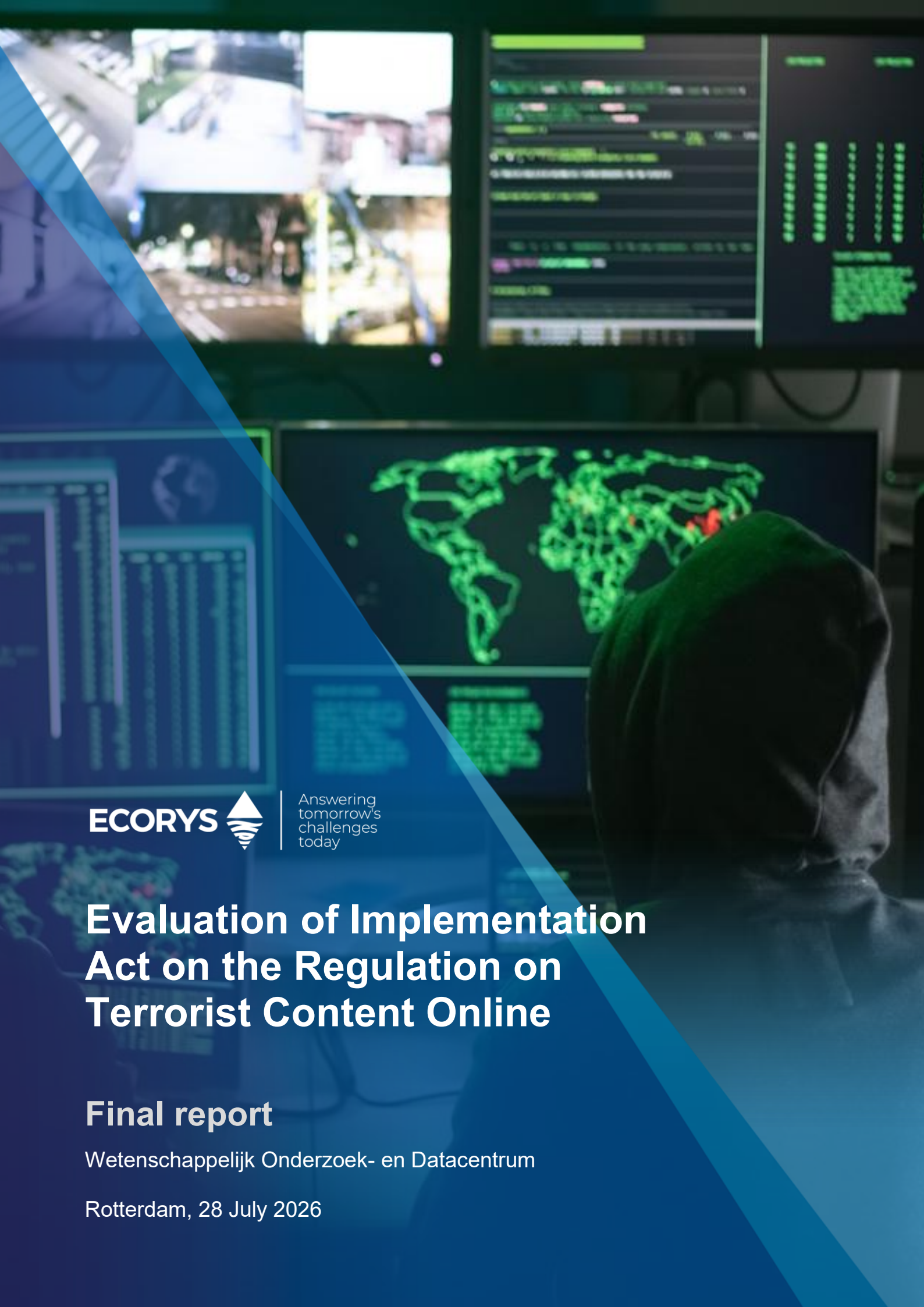


ECORYS

Answering tomorrow's challenges today

Evaluation of Implementation Act on the Regulation on Terrorist Content Online

Final report

Wetenschappelijk Onderzoek- en Datacentrum

Rotterdam, 28 July 2026

Summary

Background, objectives and research questions

To combat the dissemination of terrorist content online, Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online (the EU Regulation) entered into force in 2022. This regulation establishes a framework enabling competent authorities in EU Member States to require hosting service providers (HSPs) to remove terrorist content or disable access to it. The Netherlands implemented this regulation through the Implementation Act on the Regulation on Terrorist Content Online (Implementation Act TCO) and designated the Authority for Online Terrorist and Child Sexual Abuse Material (ATKM) as the competent authority.

The Implementation Act TCO must be evaluated within three years of its entry into force. This evaluation fulfils that statutory obligation. The evaluation has two principal objectives: assessing the effectiveness of the Implementation Act TCO and examining how the Act functions in practice. The central evaluation question is:

"To what extent is the Implementation Act TCO effective, and how does the Act function, in particular with regard to its practical application and operation, the governance structure that was chosen, and the balance between, on the one hand, the application of the Act and, on the other hand, the rule-of-law protection afforded to hosting service providers, internet platforms and users of online content?"

The research question was elaborated through five thematic areas:

a. Proper application of and compliance with removal orders;
b. Legal aspects of removal orders;
c. Capacity, feasibility and administrative burden;
d. Governance and cooperation;
e. Effectiveness and impact on online safety.

Methodology

The evaluation was carried out between December 2025 and July 2026 and covers the period from the entry into force of the Implementation Act TCO on 1 September 2023 through June 2026.[1] To answer the research questions, multiple research methods were used.

First, a literature and document review was conducted covering academic literature, policy documentation, parliamentary documents and relevant national and international publications. In addition, 28 semi-structured interviews were conducted with representatives of the ATKM, Dutch government organisations, EU institutions, foreign competent authorities, HSPs, civil society organisations and academic experts.

[1] Only article 13 and 16 entered into force later (August 2025). See: Ministerie van Justitie (2025), Nota van toelichting, Staatsblad. 2025, 216.

A so-called "*fil rouge*" workshop was also organised, during which the functioning of the Act and its implementation were reconstructed step by step. Furthermore, case studies were carried out in Germany, Ireland and Sweden, focusing on how other EU Member States have organised their competent authorities. The preliminary findings were subsequently discussed during a validation workshop attended by relevant stakeholders. The findings from these different research methods were then compared and synthesised in this final report.

The Implementation Act TCO in brief

The EU Regulation and the Dutch Implementation Act on Terrorist Content Online seek to limit the dissemination of terrorist content online. The central instrument is the removal order. Through a removal order, a competent authority can require an HSP to remove terrorist content or disable access to it within one hour of receipt of the order. In addition, the EU Regulation contains provisions on cross-border cooperation, legal remedies, transparency, sanctions and 'exposure decisions'. Through an exposure decision, an HSP that is repeatedly exposed to terrorist content may be required to take specific measures to protect its services against the dissemination of terrorist content online.

In the Netherlands, the ATKM is responsible for implementing these tasks. On the one hand, the ATKM is tasked with identifying terrorist content online and promoting or enforcing its removal or disabling of access. On the other hand, it has a broader signalling and knowledge-sharing role and is expected to share insights on developments relating to terrorist content online with relevant stakeholders. The ATKM is explicitly not a law-enforcement body and is not involved in prosecuting individuals who produce or disseminate terrorist content.

Findings

Proper application of and compliance with removal orders

The Implementation Act TCO is applied carefully in practice. The ATKM has established a structured process for identifying, assessing and issuing removal orders requiring HSPs to remove terrorist content or disable access to it. Terrorist content is identified primarily through manual open-source intelligence (OSINT) activities conducted by specialised staff. Automated detection tools are currently unavailable, meaning that detection capacity remains heavily dependent on manual monitoring.

Following identification, content is assessed on the basis of legal, substantive and fundamental-rights criteria. The assessment considers not only the content itself but also the context in which it is disseminated. In principle, assessments are conducted by multiple reviewers and include an explicit consideration of freedom of expression. No indications were found of structural errors, systematic over-removal of lawful content or other unintended adverse effects.

At the same time, only part of the identified content ultimately results in a removal order. The ATKM estimates that approximately three-quarters of flagged content is excluded because it falls within a grey area of extremist or otherwise concerning expression that does not clearly meet the legal definition of terrorist content online, or because the content is no longer accessible by the time a removal order can be issued, for example because a competent authority in another Member State has already issued an order or because the HSP has removed the content voluntarily.

As a result, a gap exists between the broader online problem as perceived by stakeholders and the specific category of content against which the Implementation Act TCO can intervene. Compliance with removal orders is high. During 2024 and 2025, approximately 330 removal orders were issued, and almost all were complied with within the statutory deadline. Notably, the ATKM accounted for around 20% of all removal orders issued by competent authorities in the Member States in 2024 and 2025. No fines or penalty payments were imposed for non-compliance. HSPs generally view the implementation of removal orders positively, although they identify challenges related to the one-hour deadline.

The main challenge lies not in compliance with removal orders but in the period preceding their issuance. Legal assessment, administrative processing and deconfliction procedures[2] with the police are time-consuming. As a result, terrorist content may remain available online for a period before action can be taken.

Furthermore, several components of the legal framework have not yet been used. No objections or appeals have been lodged to date. No exposure decisions have been issued, and no use has been made of the dispute resolution procedure. Consequently, practical experience with several important elements of the framework remains limited and their actual functioning is not yet fully apparent. The non-use of exposure decisions in particular represents a missed opportunity from the perspective of the ATKM's effectiveness.

Legal aspects of removal orders

Implementation of the Act remains within the boundaries of freedom of expression and other fundamental rights. The ATKM applies a careful assessment procedure in which substantive, legal and fundamental-rights considerations are explicitly taken into account. No indications were found of structural over-blocking, chilling effects or other unintended consequences affecting lawful online content.

However, this conclusion is subject to an important limitation. To date, no objections or appeals have been filed against removal orders issued by the ATKM. Consequently, there has been no independent judicial review of how the legal criteria are interpreted and applied. A recurring issue concerns borderline content: extremist or radicalising content that is regarded as concerning but does not qualify as terrorist content online. The current mandate of the ATKM is limited to terrorist content online, meaning that it has no legal basis for acting in relation to such borderline content.

The Implementation Act TCO does not explicitly exclude the use of referrals. Views differ regarding the desirability of such referrals. Supporters consider them a means of acting more quickly against terrorist content, while opponents point to risks for legal safeguards and the danger of shifting substantive decision-making from public authorities to private platforms.

[2] Deconfliction refers to the process whereby the ATKM consults with the police prior to taking action to determine whether identified online content is linked to an ongoing criminal or intelligence investigation, thereby ensuring that the issuance of a removal order does not compromise law-enforcement or intelligence operations.

Capacity, feasibility and administrative burden

The ATKM has rapidly established an operational organisation and a functioning primary process. At the same time, it remains highly dependent on a small group of specialised staff, and a significant proportion of the work is still performed manually.

A key concern is the absence of automated detection tools. This limits detection capacity and leaves the organisation heavily reliant on manual monitoring. The capacity available for additional activities, such as trend analysis, knowledge development and the use of supplementary instruments, is also limited. Current staffing and technical resources do not fully align with the organisation's ambitions and responsibilities.

The Act also imposes implementation burdens on HSPs, particularly the obligation to comply with removal orders within one hour. Large international platforms generally have extensive systems and procedures in place to meet this requirement. For smaller providers, however, compliance may pose a greater challenge. The research also shows that providers without a European establishment or representative are relatively difficult to reach, making enforcement towards this category less effective.

Governance and cooperation

The decision to establish the ATKM as an independent administrative authority is generally viewed positively. Its independent position enables the ATKM to maintain a constructive working relationship with HSPs. Moreover, its status has contributed to its development as an expert organisation in the field of terrorist content. Internationally, the organisation has also built a strong reputation in a relatively short period of time. Various foreign partners describe the ATKM as a knowledgeable, proactive and cooperative competent authority.

At the same time, this governance model also entails limitations. Because the ATKM is not a law-enforcement authority, it depends on the police for certain activities, including deconfliction procedures, information exchange and access to Europol systems such as SIENA. The benefits of independence therefore come with operational dependencies that also affect efficiency.

Cooperation with national partners, foreign competent authorities, Europol and HSPs is assessed predominantly positively.

Effectiveness and impact on online safety

The evaluation shows that the Implementation Act TCO demonstrably produces results at the level of individual interventions. When terrorist content is identified and a removal order is issued, that content is removed or access to it is disabled in almost all cases. At this level, the legislation can be regarded as effective.

However, it is considerably more difficult to draw conclusions regarding its impact on the broader phenomenon of terrorist content online or on national security. No baseline measurement exists, making it impossible to determine the overall scale of the problem or how much content is affected by the legislation. In addition, terrorist content frequently migrates between platforms, while some activity shifts to closed or encrypted environments that fall outside the scope of the Regulation.

Furthermore, the ATKM, like other competent authorities in Europe, is likely to detect only a proportion of the terrorist content available online. Consequently, no direct relationship can be established between the operation of the legislation and a general reduction in terrorist content across the internet. Nonetheless, it is plausible that the legislation contributes to reducing the visibility and availability of specific forms of terrorist content online.

Conclusions

The evaluation demonstrates that the Implementation Act TCO largely operates in practice as intended. The ATKM has established, within a relatively short period, a functioning organisation for identifying, assessing and removing terrorist content online. It has implemented a structured process in which legal diligence, consideration of fundamental rights and specialist expertise are central.

Removal orders are carefully prepared and are almost always complied with within the one-hour deadline. The ATKM also makes a substantial contribution to the overall number of removal orders issued across the EU. No indications were found of systematic violations of fundamental rights, excessive removal of lawful content or other unintended consequences. At the same time, no independent judicial review has yet taken place, as no objections or appeals have been submitted and no exposure decisions have been issued.

The effectiveness of the legislation is constrained by a range of factors linked to the design of the instrument, available capacity and characteristics of the online environment. Implementation relies almost entirely on one instrument: the removal order. Another instrument foreseen by the legislation, a decision requesting specific measures, has not been used during the evaluation period. This instrument has the potential to contribute to more structural measures by HSPs. To date, however, it has not been deployed due to the absence of a clear and uniform framework for the application of this instrument and the assessment of the (specific) measures taken by HSPs. Furthermore, the evaluation shows that the Implementation Act TCO does not explicitly exclude the use of referrals, although opinions differ on their desirability because of the trade-off between effectiveness on the one hand and legal protection on the other.

Detection remains manual, making it likely that only a proportion of available terrorist content is actually identified. In addition, a substantial share of content detected by the ATKM ultimately falls outside the scope of the legislation because it constitutes borderline content or has already been removed before action can be taken.

The governance model also presents both advantages and disadvantages. The independent status of the ATKM supports impartial decision-making and constructive engagement with HSPs. The organisation has become a respected international partner and plays an active role in European initiatives aimed at harmonising approaches to terrorist content online. However, its status as an administrative supervisory authority means that it remains dependent on others, particularly the police, for deconfliction, access to information sources and international information exchange.

In terms of effectiveness, the overall picture is nuanced. At the level of individual interventions, the legislation clearly works. Terrorist content is identified, removal orders are issued and the content concerned is removed or access is disabled in almost all cases within the required

timeframe. However, it cannot be determined to what extent the legislation has led to a broader reduction in terrorist content or to measurable improvements in national security.

Recommendations

Based on the findings of this evaluation, several points for attention emerge for the further development of the Implementation Act TCO and its implementation in practice. These have been divided into recommendations for the Ministry of Justice and Security and the Government, and recommendations for the ATKM.

Recommendations to the Ministry of Justice and Security and the Government

1. Reconsider the dispute resolution procedure under Article 16 of the Implementation Act TCO

The Netherlands is the only Member State that has incorporated an additional dispute resolution procedure into its implementing legislation. To date, this procedure has not been used. Moreover, the ATKM perceives her dual role in the procedure as complex; as competent authority she takes exposure decisions and in the dispute resolution procedure she might need to assess the (actions taken as a result of the) exposure decisions. Moreover, the ATKM expects the implementation of the dispute resolution procedure to be resource intensive. Given that users already benefit from adequate legal protection through administrative law procedures and through the Digital Services Act, reconsideration or simplification of this procedure is recommended.

2. Examine the policy feasibility of introducing a terrorist content online referrals as an additional instrument for the ATKM

The Netherlands is one of the few EU Member States that relies exclusively on the binding removal order. Many Member States also make use of referrals and only resort to a removal order where compliance does not follow. A referral can shorten processing times, reduce the administrative burden and provide the HSP with additional time to respond. The current legal framework appears to provide scope for the use of referrals in relation to terrorist content online. As the use of referrals alongside orders offers both advantages and disadvantages, a careful assessment should be undertaken as to whether such referrals should be introduced.

3. Examine the legal feasibility of a broader mandate for the ATKM to enable action against borderline content

At present, the ATKM is explicitly unable to use referrals in relation to borderline content. Should it be considered desirable for the organisation to address such content, alternative options should be explored, including expanding the statutory framework or designating the ATKM as a DSA trusted flagger.

4. Invest in the technical and human-resource preconditions required for the ATKM

The current budget and staffing levels are insufficient for an ATKM that is expected to operate effectively over the medium term. Investment in the development and funding of automated detection tools, staffing levels that reduce continuity risks, and appropriate accommodation that reflects the unique nature of the work should be viewed not as luxuries but as essential preconditions for the effective implementation of the legislation.

5. Facilitate the ATKM's access to relevant Europol information

The ATKM's information position is constrained by the absence of direct access to Europol products, such as Check the Web and hash lists.[3] In consultation with Europol and the police, arrangements should be established to ensure the structured and timely provision of such information to the ATKM, whilst preserving the principled distinction between supervision (ATKM) and law enforcement (police).

Recommendations to the ATKM

6. Prioritise the operationalisation of automated detection tools as a strategic priority

Manual detection currently constitutes the principal bottleneck in the primary process. Automated detection is not only an efficiency gain but also a prerequisite for scalability, including increased detection capacity and the ability to detect terrorist content outside regular office hours. The ATKM should prioritise the ongoing customised development trajectory for detection software and, where possible, make use of interim solutions that can bridge the period until full implementation.

7. Develop a framework for the use of exposure decisions

The exposure decision is a particularly powerful instrument for driving structural behavioural change among HSPs. The ATKM should, preferably in cooperation with European partners, develop an operational framework for its application, including criteria for determining when an exposure decision is proportionate and how compliance with the obligation to take specific measures should be assessed. The ATKM is encouraged to, on the EU level, request clarification with regard to the application of this instrument in practice.

8. Structure the feedback of trend knowledge to chain partners

The ATKM develops valuable knowledge regarding terrorist content online, narratives and trends. However, this knowledge is not yet systematically fed back to partners such as the National Police and the National Coordinator for Security and Counterterrorism (NCTV). Establishing periodic reporting arrangements or feedback mechanisms would strengthen the position of the ATKM within the wider governance framework and increase the broader societal value of its work.

9. Increase the visibility of the reporting portal and analyse incoming reports

The ATKM's public reporting portal for third parties, including citizens, civil society organisations and researchers, was launched in November 2025.[4] However, as of June 2026, very little communication has taken place regarding its existence. More active promotion of the reporting portal, combined with the establishment of an analytical framework for incoming reports, including reports that do not ultimately qualify as terrorist content online, would strengthen both the detection capabilities of the ATKM and its ability to learn from incoming information.

---

3 Hashlists are digital fingerprints of already identified material.

4 The portal is available through this link.