

What Parents Should Know to Protect their Kids and Youth Online

Online Extremists Recruiting Teens

Abstract

Extremist online recruitment of teenagers is a growing, global security threat where violent groups use digital platforms to groom, radicalize, and mobilize young people, with some cases involving children as young as 13 plotting attacks. Extremist groups increasingly target minors through social media, encrypted messaging apps, and popular gaming platforms.

Compiled: 18 January 2026

By: Glen Hutton

For the



Contents

Summary – Online Youth Radicalization Groups	4
Current High-Risk Online Networks	4
"The Com" (Community Networks):	4
764 (Hazard 44 / CVLT):	4
Terrorgram Collective:	4
Tactics and Recruitment	4
Platform Exploitation:	4
Gender-Specific Targeting:	4
Algorithm-Driven Radicalization:	4
Warning Signs for Guardians	5
Common behavioral changes associated with online radicalization include:	5
Resources and Reporting	5
Youth Radicalisation: A New Frontier in Terrorism and Security	6
Radicalisation of Young People	6
The evolving threat of youth radicalisation	6
The digital age and radicalisation	6
Fragmentation of extremist ideologies	6
The role of artificial intelligence and virtual reality	7
Radicalisation in conflict zones and fragile states	7
Why counter-radicalisation efforts have struggled	7
The need for a whole-of-society approach	8
Violent Extremist Groups Online Radicalization of Youth	9
Overview	9
Key issues	9
The online environment	10
Five-Eyes actions to understand the radicalisation of minors	10
Raising awareness of the radicalisation of minors	11
Enabling early intervention	11
Case studies	11
Australia – case study 1	11

Australia – case study 2	12
Canada.....	12
New Zealand – case study 1	13
New Zealand – case study 2	14
United Kingdom – case study 1.....	14
United Kingdom – case study 2.....	15
United States	16
Conclusion.....	16
Further resources	16
Canada.....	16

SUMMARY – ONLINE YOUTH RADICALIZATION GROUPS

Online youth radicalization in 2026 is characterized by the emergence of decentralized "com" (community) networks that blend violent extremism with other forms of online harm.

CURRENT HIGH-RISK ONLINE NETWORKS

"THE COM" (COMMUNITY NETWORKS):

- A primary threat identified by the National Crime Agency (NCA) and [RCMP](#) in late 2025 and early 2026. These networks target children as young as eight, using platforms like Discord and Telegram to groom youth through a "salad bar" of ideologies.

764 (HAZARD 44 / CVLT):

- Officially listed by Canada as a terrorist entity in December 2025, 764 is a transnational ideologically motivated violent extremist (IMVE) network that recruits minors through gaming and social media.

TERRORGRAM COLLECTIVE:

- An extremist network operating on Telegram that facilitates the distribution of manuals for real-world violence and incites attacks through "accelerationist" propaganda.

TACTICS AND RECRUITMENT

PLATFORM EXPLOITATION:

Recruiters have shifted from open forums to encrypted messaging apps and gaming platforms, where they create "echo chambers" that normalize radical views.

GENDER-SPECIFIC TARGETING:

- Boys: Targeted with "masculine crisis" narratives and influencers who promote harmful views under the guise of self-improvement.
- Girls: Recruited through colorful social media content featuring animals or romanticized imagery that gradually introduces extremist religious or family-role ideologies.

ALGORITHM-DRIVEN RADICALIZATION:

- Short-form video platforms (e.g., TikTok) use algorithms that can channel vulnerable youth into emotionally charged, radicalized content within hours.

WARNING SIGNS FOR GUARDIANS

COMMON BEHAVIORAL CHANGES ASSOCIATED WITH ONLINE RADICALIZATION INCLUDE:

- Becoming increasingly secretive about online interactions or using multiple encrypted apps.
- Expressing sudden, intolerant views or using "us vs. them" language.
- Justifying the use of violence to solve social or political grievances.

RESOURCES AND REPORTING

- ACT Early (UK): A [safeguarding website](#) for families to report concerns and get specialist support.
- Community Resilience Fund (Canada): Supports projects like the [Students Commission of Canada](#) to help youth navigate online grievances non-violently.
- Tech Against Terrorism: A UN-supported initiative that works with tech companies to [identify and remove terrorist content](#).

YOUTH RADICALISATION: A NEW FRONTIER IN TERRORISM AND SECURITY

Published on: March 20, 2025

The recruitment and indoctrination of youth by extremist groups are evolving rapidly, and traditional counter-extremism have struggled to keep pace, writes Cecilia Polizzi.

- <https://www.visionofhumanity.org/youth-radicalisation-a-new-frontier-in-terrorism-and-security/#:~:text=The%20digital%20age%20and%20radicalisation,sense%20of%20belonging%20and%20purpose.>

RADICALISATION OF YOUNG PEOPLE

- Radicalisation among young people has become an escalating concern in the global security landscape.
- The recruitment and indoctrination of youth by extremist groups are evolving rapidly, fuelled by technological advancements, ideological fragmentation, and socio-political instability. Traditional counter-extremism strategies have struggled to keep pace with these changes, making youth radicalisation a critical challenge that demands urgent international attention.

THE EVOLVING THREAT OF YOUTH RADICALISATION

THE DIGITAL AGE AND RADICALISATION

- The rise of the internet and social media has transformed the way extremist groups recruit and influence young people. No longer reliant on physical networks or face-to-face indoctrination, groups now operate within digital spaces, reaching potential recruits through online forums, encrypted messaging apps, and gaming platforms. The ease of access to extremist content accelerates the radicalisation process, reducing the time it takes for individuals to shift from passive consumers of propaganda to active participants in violent extremism.
- Algorithms on social media platforms also play a role in reinforcing radical ideologies. Young users engaging with extremist content are frequently exposed to more of the same, creating echo chambers where radical views are normalised. Extremist groups exploit these digital environments by crafting engaging narratives that resonate with disillusioned youth, offering them a sense of belonging and purpose.

FRAGMENTATION OF EXTREMIST IDEOLOGIES

- Traditional terrorist ideologies, such as Salafi-jihadism and white supremacism, remain significant threats, but the extremist landscape is becoming increasingly fragmented. Young radicals are now influenced by a mix of ideologies, conspiracy theories, and hybrid extremist movements that do not fit within conventional classifications. This ideological fluidity makes it more challenging to identify, monitor, and counter radicalisation efforts effectively.
- Emerging extremist movements blend elements from different ideologies, making them adaptable and attractive to a wider range of individuals. For instance, online extremist

spaces often merge far-right nationalism with anti-government sentiments, religious extremism, and anti-globalist conspiracies. This cross-pollination of radical ideologies complicates counterterrorism efforts, as it creates new and unpredictable forms of extremism.

THE ROLE OF ARTIFICIAL INTELLIGENCE AND VIRTUAL REALITY

- Extremist groups are increasingly leveraging artificial intelligence (AI), virtual reality (VR), and the metaverse to enhance their recruitment strategies. AI-generated content, including deepfake videos and automated radicalisation chatbots, allows extremists to create highly convincing propaganda tailored to specific demographics.
- The use of VR for recruitment and training is also a growing concern. Extremist groups can create immersive training simulations, allowing recruits to practice combat scenarios, bomb-making, and tactical planning within virtual environments. As VR technology becomes more accessible, its potential for extremist indoctrination and training will only increase.

RADICALISATION IN CONFLICT ZONES AND FRAGILE STATES

- In regions affected by conflict, weak governance, and socio-economic instability, youth radicalisation is particularly acute. Groups such as ISIS and Al-Qaeda have long focused on indoctrinating young people in these areas, capitalising on the absence of strong institutions and social safety nets. Without effective intervention, generations of young people exposed to extremist ideologies in these fragile states could perpetuate cycles of violence for decades to come.
- Conflict zones provide extremists with the opportunity to recruit child soldiers and expose young populations to systematic radicalisation. The combination of economic hardship, lack of education, and exposure to violence makes young individuals more susceptible to extremist narratives that promise security, purpose, and empowerment.
- The psychological manipulation of youth
- Extremist groups utilise psychological tactics to manipulate young minds. They exploit vulnerabilities such as social isolation, economic hardship, and personal grievances to lure individuals into their ranks. Many radicalised youths exhibit a deep sense of disenfranchisement, feeling alienated from mainstream society and looking for a cause to belong to.
- Radicalisation often follows a pattern: exposure to extremist narratives, reinforcement through online engagement, and eventual mobilisation into active participation. By the time a young person has fully embraced extremist ideology, they may be willing to engage in acts of violence or provide logistical support to terrorist networks.

WHY COUNTER-RADICALISATION EFFORTS HAVE STRUGGLED

- Despite increased awareness, counter-radicalisation strategies have struggled to keep up with the evolving nature of youth extremism. Law enforcement agencies often face legal and ethical barriers when monitoring minors, while education systems lack the necessary tools to identify and address early signs of radicalisation.

- Moreover, counter-extremism policies are often reactive rather than preventive. Governments and security agencies tend to focus on dismantling terrorist networks after radicalisation has already taken place rather than investing in long-term strategies to prevent it from occurring in the first place.

THE NEED FOR A WHOLE-OF-SOCIETY APPROACH

- To effectively combat youth radicalisation, a comprehensive and multi-layered approach is needed. Key elements of this strategy should include:
- Enhanced digital literacy and counter-narratives: Educating young people on the dangers of online radicalisation and equipping them with critical thinking skills to recognise extremist propaganda.
- Strengthening community-based interventions: Local communities play a crucial role in preventing radicalisation. Programmes that foster social cohesion, mentorship, and youth engagement can provide alternative pathways for at-risk individuals.
- Increased parental and educator awareness: Teachers and parents must be equipped to identify early warning signs of radicalisation and intervene appropriately.
- Collaboration with technology companies: Social media platforms and gaming companies must implement stronger policies to detect and remove extremist content while preventing algorithmic radicalisation.
- Investment in psychological support services: Many radicalised youths suffer from mental health issues, trauma, or personal crises. Providing access to counselling and support networks can help mitigate their susceptibility to extremist ideologies.
- As extremist groups adapt to new technologies and shifting ideological landscapes, counter-radicalisation efforts must evolve. A proactive approach that integrates education, digital literacy, psychological support, and community engagement is essential to prevent the next generation of extremists being shaped by online networks, AI-driven propaganda, and global conflicts.

VIOLENT EXTREMIST GROUPS ONLINE RADICALIZATION OF YOUTH

- <https://rcmp.ca/en/corporate-information/publications-and-manuals/five-eyes-insights-young-people-and-violent-extremism-call-collective-action>

OVERVIEW

Violent extremist groups have often been engaged in activities involving the radicalisation of young people (those under 25 years) towards violent extremism. Regardless of their beliefs, young people may become particularly vulnerable to radicalisation and recruitment by violent extremist and terrorist groups.

During the height of the Islamic State of Iraq and the Levant's (ISIL) caliphate, agencies saw many young people and minors (those under 18 years) seeking to join ISIL, or undertake actions inspired by ISIL in their home nations.

- As our threat environments have diversified, security and law enforcement agencies from the Five-Eyes nations of Australia, Canada, New Zealand, the United Kingdom and the United States are collectively seeing minors of varying ideological affiliations in our investigations. In some cases, this has included minors mobilising or planning to mobilise to violence in support of their radicalised ideologies.
- Minors can often do what adults can – create and distribute violent extremist content, lead violent extremist groups, recruit and radicalise others to their extremist cause, and even undertake attacks. A minor can have significant influence within extremist contexts, including undertaking or supporting others to conduct violent extremist acts.
- While the proportion of young people and minors within our respective counter-terrorism cohorts fluctuates over time, our nations have seen a rising prominence of young people and minors in counter-terrorism cases over the last few years. Many of those who are investigated as minors are also investigated into adulthood due to their violent extremist ideology.

KEY ISSUES

- Investigating minors involved in violent extremism presents multiple issues for Five-Eyes agencies. These issues are highlighted below and expanded on in the case studies.
- Minors are "digital natives" – they have grown up online and are technologically savvy. Minors often use multiple platforms and applications for different purposes – some of these platforms, but not all, are of security concern.
- The online environment allows minors to interact with adults and other minors, allowing them to view and distribute violent extremist content which further radicalises themselves and others. Online environments, particularly encrypted ones, provide a large degree of anonymity, complicating efforts to identify individuals radicalised to violence.
- Engaging with minors is more complex than engaging with adults. The unique characteristics of adolescent development require agencies to factor in additional considerations when dealing with minors. Determining intent can be harder for minors than adults, especially for minors who spend a lot of time online.

- A renewed whole-of-society approach is required to address the issue of minors radicalising to violent extremism. This is not something governments or communities can address in isolation. Mental health, community initiatives, social services, and education interventions can help to counter radicalisation before security and policing responses are required.
- The ways in which vulnerability factors (not limited to mental health or neurodiversity characteristics) impact minors' radicalisation to violent extremism is challenging. Five-Eyes agencies are informed by the latest research on these issues.

THE ONLINE ENVIRONMENT

- The online environment provides extensive opportunities for extremists. Through its global reach, extremists can contact individuals around the world. Violent extremist individuals and groups share material which individuals often consume as part of their radicalisation process. This availability makes the spread of grievances and narratives which promote violence a process which can take place entirely online. Individuals continue to be radicalised online and in person – for many individuals, it is a combination of both. Violent extremist content is more accessible, more digestible and more impactful than ever before.
- Over the last 3 decades, extremists (including violent extremists) have adopted the internet as a vector for their activities. More recently, the development of online content and environments has facilitated the entry of minors and young people into violent extremist pathways. This is concerning, as minors are particularly vulnerable to online radicalisation. Online environments provide an avenue for first approaches to minors, including through seemingly innocuous social media and gaming platforms, such as Discord, Instagram, Roblox and TikTok. In these platforms, violent extremism is made more accessible, as violent extremist content can be created within the platforms themselves.
- Minors are increasingly normalising violent behaviour in online groups, including joking about carrying out terrorist attacks and creating violent extremist content, which further complicates the role of counter-terrorism agencies in seeking to identify genuine online threats. In some cases, online influences can support an interest in targeted violence and impact a minor's online and offline behaviour.
- Young people and minors often have unrestricted access to the internet, which for many, constitutes a large portion of their lives. Parents and caregivers may have limited knowledge or understanding of these online activities. Where minors are socially isolated, the online environment can provide a key social outlet, which can make them more vulnerable to radicalisation. Mental health, adolescent development and personal characteristics can also complicate their situations and potentially make them even more vulnerable to radicalisation.

FIVE-EYES ACTIONS TO UNDERSTAND THE RADICALISATION OF MINORS

- Five-Eyes law enforcement and security agencies are collectively progressing multiple initiatives to better understand the radicalisation of minors towards violent extremism. Some of these initiatives are with established partners, and others involve new relationships outside traditional counter-terrorism partners. Our nations are collectively undertaking research into the radicalisation of minors with academic experts. Engagement with educational institutions and experts is critical to better understand vulnerability

factors around the radicalisation of minors and other factors which may impact investigations including, but not limited to, neurodiversity and mental health factors.

RAISING AWARENESS OF THE RADICALISATION OF MINORS

- In recent years, agencies have brought the issue of the radicalisation of minors to the attention of government and the public. Security and law enforcement agencies have historically been publicly prominent for their involvement in disruptions of potential terrorist attacks and prosecutions of those responsible.
- With young people and minors, Five-Eyes agencies have expressed public concern and a desire for these young people to be diverted before the threat becomes so grave that law enforcement and security agencies need to act. Agencies may take early action to understand the level of threat a minor may pose, which can provide an intervention point for earlier diversion before the threat they pose escalates. This may include diversion to countering violent extremism (CVE) programs, or support services such as mental health providers.

ENABLING EARLY INTERVENTION

- Five-Eyes agencies emphasise the importance of those close to minors looking for signs that an individual may be radicalising to violent extremism. This includes noticing and asking questions of minors, particularly given radicalisation to violent extremism can start with moderately objectionable material containing violent extremist narratives which then intensifies in its support for violence.
- Agencies stress the importance of parents and guardians understanding their children's online activities, so they can identify if their children are engaging with content online which may lead to radicalisation.
- Agencies promote available community and government-based programs to ensure both the minor and family unit or guardians are supported during intervention strategies. Many agencies have publicly released resources about the signs of radicalisation, to provide parents, guardians, teachers and others with a better understanding of what signs to look for and where to access support and guidance.

CASE STUDIES

- These case studies display some of the trends our nations are seeing in our respective security environments. For each case study, the language reflects the national terminology used for the involved types of violent extremism.

AUSTRALIA – CASE STUDY 1

- The Joint Counter Terrorism Team (JCTT) investigated a minor (who was 16 years at the time of offending) following initial reporting they were mobilising to commit an act of ideologically motivated violent extremism (IMVE). JCTTs exist in all states and territories of Australia and consist of the Australian Federal Police (AFP), the relevant State or Territory Police, the Australian Security Intelligence Organisation (ASIO) and, in New South Wales (N.S.W.), the N.S.W. Crime Commission.

- The minor was part of a loosely connected online network involving hundreds of local and international participants, some of whom shared similar IMVE ideologies. The minor was sharing IMVE documents, images and videos, and advocating for attacks on persons of non-Caucasian appearance and urged others to prepare for an upcoming race war to "defend the white race." This included discussing carrying out a mass killing offshore, posting about live-streaming a shooting on Facebook, requesting assistance in bomb-making, praising mass shooters, and suggesting the targeting of "high profile enemies."
- During the JCTT investigation, the minor was observed to have very few real-world relationships which consisted primarily of work colleagues and family members. He did not participate in any extra-curricular activities and appeared to spend limited time socialising offline.
- The risk of the minor undertaking some form of physical attack was assessed as too great, so the AFP moved to overt resolution. The minor was charged with advocating terrorism and urging violence against members or groups. The arrest of the minor and dissemination of intelligence to international partners also led to the arrest of a person of interest offshore who had links to the minor's Telegram posting.
- The minor was sentenced to an 18-month term of imprisonment with a non-parole period of 14 months. Upon sentence expiry, the minor was an adult and was released into the community on an Interim Control Order and has engaged with CVE programs and engagement, and support programs on a number of occasions.

AUSTRALIA – CASE STUDY 2

- The JCTT investigated a minor (14 years) who adhered to a nationalist and racist violent extremist (NRVE) ideology and expressed strong admiration for a terrorist and terrorist attacks.
- The JCTT received information through Crime Stoppers, a community reporting hotline, that the minor had been actively posting IMVE-related content on their Snapchat account, that they planned to conduct a school shooting at their high school and that they had access to firearms and explosives, sufficient to kill a large number of students. The jurisdiction's education department confirmed the minor was known for undertaking racist actions, particularly towards Asians and First Nations people.
- A search warrant executed at the time of the minor's arrest resulted in the seizure of a tactical vest, ballistic helmet and drawings of an extremist nature. Following a search warrant, the minor was charged with a number of offences relating to their use of a carriage service to make threats as well as a charge for advocating terrorism.
- The minor was sentenced to a 2-year good behaviour bond and 12 months' probation. Since the minor's arrest, they have undertaken CVE engagements and were allocated a case manager to provide bespoke CVE support to de-escalate their ideology and behaviours.

CANADA

- The Royal Canadian Mounted Police (RCMP) received information that a social media user had been promoting involuntary celibate (incel) ideology online. However, the suspect went beyond simply advocating misogynist incel philosophies. The RCMP uncovered that the suspect made specific criminal threats to harm a female student in their school.

- Through judicial authorisations and subsequent interviews, the RCMP located the minor who had no documented history of violence and no criminal record. The parents stated their son suffered from a developmental disorder but noted no other health concerns.
- The minor and his family consented to police interviews and spoke openly about the situation. In addition, RCMP obtained search warrants to seize and search the minor's electronic devices. The interviews and search of electronic devices uncovered information, which further confirmed the minor's mindset. The RCMP also discovered that the suspect made many references to Elliot Rodger and Alek Minassian, two often revered figures in the incel movement.
- The most concerning point occurred when the suspect unveiled a violent fixation and fantasy towards one of his female classmates. The suspect openly disclosed many of his violent fantasies online and more specifically his suicidal and homicidal ideations.
- Following these revelations, the RCMP had a duty to warn the school and the female classmate. The RCMP arrested the suspect on a Fear of Terrorism Peace Bond, which is a recognition that reasonable grounds exist to fear a person may commit a terrorism offence. In this case, the RCMP articulated the terrorism offence through the suspect's ideologically motivated violent incel threats. The judge presiding over the case allowed the minor to continue living in the community, but with many restrictions and conditions. One of those conditions was for the minor to work with a third-party non-government organisation (NGO) focused on CVE.
- In addition to working with a third-party NGO, the minor had built a rapport with RCMP investigators during the course of the investigation. Therefore, the RCMP officers from a specialised national security team (that focused on the prevention of violent extremism) continued to monitor and engage with the minor.
- Current information (October 2024) indicates the minor has now denounced the radical misogynist lifestyle he once adhered to. Both the suspect and his parents continue to cooperate with police and the third-party NGO working with them. By all accounts, there have been no issues with this minor and he appears to be living a pro social lifestyle within the community.
- At times, a debate exists regarding who is best placed to interact with suspects who are minors and provide a pathway towards disengagement. This case highlighted that the answer does not need to be binary. All partners including, but not limited to the RCMP, the third-party NGO, educational institute, justice system, and family, had a part to play.

NEW ZEALAND – CASE STUDY 1

- The New Zealand Security Intelligence Service (NZSIS) received information about a possible New Zealand-based account that had been engaging in violent rhetoric on what the New Zealand Government terms "white identity extremist" social media groups. The individual made racist, misogynistic and anti-authority comments, as well as statements indicating a desire to die or commit suicide. Separately, a minor's family member believed that the minor was being groomed online by an adult who appealed to the minor's religious identity and lack of a strong male figure in their life. The user of the account was eventually identified as a New Zealand-based minor. This was confirmed by police analysis.

- Police engagement with the minor's family member provided insight into potential vulnerabilities which may have explained their radicalisation. This included family issues, indications of neurodivergence, and isolation.
- In an effort to disengage the minor from concerning activity, their family enrolled them in a youth group, restricted their time online and confiscated concerning items which family members had noticed they were more openly using around the house. Police continued to engage with the family to provide support for their efforts to disengage the minor.
- NZSIS closed its security investigation as it assessed the minor had limited intent and capability to conduct an act of ideologically motivated violence.

NEW ZEALAND – CASE STUDY 2

- A minor came to law enforcement and security service attention following online threats to blow up a prominent building and places of worship. A formal investigation was commenced following indications the minor held a violent extremist ideology and had a desire to kill specific people. Reporting also indicated that the minor was participating in online groups espousing a wide range of ideologies and was in contact with overseas-based individuals of concern. The minor was arrested and charged with offences related to the threats to kill specific individuals.
- Following the minor's arrest, they were placed in a government-run care home for people under 18 years of age. The minor was also accepted into a young person's disengagement program where they were provided with a variety of support services.
- The minor's wrap-around support aimed to address issues which were impacting their mental health, interpersonal relationships, identity struggles, and lapses in education or employment. While there were setbacks including leaving education, committing non-national security-related crime, and initial difficulty in getting the family to engage with support services, the minor actively participated in the process and was phased out after spending just over a year in the program.

UNITED KINGDOM – CASE STUDY 1

- U.K. Counter Terrorism Policing (CTP) Wales investigated racist and extreme right-wing graffiti and other damage offences at various locations around South Wales, in the summer and autumn of 2022. Community tensions increased as a result, particularly in the Port Talbot area, where one of the offences involved the daubing of extreme right-wing insignia on the Windrush Memorial of a local woman who had died in the pandemic.
- CTP Wales Investigations quickly identified 2 minors (17 years and 15 years) from the local area. They were arrested for criminal damage offences first, and during their initial interviews, both made a number of admissions and were bailed for further inquiries. Their electronic devices were seized and subsequently examined. On examination of huge volumes of digital media, it became clear that the 17-year-old in particular was breaching terrorism laws. Neither male had criminal convictions.
- Through evidence gathered from their electronic devices, it was clear that both males had developed extreme views before they came into contact with each other. They said in an interview that they met in an Instagram group chat before making contact via Telegram on a one-to-one basis from May 2022. They shared their views online and met in person shortly

afterwards when they became close friends over a period of 6 months. They lived approximately 32 km (20 miles) away from each other and met in various parts of South Wales to commit the offences.

- Following an extensive investigation of huge volumes of digital media and "real-world" offending, both were arrested for terrorism offences. The 17-year-old was subsequently charged with numerous Terrorism Act and other offences. He pleaded guilty at Crown Court and was sentenced to 19 months in youth custody. The 15-year-old was charged with a number of racially and homophobically aggravated criminal damage offences and was given a 2-year Criminal Behaviour Order and a one-year Youth Rehabilitation Order.

UNITED KINGDOM – CASE STUDY 2

- U.K. CTP initiated an investigation after receiving information that a minor of school age was engaged in Islamist extremist online activity. Specialist counter-terrorism officers investigated the individual for possible terrorism offences.
- A decline in the minor's mental health (suicidal ideation) increased the risk in the investigation and clearly raised safeguarding concerns. U.K. CTP officers executed a search warrant at the minor's address.
- During the course of the search, the minor's phone was seized and subsequently examined. Some alarming content was found on the minor's phone of a pro-ISIL nature. Officers also noted the vulnerability of the minor who displayed signs of possible autism, although undiagnosed. This further opened the possibility of targeted grooming for radicalisation, so Children's Services were informed.
- The minor was interviewed about the contents found on his phone. He had encouraged and glorified terrorist violence and had accessed violent extremist literature, but there was also a belief that the minor had been in contact with, and been groomed for radicalisation online by, the group al-Muhajiroun and an ISIL member. Officers also identified concerns around isolation, as the minor stated that he did not have many friends.
- Following the Senior Investigating Officer's review of the investigation and case disposal, the minor was referred to "Prevent". Rather than charge the minor with terrorism offences, police decided the minor should be offered support through the Channel Program with an Intervention Provider to examine his beliefs and, if required, offer an alternative narrative. The Channel Program accepted this case, and an intervention provider began work with the minor.
- The minor had been exposed to a great deal of extremist material, and the level of indoctrination and radicalisation was high. To mitigate the extremist narrative, he had been exposed to, a significant number of interventions were completed with the minor, where he was shown alternative ways of fulfilling his religious desires.
- The minor made progress through a large number of Intervention Provider sessions, concentrating on supporting him emotionally and spiritually, especially through his academic exams. Sessions focused on problematic theology and ideology. Topics were covered repeatedly to gauge whether or not the minor was remorseful or showing false compliance. Intervention sessions had some positive impacts.

UNITED STATES

- On 10 May 2021, local police in Arizona arrested a 14-year-old U.S. person on state terrorism charges involving the construction of an improvised explosive device (IED) and the online dissemination of IED-making instructions. During the execution of the federal search warrant at the minor's residence, law enforcement located one fully constructed IED, one partially constructed IED, and a box of parts for the construction of additional devices. The minor admitted to disseminating the instructions used to build the IED, which were from the "How to make a bomb in the kitchen of your mom" article in the first issue of al-Qa'ida in the Arabian Peninsula's Inspire magazine, to other individuals online.
- Following the minor's arrest, they were sentenced to a minimum of 18 months in an Arizona Department of Juvenile Corrections facility, not to exceed the minor's 18th birthday. The minor was released from the detention facility in July 2023 and is currently required to meet all conditions of their supervised release.

CONCLUSION

- These case studies highlight the challenges of minors in counterterrorism. Minors can pose the same credible terrorist threat as adults, with some minors attracted to violent extremist content and ideologies – especially online. Law enforcement and security agencies intervene when there is a potential threat to public safety, but these disruptions are not the only response to this issue. Several of the case studies demonstrate that diversion and CVE programs can make a difference.
- Protecting our nations and young people from violent extremism is a shared responsibility. Five-Eyes law enforcement and security agencies call for a renewed whole-of-society response to help identify and deal with the radicalisation of minors, and minors involved in violent extremist activities. There is a role to play for law enforcement, security and government agencies, the education sector, mental health and social well-being services, communities, and technology companies.

FURTHER RESOURCES

- For more information about understanding radicalisation and where to go for support, refer to the links below.

CANADA

- The RCMP along with municipal police agencies throughout Canada proactively work to disengage individuals identified as being on a pathway to violence. The RCMP conducts disengagement efforts in conjunction with civilian (non-police) CVE groups.
- To learn more or to see a list of CVE groups in your area please visit: [Prevention and Intervention Programs](#)
- To report a non-emergency National Security offence please reference:
- The RCMP National Security Information Network: 1-800-420-5805 or [online](#)
- CSIS' reporting line: 613-993-9620 or [online](#)