

## Challenge

Over the last two decades, the world has undergone a digital transformation. New digital technologies allow people to spend more time online than ever before. News sites, social media channels, video gaming platforms and chat rooms are just one click away. This also means that people are more easily targeted by violent extremists, who proliferate disinformation, fake news, conspiracy narratives and extremist propaganda to further their agenda.



**4.7** billion social media users around the world



**7.4** different social platforms used by a typical social media user each month



**2½** hours average time spent per day using social media

## Platforms

Violent extremists use a variety of social media channels, online gaming platforms, chat rooms and encrypted messaging sites to target, reach, radicalise and recruit vulnerable individuals online. These include, among many others:

**Twitter**  
**Facebook**  
**YouTube**

**TikTok**  
**Telegram**  
**4chan**

**8kun**  
**Gab**  
**Twitich**

## Papers



[Lone Actors in Digital Environments](#)

[Digital Grooming Tactics on Video Gaming & Video Gaming Adjacent Platforms](#)

[An online P/CVE approach for local authorities](#)

[Integrating the online dimension into offline pedagogical practices](#)

[Spotlight on digital ecosystem](#)

## Examples of recent events

### Christchurch Mosque attacks

In March 2019, 51 people were killed in mass shootings at two mosques in Christchurch, in New Zealand. The first of these attacks was live-streamed on Facebook. Prior to the attack the perpetrator had published a manifesto online.

### Bratislava shooting

In October 2022, two people were killed in a mass shooting in Bratislava, Slovakia. The shooting was declared an anti-LGBT hate crime. The perpetrator used Twitter to communicate, posting a series of hashtags such as “Now what, got any last words for me guys?” and “Bye bye, see you on the other side”.

### Buffalo shootings

In May 2022, ten people were killed at a mass shooting in Buffalo, New York in the US. The attacker was an ethno-nationalist who voiced support for the ‘Great Replacement’ conspiracy theory. He livestreamed the attack on Twitch and posted a 180-page manifesto, which was shared widely online.

## Challenges for practitioners

### Skills and knowledge

Practitioners need to gain more digital savviness, such as knowledge about current platforms and recruitment tactics that are being used, how to identify and target audiences online, and how to translate offline activities online.

### Capacity

Practitioners need more time and means to keep track of digital trends, monitor online traffic, spend time on relevant social media platforms, and assess the latest online narratives which are propagated.

### Audience engagement

It is difficult to segment the audience in order to make the right distinction between vulnerable youths, the radical agitators who need to be banned or prosecuted and the ‘trolls’.

### Exposure

Working online can cause danger or exposure to hate speech for practitioners – which can be a mental health challenge – and may require them to seek alternative ways of working.

### Legal structures

Legal structures concerning working online are currently vague or absent. For instance, should practitioners engage on the dark web with its illegal content? How far can or should they go? What are the ethical boundaries?

### Information sharing

Sharing information about online observations is challenging regarding legal regulations.

### Collaboration with the tech industry

The interests of local coordinators and practitioners might not align with those of the tech companies.

## Tips for practitioners

- Use artificial intelligence to detect and monitor extremist content
- Consider how online interventions can be included in existing approaches
- Assign roles for sharing of information
- Involve youth in online activities
- Promote alternative narratives
- Raise public awareness of online risks
- Conduct outreach to vulnerable individuals online