

Online platforms and extremist communities in Denmark 2025

Content

| | |
|--|----|
| Summary | 3 |
| Introduction | 4 |
| Online platforms – types and use | 5 |
| Changed conditions for communication and behaviour | 6 |
| Propaganda on online platforms | 9 |
| Recruitment via online platforms | 11 |
| Impact on the terrorist threat | 13 |
| Appendix | 15 |



Summary

Continuous technological progress and a growing number of online platforms in the West, including Denmark, are changing the dynamics of communication and behaviour. This change also affects extremist communities that use online platforms for disseminating propaganda, recruiting members, organizing activities and communicating internally.

Online communication eliminates the need for physical presence and offers anonymity. When participation in online activity is not regulated by such criteria as geographic distance, age, gender and ethnicity, *the number of potential participants and the access to international extremist communities expand.* Also, online platforms offer greater access to informal interactions and communities. Further, the technical options can *accelerate the speed of dissemination and facilitate the creation of online material and content*, which increases the overall volume of such content online.

The implication of the above developments is that *a growing number of extremists, including very young individuals and minors, can become important online actors.* Another outcome is that *the average user of online platforms is at greater risk of being exposed to unwanted extremist material.* This also applies to mainstream online communities that are not extremist in nature.

The freedom to navigate online means that *extremists are less rooted in clearly defined ideological frameworks than previously.* The extremist online communities serve as echo chambers and may quickly push the participants' ethical and social boundaries. *Online extremist content, statements and behaviour may in that connection increasingly be conceived as normal by the users.*

Overall, extremists' use of online platforms increases and changes the requirements facing authorities in relation to preventing and counteracting extremism. In the short term, this may *strengthen the resilience of certain extremist communities to authority initiatives.* Thus, these developments may potentially affect the terrorist threat to Denmark across all types of extremism.

Introduction

A number of Danish sentences relating to online facilitation of terrorist activities have been delivered in recent years. In CTA's Assessment of the Terrorist Threat to Denmark 2024, CTA assesses that radicalization increasingly takes place via online communication platforms, gaming platforms and social media. Below, we refer to all three groups as "online platforms". For instance, extremist actors in the West use online platforms for disseminating propaganda, recruiting members, organizing activities and communicating internally, all of which contribute to radicalization.

Extremist communities continue to examine the options offered by online platforms and related tools, such as AI, for promoting their agendas and going under the radar of the authorities.

Therefore, the purpose of this analysis is to examine and describe how the above dynamics can affect the available options and behaviour of Danish extremist communities and the importance this may have on the terrorist threat to Denmark across all types of extremism.

Online platforms – types and use

The internet offers access to an extensive and continuously changing space of online platforms with a mix of focus, structure and functionality. Thus, the platforms have different features, content, and target groups/users.

Extremist communities use all types of online platforms. The specific choice of platform is dynamic and does not follow a standard pattern, but depends on a number of sometimes competing factors such as *the popularity and knowledge* of the platform among the general public or the specific target group, the *purpose* of the platform, the extent of *content moderation* on the platform and *its encryption capability*.

These factors contribute to determining the platforms chiefly used in each extremist community, and therefore platforms may vary significantly. However, CTA assesses that there is a tendency for extremists to mainly apply large, widely used and easily accessible platforms for propaganda and initial recruitment steps, whereas the more specialized platforms with a lower degree of content moderation and superior encryption capability are more commonly used for internal communication and recruitment.

DEFINITIONS



This analysis distinguishes between the following concepts:

Online platform denotes a digital application that may be used to communicate with other individuals.

Online forum denotes a specific group or channel on an online platform.

Online network denotes a large number of individuals who are loosely connected via an online platform used for joint communication.

Online community denotes a number of individuals who share an opinion on a given topic, but who may not necessarily be in direct contact.

Online organization denotes a number of individuals engaged in a structured collaboration aimed at a specific target via an online platform.

Changed conditions for communication and behaviour

Growth in online communication has significantly changed the conditions for communication and social communities in society and thus also in extremist communities.

Conditions for communication

Online communication eliminates the need for physical presence and offers anonymity for both the sender and the recipient. When participation is not necessarily regulated by such criteria as geographic distance, age, gender and ethnicity, the number of potential participants grows.

These dynamics also prevail in Danish extremist communities, which may increase extremist communication, online activity, and the number of potential participants. As online communities are not geographically limited, the use of online platforms increases the access of extremists in Denmark to international extremist communities and networks, which enhances the risk of radicalization and the possibility of finding peers. Thus, small and geographically dispersed extremist communities have a tool for maintaining continuous contact and mutual relations – also across borders. CTA assesses that this may sustain and reinforce extremist narratives in Denmark.

The structure of the platforms enables individuals with administrator rights to maintain tightly controlled one-way communication and strict control over participation and content relating to the online forums they control. This may improve extremists' ability to control access to the dissemination of, and/or to affect the content of, specific extremist narratives.

Automated user accounts, or bots (see page 10) operated automatically by AI (i.e. a robot), can also be created. This means that online forums operated by bots have a fast response time and a high non-stop operational capability. This speeds up the dissemination of extremist narratives considerably, while providing a security layer of anonymity between the human sender and the recipient of extremist messages.

Anonymity, dynamic use of online platforms and *"tactical crossposting"*¹ enable extremists to change forums quickly and continuously without losing data that is valuable to their cause. In this way, *"de-platforming"*, i.e. content moderation and banning by the provider, is avoided, which strengthens the viability of virtual extremist networks.

Behavioural effect

In parallel with tightly controlled online forums, online platforms enable extremist users to move quickly and freely between different communities and interactions of an informal nature. This paves the way for new types of networking and organizing that are less hierarchical and free of central regulation. Therefore, the behaviour characterizing extremist online networks is less rooted in clearly defined ideological frameworks than previously and is often affected by individual interpretations and local agendas. Changes in these networks are accelerated by the automated user accounts mentioned above.

CTA assesses that these trends contribute to the hybridization² and ever-changing organization which is a distinct trait in parts of the virtual extremist communities in the West, including Denmark.

The growing number of extremist online networks, coupled with more informal relations, increases the possibility that individuals find a community reflecting their own world views. Sometimes, this may encourage individuals to search for stronger affiliations. Stronger affiliations may in turn cause members of extremist online communities to experience that the extremist behaviour they engage in becomes normalized, as the community serves as an echo chamber and a frame of reference. The perceived normality may potentially step up extremist behaviour.

-
- 1) *The concept of tactical cross-posting denotes the practice that groups or individuals on various online platforms create a great number of profiles and channels that are interconnected via references and links in order to minimize the effects of banning*
 - 2) *Hybridization denotes a process in which different ideologies, world views or communities are mixed to form new extremist narratives and modi operandi among individuals, groups or communities. For further information, see CTA's Assessment of the Terrorist Threat to Denmark 2023 and 2024.*

The combination of anonymity, easy access, and freedom to navigate on online platforms creates a community in certain online spaces where extremist and non-extremist content is mixed, and where the boundaries of acceptable behaviour are blurred. For instance, extremists benefit from this situation by spreading propaganda and pushing the boundaries of the surrounding society in terms of what is considered acceptable statements and views³.

TONE OF VOICE AND BEHAVIOUR ON ONLINE PLATFORMS



Extremists have an online presence in forums characterized by the possibility of anonymity afforded by the internet. Anonymity eliminates regulating social norms, leading to a higher prevalence of ironic and offensive language and behaviour in online forums than in physical ones. This phenomenon is referred to as the *internet disinhibition* and comes in such forms as *LARPing* and *shitposting*.

LARPing (Live Action Role Playing) denotes a situation in which individuals may have a few or many alternative identities on the internet and may display boundary-pushing behaviour.

Shitposting denotes the behaviour displayed by individuals who use the anonymity of the internet and a very offensive language to criticize or outright harass other people with the sole purpose of derailing a dialogue.

The above behaviour may create dynamics that lead members of extremist communities to communicate online about attack planning and weapons capability even though they may lack genuine intent or feasibility.

In addition, extremists' niche interests and need for communicating with peers on public platforms contribute to the development of "coded language" including the use of implicit references from gaming language or numerical codes. This phenomenon is also referred to as *implicit hate speech* (IHS). In other contexts, the term *dogwhistling* is used, as only insiders can respond correctly to the message.

3) This theoretical concept is also referred to as the *Overton Window*, named after the American researcher Joseph Overton. The concept is used to describe how the boundaries of generally accepted political views in society may shift over time.

Propaganda on online platforms

The technological options offered by online platforms reinforce extremists' possibilities of rendering extremist propaganda accessible..

The algorithms of online platforms support and reinforce the dissemination of (extremist) messages, as users are directed towards content which is similar to their previous searches. Thus, users are exposed to content that is increasingly homogenous, and therefore users end up in an echo chamber with peers.

Extremists leverage algorithms by using hashtags and content titles that do not violate the guidelines of the platforms, but continue to lead users towards extremist material. For instance, right-wing extremist hashtags, below #andersbehringbreivik, are combined with common hashtags like #europe and #foryoupage (the user's personal TikTok front page), see Figure 1.

Thus, extremists seek to use the algorithms of platforms to ensure larger exposure of their posts – also among individuals who do not actively search for extremist content. In the same way, extremist content is disseminated by referring to popular tunes and current topics in similar posts to leverage the tendency of the algorithm to share what is currently trending on the platform.

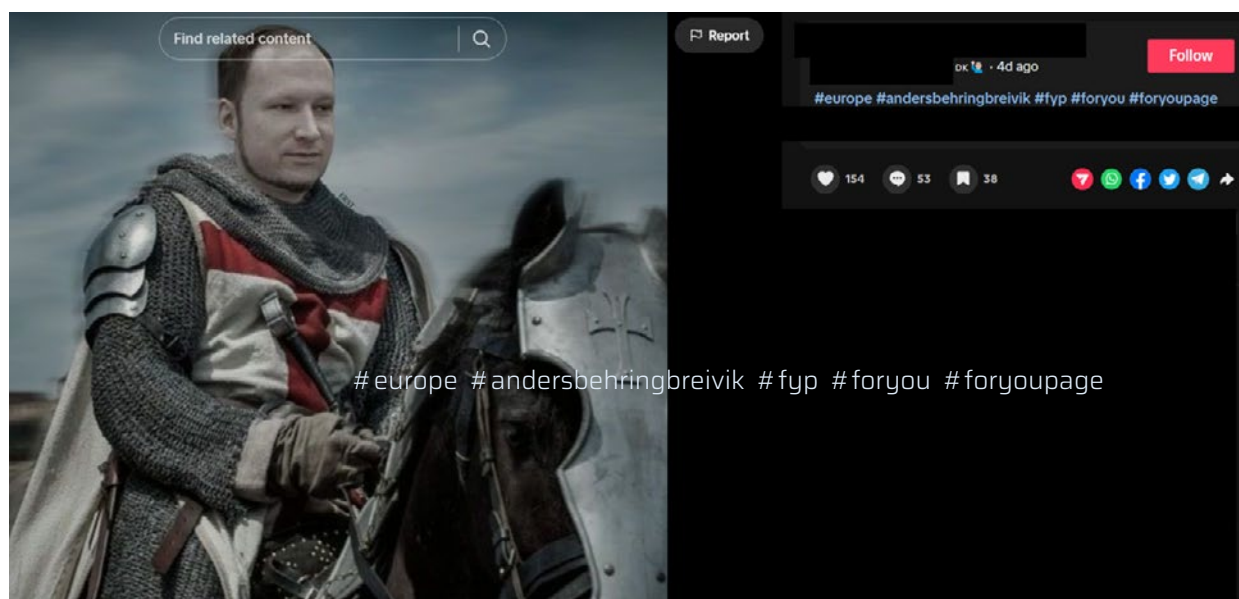


Figure 1: Example of a TikTok post with hashtags.

Some technologies (see the fact box below) make it possible to rapidly create material that engages users and reduces the risk of being banned by moderators. This accelerates the risk that the average user of online platforms is exposed to unwanted extremist material.

CTA assesses that users often disregard extremist content simply by scrolling past it rather than notifying the moderators of the platforms. This prolongs the online life of extremist content.

CTA assesses that this behaviour, coupled with mass dissemination, is instrumental in enhancing knowledge of extremist messages. As previously mentioned, these dynamics may push the recipients' ethical and social boundaries for what is considered acceptable behaviour and may potentially contribute to a radicalization process.

TECHNOLOGIES AND COMMUNICATION TECHNIQUES



Extremists use online technologies and communication techniques to create and edit material and promote user involvement:

The concept of bots denotes automated user accounts, see page 6 for more details. Extremists may use bots on online platforms for *rapid dissemination and sharing or resharing of material*. Bots also offer an extra layer of anonymity between the sender and the recipient of extremist messages.

AI such as the large language model that powers ChatGPT may be used to create new text and to translate or simplify text with extremist messages which is written in other languages or is otherwise difficult to access.

Generative AI is a type of artificial intelligence capable of generating new and complex content via algorithms and bulk data. Extremists may use generative AI to easily and *rapidly create new visual material* designed to engage social media users. The technology can blur extremist messages and thus render moderation more difficult, for instance by concealing or modifying extremist symbols and incorporating them graphically into landscape pictures. It is also possible to create seemingly real, but fake, material that supports extremist narratives and thus strengthens the extremist agenda. This may be used to reinforce conspiracy theories and misinformation.

Gamification is a technique used to disseminate messages by *influencing user behaviour and views through gaming design and techniques*. In an extremist context, users may be activated or rewarded, and highscore lists may be applied to generate empathy and involvement in users who may potentially come into contact with extremist communities without being aware of it initially.

Gamification takes many forms, for example when extremists build copies of concentration camps in Minecraft and publish recordings of it on online platforms, or when extremist fantasies are enacted in computer games and published in the same way. This type of content prompts extensive interaction, and its references to popular culture reach an audience far beyond extremists' own ranks.

Gamification has sometimes been used in connection with terrorist attacks in the West, with perpetrators describing their targets using gaming terminology – for instance as so-called *achievements*, which trigger a reward in the gaming world.

Recruitment via online platforms

An extremist recruitment process may be described as a "funnel", in which individuals gradually move towards more explicit extremist content and more closed groups. Online platforms do not change these dynamics; by contrast they offer new possibilities. Overall, recruitment becomes easier, less resource-intensive, more anonymous and therefore less risky. In addition, online forums widen the recruitment reach, because they are used across country borders and cultural and social differences.

Online recruitment is not a linear process, and each process is unique. Thus, a recruitment process may change from online to offline contact, move from one level to another in the funnel, or take place at several levels simultaneously. Different platforms may also be used at dif-

ferent levels of the funnel. Accordingly, the figure below is a general description of the process with a focus on the role of online platforms.

Large, public and easily accessible platforms such as Facebook, TikTok, Instagram and YouTube are often a stepping stone to initial contact with extremist communities. Here, current agendas are mixed with subtle extremist references and messages, and they are shared in order to arouse interest in extremist narratives. Extremist content is referred to either in general terms or is used in edited versions as memes, coded language or emojis that may be related to extremist narratives depending on the context.

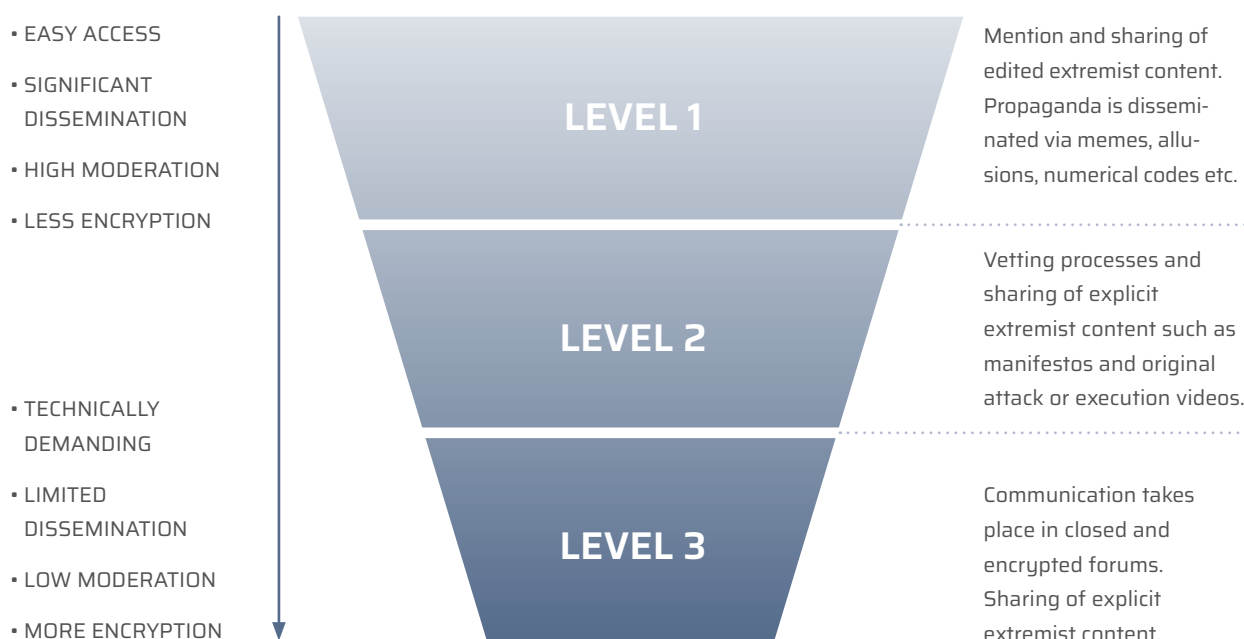


Figure 2: Indicative figure of online platform characteristics and of how they may be used by extremists for recruitment. However, in practice all types of platforms may be seen at all funnel levels depending on the specific use (see the appendix for an overview of platforms).

Users showing an interest in extremist content may then be invited to visit other platforms with more encryption and less moderation and/or may be invited to join closed online groups, thus moving further down the funnel. At this level, we see explicit communication relating to extremist narratives, actual vetting processes and sharing of unedited extremist content such as bomb-making manuals and execution videos.

At the bottom of the funnel, extremist groups communicate internally in encrypted and closed forums with access for group members only.

CTA assesses that these funnel dynamics are exacerbated by the algorithms of the platforms as they direct users towards content which is similar to their previous searches and thus potentially towards increasingly extremist material.

COMMUNICATION ON ONLINE PLATFORMS



Communication on online platforms is generally divided into three levels across a multitude of platforms:

Page/user/profile are used for an individual presentation of the user/profile.

Channels, private or public, are used for communication between one sender and multiple recipients, giving the sender full control of interaction on the channel.

Groups, private or public, where one or more administrators regulate group member interaction according to the given guidelines.

Impact on the terrorist threat



Extremists' use of online platforms does not equal an absence of traditional relations and activities in physical extremist communities. The platforms offer new opportunities, for instance in terms of speed and access to extremist propaganda and new communities, and they are used in parallel with, and as a supplement to, physical activities. According to research, the vast majority of people no longer consider online and offline domains as essentially different "worlds".⁴ Actions in one domain are often caused by or lead to actions in the other domain – like when a physical conversation is continued on an online platform. One domain does not replace the other – they are dynamically interlinked.

The development in online platforms and their use by extremists is dynamic and is determined by factors such as technological progress and the efforts of platforms to remove extremist content. Therefore, it is difficult to make a specific assessment of how extremists' use of online platforms will affect the terrorist threat to Denmark in the long term.

However, CTA assesses that the use of online platforms, as described in this analysis, will continue, as the platforms offer extremists new opportunities, for instance in terms of communication and identity concealment. Against this background, CTA assesses that extremists' use of online platforms may contribute to increasing radicalization and attempts at recruiting people to extremist communities, which in the long run may enhance the terrorist threat from extremist groups, which may use platforms for propaganda and recruitment, and from individuals who find inspiration and justification for attacks, for instance in online forums. Developments necessitate enhanced authority capabilities for preventing and countering radicalization and extremism.

The dissemination of extremist material in more mainstream online communities may cause individuals to be increasingly exposed to extremist messages. CTA assesses that this may potentially radicalize vulnerable individuals, including young people and minors, who are not necessarily aware of the initial stage of the radicalization process or who do not understand the consequences of accessing and sharing propaganda.

CTA assesses that, for the time being, AI in an extremist context is mainly being used to provide access to, and facilitate the production of, propaganda. Examples of such use are translation of material and production of images and videos. In the short term, AI may be instrumental in enhancing the reach of extremist material and in circumventing content moderation on online platforms. In the long term, AI may be used to produce new and unique material aimed at a specific audience.

4) See also the article by Joe Whittaker (2022): *Rethinking Online Radicalization in Perspectives on Terrorism*, which summarizes research in this field.

In conjunction with a number of technologies and techniques, online platforms enable individuals, including very young actors, to mass disseminate propaganda with minimal effort via multiple forums. CTA assesses that these dynamics can accelerate, retain and promote radicalization and build intention and capability. In the long term, it may also result in a higher tendency to share user-generated propaganda on mainstream platforms such as TikTok, Instagram, Discord and Roblox, which do not generally disseminate extremist material. This may potentially expose a growing number of young people and minors to extremist propaganda. This may be instrumental in radicalizing a broader range of people and, over time, push the users' ethical and social boundaries for what is considered acceptable behaviour in relation to extremist narratives and violence.

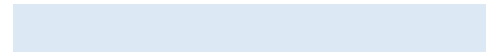
Owing to the fact that online communities are not geographically limited, the use of online platforms in Denmark gives extremists access to international extremist communities. This may potentially increase inspiration and networking in extremist communities across borders.

The assessments of this analysis do not change the overall threat picture in Denmark. For further reading, see Assessment of the Terrorist Threat to Denmark 2025.

Appendix

| TYPE | PLATFORMS | PRINCIPAL USE |
|----------------------------------|--|--|
| Messaging services | For instance Telegram, Discord, Signal, Messenger and WhatsApp | These services are used for direct communication in large or small (personal/private) forums. One person may communicate with many in a so-called channel or in private groups with restricted access. The services may also be used for sharing files. |
| Social media | For instance Facebook, Instagram and X | Social media are used for networking, which is powered by algorithms recommending content to the users. These media are generally public, but they may also be used by private groups. |
| Video-sharing platforms | For instance YouTube, TikTok, Twitch and BitChute | These platforms focus on video sharing from one sender to others. The sender controls the communication, which takes the form of comments on the videos. |
| Game-related platforms and games | For instance Steam, Twitch, Discord, Roblox, Minecraft and a host of games | This category is a mix of platforms and games. Gaming platforms like Steam offer communication features. In addition, platforms like Twitch facilitate commenting during livestreams, while Discord provides chat functionality. Many games, including Roblox and Minecraft, feature in-game chat for direct player communication. |
| Message/image boards | For instance Reddit, 4chan and 8chan | In these discussion forums, it is possible to share images and files. |

Overview of types of online platforms used by extremist communities in Denmark. In many cases, platforms have overlapping functionality, and they are therefore classified on the basis of their principal purpose.



DANISH SECURITY AND INTELLIGENCE SERVICE & CENTRE FOR TERROR ANALYSIS
ONLINE PLATFORMS AND EXTREMIST COMMUNITIES IN DENMARK
PUBLISHED: MARCH 2025



DANISH SECURITY AND INTELLIGENCE SERVICE
KLAUSDALSBROVEJ 1
DK-2860 SØBORG
TEL: 45 15 90 07 • PET@PET.DK • WWW.PET.DK