines
APRIL 2023

This report was written by Cecilia Polizzi,
Founder, President / CEO
CRTG Working Group

C R T G

Contents

Executive Summary

The 2023 Children Affected by the Foreign Fighter Phenomenon (CAFF) Series aims to provide insight and advice for states, professionals, practitioners, and other relevant stakeholders. The CAFF expounds the trajectory of child involvement with the Islamic State of Iraq and the Levant (ISIL) in relation to the foreign fighter phenomenon and the life-cycle of the present scenario, offering solutions across sectors and disciplines and tackling the full range of issues it exerts. It encompasses key themes such as online safety, the Al-Hol crisis, repatriation, reintegration and rehabilitation, and offers four sets of Guidelines.

This line of effort by the CRTG Working Group proposes comprehensive, integrated and multi-faceted approaches to progress towards sustainable and meaningful solutions to the prolonged child protection and security crisis stemming from the issue of foreign fighters. Central to CAFF is ensuring that human rights, the rule of law, and children's rights remain at the forefront throughout the development and implementation of interventions and programs.

These syntheses of accumulated experience and expertise on selected themes provide comprehensive, detailed, and nuanced overviews of their subject matter. The present Guidelines initiate this line of thematic work by the CRTG Working Group in a very important area - the online ecosystem of terrorism and violent extremism. It is the result of CRTG Working Group specialized knowledge and draws from a CRTG Working Group-led technical session with Ms. Hallie Stern, Founder and Director of Mad Mirror Media, and Mr. Ardian Shajkovci, Co-Founder and Director of the American Counterterrorism Targeting and Resilience Institute, concerned with preventing and mitigating harms against children in the digital sphere. Thus, acknowledging how ISIL and other terrorist and violent extremist actors exploit technological innovation, social media, and the Internet to entice, mobilize, recruit and radicalize children and seeking to enable appropriate responses, guaranteeing online safety and a secure online experience for all children and young people.

The CRTG Working Group´s technical session sought to expose the complexities of the online ecosystem of terrorism and violent extremism as related to the targeting of children and respond to the following questions:

1. What are the primary ways in which terrorist groups use the Internet to recruit and radicalize children, and what strategies can be employed to prevent such activity? What is the role of governments, tech companies, civil society, and non-professionals?

2. Is child protection truly possible in the digital environment? If yes, through which strategies and in which manner should prevention and mitigation efforts occur?

The Recommendations are categorized into three distinct sections, specifically designed to cater to the roles and responsibilities of different stakeholders: 1. Tech Guidelines; 2. Policy Guidelines; and 3. Non-Professional Guidelines.

Background

The issue of foreign terrorist fighters (FTFs) has been a priority on the political agenda of a number of states for at least the past five years. Since the inception of the Syrian crisis, thousands of foreign nationals have traveled or attempted to travel in a conflict zone in Syria and Iraq with the intent to join the Islamic State of Iraq and the Levant (ISIL) and other insurgent terrorist groups. Following official estimates, at least 4,640 children, constituting between 9-12% of the group´s total foreign affiliates, were either brought by their parents to the conflict zone or were born to FTF families in the region.[1] To these statistics should also be added the hundreds of other foreign minors who traveled on their own accord because of their exposure and enticement to ISIL´s propaganda campaigns and recruitment strategies online. In recent years, social media and the Internet have expedited the dissemination of information, reduced costs, and provided increasing opportunities for communication, engagement and outreach across national boundaries, cultures, and languages. Terrorist and violent extremist groups have leveraged these new mechanisms and platforms to ensure a continuous flow of supporters and sympathizers into their movements and incite attacks regardless of chains of command, training, instruction, material assistance, or operational planning. The promotion of violence and extremist rhetoric encouraging violent acts are common trends in terrorism propaganda across Internet-based platforms. However, terrorist propaganda contains significantly more than religious rhetoric or military strategy. Rather, these narratives are part of a process that crystalizes a jihadi subculture designed to appeal to disaffected and/or marginalized individuals and societal groups. The influence of violent extremists´ propaganda, messaging, and recruiting strategies in the digital realm disproportionately impacts children and young people, who not only comprise a large portion of users but also present heightened vulnerabilities. ISIL demonstrates a heavy reliance on the Internet, social media platforms, games and magazines as propagandistic tools, as well as adroitness in manipulating the media to alter domestic and international opinion in the form of psychological operations.[2] Its ability to radicalize, mobilize, influence, or entice minors cannot be underestimated. In fact, ISIL not only produces some of the most technologically advanced propaganda yet but has also proven highly successful in spreading its narratives throughout a variety of diverse platforms and in devising articulated grooming strategies across the digital space.[3] ISIL's propaganda machine is highly sophisticated. At the height of the group´s occupation of territories across Syria and Iraq, through a number of official media producers and the Al-Hayat Media Center, an ISIL-media branch targeting young viewers and generating content in multiple languages, ISIL produced and disseminated multi-media content, including

[1] Cook, Joana and Gina Vale. "From Daesh to 'Diaspora': Tracing the Women and Minors of Islamic State." ICSR, 2018.
[2] Polizzi, Cecilia. "Fourth Generation Warfare: An Analysis of Child Recruitment and Use as a Salafi-Jihadi Doctrine of War." Small Wars Journal, 2022.
[3] Lieberman, Ariel Victoria. "Terrorism, the Internet, and Propaganda: A Deadly Combination." Journal of National Security Law & Policy 9, no. 1 (Year): 95-120.

Hollywood-style documentaries and jihadi-travel shows[4] portraying life under ISIL as glamorous and utopian and its members as heroic and desirable. Reportedly, 2000 foreign citizens per month, including women and children, traveled to Syria and Iraq in 2014. The territorial defeat of the ´caliphate´ did not alter the group´s online strategy. In 2017, ISIL´s media machinery continued to produce as many as 90,000 posts on Twitter, YouTube, Facebook, and many other social media platforms every single day. According to some commentators, following the loss of territory, the group progressively retreated into a "virtual caliphate", a phase during which propaganda assumed increasing relevance. The COVID-19 pandemic also rendered efforts to maintain a foothold in the digital realm more critical as a means of survival.

While states continue to experience a strong set of unprecedented challenges concerning legal, ethical, and practical questions with respect to their obligations and capabilities of handling the child returnee contingent, the use of the Internet for malign purposes has added new layers of complexity to addressing terrorism and violent extremism involving children and youth, and calls for appropriate and coordinated responses. However, due to the vast variety of online platforms, the evolving nature and breadth of exploitative techniques used, the proliferation of online terrorist and violent extremist content remains one of the major policy issues facing counterterrorism authorities and digital communications technology providers.[5]

[4] Al Hayat Media's programming includes a jihadi-type travel show called "Eid Greetings from the Land of Khilafah," filmed in Raqqa, Syria, which features ISIS fighters from Western countries proclaiming how happy they are to be there.; Steve Rose, The ISIS Propaganda War: A Hi-Tech Media Jihad, THE GUARDIAN (Oct. 7, 2014), http://www.theguardian.com/world/2014/oct/07/isis-media-machine-propaganda-war.

[5] Clifford, Bennett. "Moderating Extremism: The State of Online Terrorist Content Removal Policy in the United States." Program on Extremism at George Washington University, December 2021.

I. Tech Guidelines

01. Consider algorithmic pattern changes and seek to moderate data collection on children to prevent the hyper-targeting of violent extremist propaganda and reduce radicalization and recruitment risks.

In the rapidly evolving landscape of social media platforms, algorithmic patterns and data collection practices have become subjects of intense scrutiny and debate. This section sheds light on the impact of algorithmic changes made by major tech giants, such as Facebook and Google, and the implications of data collection within the context of marketing, ad tech, and content moderation. In 2016, Facebook, Google, and other leading platforms modified their algorithms to create personalized echo chambers within users' networks.[6] By leveraging human ranking and specific user interactions, the algorithms were designed to prioritize content that resonated most with individuals. While this approach yielded favorable outcomes for marketing and ad tech purposes, it also opened avenues for malicious exploitation, such as the manipulation of content dissemination by terrorist and violent extremist actors across the ideological spectrum. This highlights the need to reassess the algorithmic patterns deployed by these platforms to mitigate the potential for unintended consequences. Inextricably linked to algorithmic patterns is the collection of vast amounts of user data. The ability to precisely target audiences based on demographics, interests, and even geographical locations has revolutionized the ad tech industry. However, this practice raises ethical concerns, particularly when it comes to data collected from individuals under the age of eighteen. Understanding the implications of data collection on children and the risks posed by algorithmic models can serve violent extremism prevention and mitigation efforts and help ensure the integrity of digital platforms. In this framework, a revisitation of algorithmic patterns, emphasizing diversity of content and reducing risks of fostering echo chambers, and discussions surrounding the scope of data collection on children may support tech companies in navigating these complex challenges and guide towards establishing a balanced approach between user experience, privacy, and children´s and societal well-being.

02. Seek to enhance cross-platform information sharing and collaboration among tech companies in order to address the challenges of identifying and managing digital risks, particularly for those with limited resources.

[6] Eg, R., Demirkol Tønnesen, Ö., & Tennfjord, M. K. (2023). A scoping review of personalized user experiences on social media: The interplay between algorithms and human factors. Computers in Human Behavior Reports, 9, 100253. https://doi.org/10.1016/j.chbr.2022.100253.

The current landscape of online violent extremist content was shaped in large part by decisions made by major social media companies to alter their content removal policies. Terrorist and violent extremist groups reacted to this heightened enforcement in a number of ways, but centered their strategies for survival online on adaptation and migration.[7] Audrey Alexander observed that supporters of extremist groups "demonstrate tremendous agility across multiple platforms" in reacting to major social media companies' increased enforcement of TOS, noting that "some accounts rallied in the face of shutdowns [while] others expressed interest in migrating to online environments that were more hospitable or optimal for extremist users."[8] Despite the investments of major platforms in TOS enforcement, extremist actors seek to maintain footholds on major social media platforms to access global audiences.[9] Yet, they have generally been successful in migrating to other social media platforms, which they can exploit as alternatives when the major services are inaccessible.[10] While using alternative platforms can be disadvantageous in attaining a high rate of audience engagement and is oftentimes subject to service disruptions,[11] one clear advantage is found in the relatively more suitable environments for extremist content that these platforms guarantee. Many smaller providers lack the personnel, resources, and expertise necessary to institute a broad-based terrorist content removal paradigm.[12] A commonly cited example of this type of company is JustPaste.it, a file-sharing site operated by a Polish social media startup. Due to the platform's simple design and accessibility features, including operating with right-to-left alphabets like Arabic, ISIL supporters exploited the platform to host multimedia propaganda releases.[13] In the early days of ISIL social media campaigns on JustPaste.it, the company had one staff member and a minimal budget; it simply could not keep up with the influx of violent extremist content.[14] Following these considerations, cross-platform collaboration and partnership between tech companies of different sizes, such as start-ups and tech giants, may hold great potential in preventing and countering violent extremism online targeting children. This collaborative framework paves the way for joint research and development endeavors, specifically focused on enhancing content moderation technologies, devising effective detection algorithms, bolstering the identification and removal of violent propaganda materials, and fortifying reporting mechanisms. In conjunction with collaboration, the provision of technical assistance and tools emerges as a vital aspect of supporting smaller tech companies. Big tech companies, acting as mentors, can extend technical aid and provide access to tools such as Application Programming Interfaces (APIs) and software development kits (SDKs). These invaluable resources aid in the identification and removal of violent propaganda

---

7 Alexander, "Digital Decay"; Alexander and Braniff, "Marginalizing Violent Extremists Online"; Clifford, Bennett. 2020. "Migration Moments: Extremist Adoption of Text-Based Instant Messaging Applications." Global Network on Extremism and Technology. November 2020. Accessed [May 1, 2023]. Available at: https://gnet-research.org/wp-content/uploads/2020/11/GNET-Report-Migration-Moments-Extremist-Adoption-of-Text%E2%80%91Based-Instant-Messaging-Applications_V2.pdf.

8 Alexander, "Digital Decay."

9 Clifford, Bennett, and Helen Powell. 2019. "De-Platforming and the Online Extremist's Dilemma." Lawfare. June 6, 2019. Accessed [insert date accessed]. Available at: https://www.lawfareblog.com/de-platforming-and-online-extremists-dilemma.

10 Ibid.

11 Clifford and Powell, "De-Platforming and the Online Extremist's Dilemma".

12 Tech Against Terrorism, "The Online Regulation Series".

13 Ibid.

14 Ibid.

materials, enabling small tech companies to integrate robust content moderation and filtering systems into their platforms. The seamless incorporation of these technologies ensures a more secure and responsible digital environment. To further equip small tech companies with the tools and insights necessary to enable proactive measures in detecting and removing violent propaganda, training programs and capacity-building initiatives may also be considered.

03. Strengthening collaboration between tech companies and law enforcement: establishing clear protocols to safeguard privacy, protect public interests, and combat harmful activities against children in the online realm.

In today's digital landscape, the regulation of online discourse, particularly when it veers into the realm of violent extremism and harm against children, presents a multitude of challenges. The importance of clear definitions and frameworks for identifying and addressing hateful speech and harmful content targeting children, in addition to the need for metrics to measure impacts, is evident. While the limitations faced by tech companies in sharing private data and difficulties in accessing social media-related information are acknowledged, within the context of online regulation, the establishment of transparent protocols can be an effective way to safeguard privacy, protect public interests, and prevent and mitigate harmful activities against children. These protocols should encompass comprehensive guidelines that outline the appropriate procedures and methodologies, including the identification and removal of abusive content, the reporting and escalation mechanisms for suspicious behavior, and the implementation of proactive measures to prevent the dissemination of such content. These protocols should adhere to legal and ethical standards, respecting privacy rights while still enabling the necessary collaboration between tech companies and law enforcement agencies. Ensuring a balance between data accessibility and privacy protection is paramount, necessitating a careful examination of constitutional and legislative limitations and the formulation of protocols that align with relevant norms. By engaging in a multifaceted dialogue with a range of stakeholders, including policymakers, child protection entities, and legal experts, tech companies can ensure that the protocols address diverse perspectives and concerns, fostering a collective effort to combat harmful activities against children in the online ecosystem. In terms of implementation, adequate resource allocation may support the provision of training programs focusing on equipping staff with the necessary knowledge and skills to effectively implement the protocols, including techniques for content moderation, identification of potential risks, and handling sensitive information, therefore building capacity to address harmful activities against children on their platforms and helping create a safer online environment.

II. Policy Guidelines

04. Consider mainstreaming technical perspectives and data science into policies, laws, and initiatives aimed at preventing and mitigating online harm for children.

A viable strategy to combat the dissemination of terrorist content online involves the proactive removal of individual posts or websites by technology companies or external entities. This approach is implemented through various means, including government entities issuing requests for content removal, technology companies adopting self-regulatory measures to eradicate such content, leveraging artificial intelligence techniques such as "upload filters," and engaging individual hackers or civil society-led initiatives for content takedown. While the removal and filtering of terrorist and violent extremist content does impede the dissemination of terrorist propaganda, it does not completely eradicate it. This challenge can be aptly described using the metaphor of "Whack-A-Mole," drawing upon the analogy of the classic amusement park game where a mallet is used to strike furry rodents as they randomly emerge from various holes on a board.[15] When terrorist content is removed from one website, it swiftly reappears on a different channel or multiple channels. The online landscape is in a perpetual state of flux, presenting those responsible for content takedown and filtering with an incessant and exponentially expanding stream of identical materials surfacing across multiple platforms. A narrative-driven approach alone, in addition, may neglect the intricate technical and algorithmic elements that feed the AdTech economy and the digital advertising ecosystem and inadvertently support the dissemination of harmful content to children. The data collected from social media users to create detailed user profiles, including demographic information, interests, and online behaviors is exploited by terrorist and violent extremist actors seeking to identify and engage children at risk. Understanding disinformation, misinformation, and propagation as cybersecurity and information security issues will assist not only in avoiding potential conflicts with constitutional principles, such as freedom of speech, but also in formulating informed policies that align with the complexities of the digital ecosystem and its technological infrastructure and foster a safer online environment and experience. Machine learning, data science, and network analysis specialists may help shed light on data collection and the ways in which it is used for malignant intents to hypertarget violent content, and mainstream this knowledge into regulatory frameworks, policy development, and implementation.

---

[15] Peritz, Aki, 'What Whac-A Mole Can Teach Us About How to Fight Terrorism,' *Foreign Policy*, 12 August 2015. Available at: https://foreignpolicy.com/2015/08/12/what-whac-a-mole-can-teach-us-about-how-to-fight- terrorism/.

05. Consider establishing a community-led panel of modifiers to discuss and provide input on trust and safety issues and help enforce regulation aimed at mitigating online harms against children in the digital environment while effectively balancing the relationship between governments, tech companies, and the collective interest.

The ubiquitous principles of libertarianism and capitalism, which constitute the foundations of the free market paradigm, wield a substantial influence over the regulatory capacity of governments concerning content control on privately owned platforms that profit from algorithm-based business models. This influence assumes particular significance when contemplating the potential risks inflicted upon children who might become susceptible to online radicalization or recruitment by terrorist and violent extremist actors. Libertarianism, as an ideology, champions minimal governmental intervention in market affairs, emphasizing individual freedom and restrained regulation. It espouses the notion that private entities should possess considerable latitude in their operations, with minimal encroachment from governing bodies. Consequently, this perspective posits that governments ought to abstain from imposing content-related restrictions, granting them the autonomy to fashion their own policies. Capitalism further buttresses the ideology of the free market by accentuating the pursuit of profit and fostering competition among private entities. Within the domain of privately owned platforms that derive profit through algorithmic mechanisms, the primary objective revolves around maximizing user engagement and generating revenue. Algorithms, engineered to optimize user experiences and bolster platform usage, frequently accord precedence to content that elicits heightened levels of engagement. This predisposition can inadvertently lead to the amplification of sensational or provocative material, which may encompass harmful or extremist content. Within this milieu, the profit-oriented nature of capitalism and the dependence on algorithms engender obstacles for governments endeavoring to regulate injurious content that targets children. Governments commonly harbor a vested interest in safeguarding citizens, including children, from exposure to harmful materials and thwarting the dissemination of radical ideologies. However, the dynamics of the free market, impelled by libertarian and capitalist principles, circumscribe the government's capacity to impose regulations that exert direct influence over privately held platforms. The economic viability of these platforms hinges heavily on user-generated content and engagement, and stringent regulations may impede their growth prospects or erode their competitive advantage. Furthermore, the expansive scale and global reach of these platforms engender intricate jurisdictional complexities, rendering it arduous for individual governments to uniformly enforce regulations across borders. This perspective raises a crucial question: What does the platform itself desire, and how does it serve broader societal interests? Engaging in this line of inquiry leads to a paradoxical situation wherein delineating the responsibilities of various stakeholders becomes challenging. A potential solution involves establishing a citizens advisory board or an independent oversight panel that fosters substantive discussions and input on trust and safety issues. While abstaining from direct voting power, these entities could voice concerns or preferences and contribute to the

definition of standards within the tech platform. It is important to acknowledge that this perspective may exhibit certain limitations, warranting further scrutiny. Nonetheless, the establishment of third-party entities, distinct from both platform interests and governmental influence, with a primary focus on representing the general community perspective, could offer an intriguing avenue for mitigating potential harm inflicted on children in the digital realm.

06. Conduct comprehensive examinations of violent extremist ecosystems in the digital space for evidence-based policies and child-centric intervention measures.

The online ecosystem provides terrorist and violent extremist actors with fertile ground to disseminate their ideologies, recruit, and exploit children. Through the Internet's global reach and the ease of online communication, terrorist and violent extremist actors amplify their messages and engage with children on a scale previously unimaginable. Over time, the online ecosystem has evolved, adapting to technological advancements and changes in user behavior. Terrorist and violent extremist actors have become increasingly sophisticated in their use of the Internet and social media platforms, employing various tactics such as targeted messaging, online forums, encrypted messaging apps, and video sharing platforms to disseminate violent ideologies.[16] This evolution has posed significant challenges to traditional counter-terrorism efforts, necessitating a holistic understanding of the online landscape. Despite the increasing focus on violent extremism in the digital sphere, there remain fundamental gaps in understanding its characteristics, impact, scope and reach, which limit the identification of appropriate policy responses. In addressing a continuously evolving scenario, a comprehensive examination of the digital spaces, including key actors, networks, influential communities, communication channels, and interactions, will allow for a nuanced understanding of the online ecosystem, its vulnerabilities, and the dynamics of online radicalization and recruitment as they relate to children. The mapping process, involves collecting and analyzing vast amounts of data, including user profiles, online discussions, multimedia content, and network connections. Advanced data analytics techniques, such as machine learning and natural language processing, can be employed to identify patterns, trends, and indicators of child radicalization and recruitment. This analytical approach enables the detection of potentially harmful content, the identification of high-risk individuals, and serves as a foundation for evidence-based policymaking and the development of targeted intervention measures.

Best Practice

Ensuring youth and children's safety online and offline from extremist and terrorist group targeting is a critical aspect of a project carried out by the American Counterterrorism Targeting and Resilience Institute (ACTRI). The

[16] Marone, Francesco, and Paolo Magri, eds. Digital Jihad, Online Communication and Violent Extremism. ISPI, November 2019.

ACTRI's Social Media Monitoring Project (SMMP) is an ongoing initiative that focuses on proactive, daily monitoring of extremist and terrorist content and activities taking place, particularly online. It involves a thorough analysis of extremist and terrorist-affiliated groups, conspiracy theories, and the spread of mis-and disinformation on platforms like Telegram and other mainstream and alternative social messaging platforms. ACTRI and its partner Storyzy have developed AI-led and other automated applications that enable the identification, storage, and maintenance of extensive datasets across different social media platforms that promote harmful extremist content and mis-and-disinformation. The primary objective of this initiative is to trace the developments, trends, and changes in such platforms in terms of extremist and terrorist content and activities and mis-and-disinformation. New groups and activities are continuously updated and incorporated into the monitoring process to facilitate effective tracking of extremist content and mis-and-disinformation online, with a particular focus on closely observing the impact of such content on local communities in the United States and beyond.

07. Consider implementing a multifaceted, multi-sectoral approach to ensure that children who have been radicalized online are provided with appropriate support and intervention measures.

Inter-agency cooperation is the most challenging area to address when promoting multi-faceted, multi-sectoral strategies. Although such cooperation is difficult in any thematic area, it is particularly problematic in the case of preventing and countering violent extremism due to a legacy of securitization resulting in an absence of trust, credibility, and legitimacy.[17] The lack of existing mechanisms for coordination and the technical skills required to conduct effective partnerships and engagements may also hinder the success of inter-agency cooperation approaches.[18] However, while complex, partnerships between relevant governments and non-governmental actors may bring a wide array of benefits in both the short and long term. The development and effective implementation of an inter-agency cooperation framework may enable information sharing, support increased understanding and awareness of emerging trends in the exploitation of the online ecosystem by terrorist and violent extremist actors, serve the identification of existing gaps, and enable timely interventions. Additionally, by leveraging the strengths and capabilities of different sectors, inter-agency collaboration allows for a holistic assessment of the needs of children and the delivery of a more robust, comprehensive, and tailored response.

Best Practice

[17] Organization for Security and Co-operation in Europe. "Preventing and Countering the Use of the Internet for Terrorist Purposes." Accessed May 24, 2023. https://www.osce.org/files/f/documents/a/7/444340_0.pdf.

[18] Ibid.; The organization of regular meetings, joint training sessions, the development of shared protocols and guidelines as well as adequate resource allocation may assist in overcoming obstacles to successful interagency collaboration.

The Danish Government has developed a model (the Aarhus model)[19] for preventing and countering violent extremism and radicalization, with a particular emphasis on preventing individuals from traveling to Syria and Iraq and the returnee contingent. The Aarhus model is based on the development of new initiatives and methods through multi-agency collaboration and coordination among diverse social service providers, including the educational system, the health care system, the police, and the intelligence and security services, which has evolved over a decade. Local practitioners receive guidelines from the state, and after testing them in actual conditions, they provide feedback that is used to refine the guidelines further. Alternatively, local practitioners may develop concrete initiatives or methods and put them into practice, after which they are adopted at the state level and copied in other local contexts. The approach and its concrete methods are therefore continuously being developed both top-down and bottom-up, a process that allows them to be adapted to changes in an evolving environment. Many of the initiatives developed revolve around helping people self-help through, for example, mentoring, counseling, and exit programmes. Crucial to this approach is the fact that participation is voluntary and numerous cost-free offers of assistance are made available.

08. Enhance the knowledge and awareness of children and young individuals regarding the potential risks associated with the online environment and their interaction on social media platforms through the implementation of focused public awareness campaigns.[20]

Neuroscience, psychosocial science and indeed all disciplines investigating brain function further inform regarding child vulnerabilities and developmental needs.[21] It is recognized that children and young people have rudimentary skills of factual cognition or mental processes such as learning, using and understanding language, memory, thinking and perception, but also moral cognition and conative ability, regulating impulse control.[22] Children´s evolving cognitive capacities may result in an enhanced disregard for risks and an inclination towards engaging in risk-taking behavior. Compounded by their limited understanding of the online environment, children may unknowingly expose themselves to various dangers, including violent propaganda campaigns[23] and harmful content, grooming, and sustained radicalization and recruitment strategies enacted by terrorist and violent extremist actors. The implementation of tailored awareness-raising campaigns for children and youth assumes a significant role. These campaigns may equip young individuals with the necessary skills to identify age-inappropriate or harmful content, withstand radicalization, and resist triggers or encouragements to engage in unsafe action or associate with terrorist and violent extremist actors. By empowering children and youth with the

---

19 Folketinget. "Bilag 248 - Samling 2015-16 - Alm.del - Reu - Bilag 248 Offentligt." Accessed May 24, 2023. https://www.ft.dk/samling/20151/almdel/reu/bilag/248/1617692.pdf.

20 This recommendation may be applicable to both governments and civil society organizations.

21 Cecilia Polizzi. "Inside Salafi-jihadism: the Rationale Driving the Recruitment and Use of Children" YouTube, May 1, 2023, https://www.youtube.com/watch?v=y7H8dsUZ1lo.

22 Ibid.

23 Speckhard, Dr. Anne; Shajkovci, Ardian; Wooster, Claire; and Izadi, Neima. "Engaging English Speaking Facebook Users in an Anti-ISIS Awareness Campaign." Journal of Strategic Security 11, no. 3 (2018) : 52-78. DOI: https://doi.org/10.5038/1944-0472.11.3.1679 Available at: https://digitalcommons.usf.edu/jss/vol11/iss3/4.

ability to navigate the online world more safely and make informed decisions, these awareness-raising campaigns can serve as a vital preventive measure against the potential risks and consequences associated with their online interactions.

III. Non-Professional Guidelines

09. Incorporate digital resilience and media literacy education into the scholastic curriculum to empower children to responsibly navigate the online landscape.

One approach to prevent online terrorism is by fostering digital resilience and media literacy skills.[24] This strategy is built on two assumptions. Firstly, by developing digital resilience and media literacy, individuals can effectively address grievances that may lead to radicalization based on misinformation or disinformation. Secondly, individuals who can critically evaluate information and assess the credibility of sources are less likely to be influenced by terrorist propaganda.[25] The formal education sector plays a vital role in equipping children with the ability to discern various tactics employed by terrorist groups in disseminating their messages. Educators devote their efforts to enhancing students' inclinations, interests, and educational requirements, drawing from their own wealth of experiences. They serve as exemplars for their students, striving to shield them from various forms of deleterious behaviors. In line with their responsibility to safeguard students from detrimental influences, teachers may also crucially contribute to shielding them from the ramifications associated with extremist ideologies. This is of paramount importance as radicalization and extremist narratives have the potential to yield destructive outcomes for children, families, communities, and society.[26] By integrating digital resilience and media literacy education into the scholastic curriculum, teachers can empower students to navigate the online landscape responsibly. Some educators may not consider themselves qualified to engage in prevention unless they possess a certain level of expertise.[27] While the affordability of specialized training for educators in line with human rights, the rights of children, and do-no-harm principle[28] is to be prioritized, activities such as mentoring and counseling, pedagogical support, active or strategic listening, communication skills, and critical thinking are a few examples of

[24] UNESCO offers tools, such as a framework and assessment tools, to monitor the global progress of digital literacy skills, aligning with Sustainable Development Goal 4 on Quality Education. This framework provides guidelines on various digital competencies, including information and data literacy (e.g., browsing, searching, and evaluating online data), communication and collaboration (e.g., interacting and sharing through digital technologies), digital content creation (e.g., developing digital content and understanding copyrights and licensing), safety (e.g., protecting devices, personal data, and well-being), and problem-solving (e.g., identifying needs and digital/technical solutions). It is important to note that the digital literacy framework has a broader scope beyond terrorism prevention online and is intended for integration into school systems worldwide.; Law, Nancy, David Woo, Jimmy de la Torre, and Gary Wong. "A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2; Information Paper No. 51." June 2018. UIS/2018/ICT/IP/51; UNESCO.

[25] Zeiger, Sara and Joseph Gyte. "Chapter 12: Prevention of Radicalization on Social Media and the Internet." In Handbook of Terrorism Prevention and Preparedness, 358.

[26] Koçak, Emrah. "A Guide for Empowering Teachers Against Extremism." SAVE, Erasmus+ project. 2017-1-TR01-KA201-046311.

[27] Doda, Alush and Marina Mclellan. "Promoting a Multi-Stakeholder Approach to Preventing and Countering Violent Extremism and Radicalization that Lead to Terrorism: Summary report of roundtable discussions on the National Strategy for Countering Violent Extremism in the Republic of North Macedonia." OSCE.

[28] UNICEF. "Ethical Guidelines"Accessed May, 1 2023. URL. https://www.unicef.org/serbia/en/ethical-guidelines#:~:text=Guidelines%20for%20interviewing%20children,and%20grief%20from%20traumatic%20events..

educators´ abilities and capacity to offer support. Critical thinking skills are particularly valuable in this framework as they serve as an enabler of students´ capacity to question the accuracy and credibility of information they encounter, develop and strengthen resilience.

10. Address the risks of radicalization in holistic manner accounting for both the offline and online domains.

The Internet and social media have provided enhanced opportunities for terrorist and violent extremist actors across the ideological spectrum. Digital technologies have not only facilitated the dissemination of extremist propaganda but have also fundamentally altered the mechanisms of recruitment, mobilization and active participation. In Western societies, the vast majority of cases involving jihadist radicalization cannot be dissociated from their online components, which often include sporadic consumption of extremist propaganda.[29] As active Internet users, children and adolescents are at particular risk. While addressing the online ecosystem of violent extremism targeting children is critical and requires concerted efforts and targeted initiatives, to adequately prevent and mitigate risks of child radicalization and/or involvement with terrorism and violent extremism, it is equally crucial to focus on the offline elements that contribute to child vulnerability and susceptibility to extremist ideologies, therefore accounting for both the online and offline spheres in a balanced manner. Children and young people oftentimes face a plethora of underlying issues such as social exclusion, trauma, poverty, and discrimination, which constitute, among other factors, the root causes of child vulnerability to violent extremism in the digital environment. Understanding the interconnectedness between the drivers of violent extremism and the ways in which these manifest in children´s behaviors and approaches online is essential to formulating a cohesive approach to prevent and mitigate the risks of child radicalization, the potential for child involvement in violent acts or association with terrorist and violent extremist groups.

11. Build self-awareness and foster a greater understanding of the risks associated with online radicalization and recruitment among children.

In today's digital age, it is essential for parents and caregivers to be vigilant and proactive in protecting their children from the risks of online radicalization and recruitment by terrorist and violent extremist actors. Families are oftentimes insufficiently equipped with knowledge or tools to understand and address violent extremism and radicalization.[30] In some instances, family members may be able to identify early signs of radicalization to violent extremism. However, early detection may be challenged by the fast evolution of radicalization processes or by

[29] Marone, Francesco, and Paolo Magri, eds. Digital Jihad, Online Communication and Violent Extremism. ISPI, November 2019.
[30] CRTG Working Group, Right Wing Extremism: Children´s Perspectives, Policy and Practice (2022).

existing analogies between early indicators of radicalization and other challenges, including trauma, depression, addiction, discrimination or marginalization, among others. Families play an important role in safeguarding children at risk. It is therefore critical that the tactics and strategies employed by terrorist and violent extremist groups targeting children in the digital environment, as well as the nature of radicalization processes are adequately understood. Consistent educational programs and authoritative and reputable sources,[31] informing about terrorism and violent extremism, radicalization, child vulnerability, online safety, social media use and dialogue may support increased awareness, intervention and responses.[32] Parents or caregivers may also play a constructive role in the prevention and mitigation of radicalization risks through communication. By creating an environment where children feel comfortable discussing their online activities and experiences, parents or caregivers may establish a strong foundation for promoting digital literacy, critical thinking, identifying potential vulnerabilities, and addressing risks. This involves encouraging open communication and dialogue without moralizing or judgment, ensuring that children understand they can approach their parents with any concerns or questions. The role of parents and caregivers is complementary and supportive of the one played by governments, tech companies, and civil society. While these stakeholders have distinct responsibilities and contributions, a comprehensive approach to safeguarding children from the influence of extremist ideologies is crucial.

[31] UNESCO, Preventing Violent Extremism through Education: A Guide for Policy-Makers (2017).
[32] Ibid.

C R T G