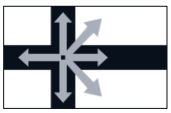


| NORDIC SECURITY ADVISORY | | |
|---|---|---|
| 12 February 2026 | RELEASABLE (*PUBLIC*)<br>~~RESTRICTED (*CUI*)~~<br>~~SECRET (*SECRET*)~~ | This report is an analytical product and does not constitute operational or policy directives. For more information, please visit NordicSecurity.org. |

Nordic counterterrorism and counterintelligence agencies operate in a digital environment increasingly shaped by actors outside their legal jurisdiction. This report examines two distinct but interconnected vulnerabilities affecting investigative and institutional resilience. The first concerns access to digital evidence. Radicalisation, recruitment, and foreign intelligence activity now occur largely on commercial platforms headquartered outside Europe, making timely access to investigative data uncertain and often slow. The second concerns reliance on foreign-controlled digital infrastructure used by public institutions, particularly cloud services and communications platforms operated by U.S.-based providers.

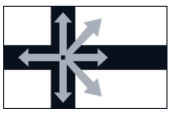
Using the Nordic region as a case study, the report analyses how these dependencies interact with highly digitalised societies, limited investigative resources, and fragmented legal frameworks governing cross-border evidence access. While current debates on technological sovereignty increasingly address infrastructure dependence, the investigative challenges posed by platform-controlled digital environments remain less resolved. The report concludes with policy recommendations aimed at strengthening Nordic cooperation, improving digital investigative capabilities, and addressing the gap between evolving digital threats and existing institutional responses.

# BEYOND REACH: PLATFORM AND INFRASTRUCTURE DEPENDENCIES IN NORDIC COUNTERTERRORISM AND COUNTERINTELLIGENCE

RADICALISATION TO POTENTIAL PROSECUTION AND WHAT LIES BETWEEN

Kara Liblick

## Table of Contents



# 1. Executive Summary

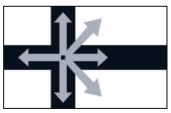
European counterterrorism and counterintelligence agencies operate in a digital environment largely controlled by actors outside their legal jurisdiction. Two distinct forms of dependency arise from this reality. The first concerns the platforms on which radicalisation, recruitment, and foreign intelligence activity occur. Evidence relevant to investigations increasingly resides on commercial services headquartered outside Europe, governed by foreign legal frameworks that do not oblige timely cooperation with European authorities. The second concerns the infrastructure on which public institutions themselves operate. Across Europe, including the Nordic region, government communications, data storage, and administrative systems rely heavily on cloud and productivity platforms owned by foreign companies and subject to foreign legal authority.

These two dependencies are structurally different and require different responses. Platform dependency concerns investigative access to digital evidence and the ability of security services to monitor and disrupt threat activity that unfolds online. Infrastructure dependency concerns institutional resilience and the risk that a foreign legal authority could disrupt the services on which public institutions rely. Recent political debates in Europe have focused primarily on the second problem, often framed under the concept of technological sovereignty. The first problem, which directly affects the ability of counterterrorism and counterintelligence agencies to investigate threats, has received considerably less attention.

The Nordic region illustrates both vulnerabilities in particularly clear form. Finland, Sweden, Norway, Denmark, and Iceland are among the most digitally connected societies in the world. Government services are highly digitised, public institutions rely extensively on foreign cloud infrastructure, and online platforms play a central role in social and political life. At the same time, the region faces significant geopolitical exposure. Finland and Sweden have both identified Russian intelligence activity as a persistent concern, while digital environments increasingly serve as venues for radicalisation, recruitment, and influence operations targeting younger populations.

Legal and institutional frameworks governing access to digital evidence further complicate this landscape. While the European Union has introduced new mechanisms intended to improve investigative access to electronic evidence, their benefits are unevenly distributed across the Nordic region due to differences in EU membership and legal opt-outs. At the same time, initiatives aimed at reducing technological dependency focus primarily on government infrastructure rather than on the platforms where threat activity occurs.

This paper examines these dynamics in four parts. It first analyses how radicalisation, recruitment, and foreign intelligence operations unfold across digital platforms and why the architecture of these platforms complicates investigation. The second section examines the mechanisms through which European authorities seek access to platform-held evidence and the limitations of existing legal frameworks. The third section analyses the Nordic configuration specifically, including regional legal arrangements and emerging efforts to reduce technological dependency. The paper concludes with policy



recommendations aimed at addressing the gap between current institutional capabilities and the digital environment in which contemporary security threats develop.

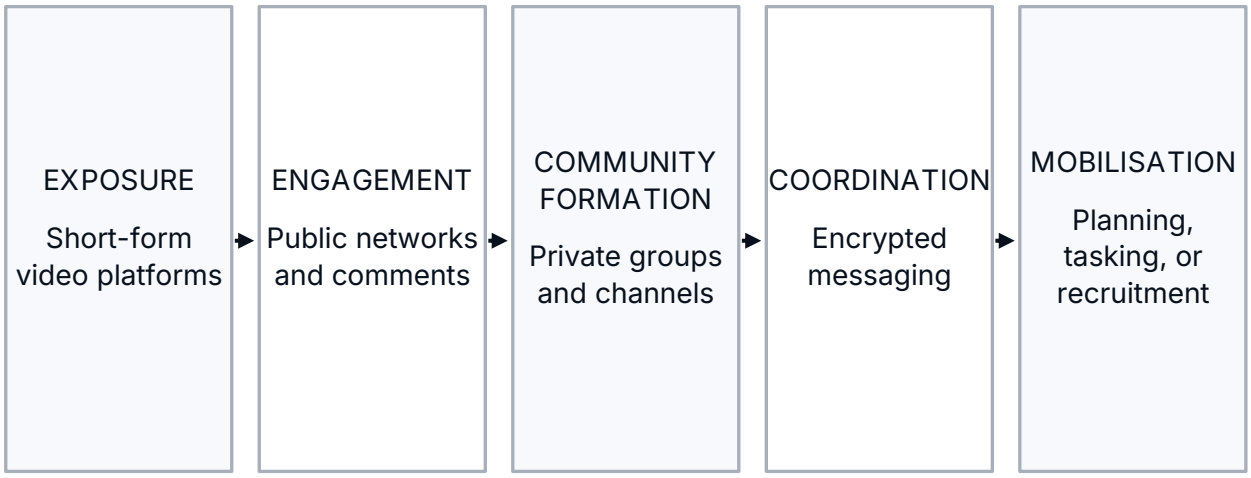
## 2. Online Radicalisation, Recruitment, and Foreign Intelligence Exploitation

Radicalisation, recruitment, and elements of foreign intelligence activity increasingly unfold within digital environments. Online platforms are not simply channels through which these processes occur. Their technical architecture actively shapes how individuals encounter ideological content, form relationships, and transition from passive engagement to operational involvement. Algorithm-driven recommendation systems promote emotionally engaging material and repeatedly expose users to similar content based on previous interactions. Short-form video platforms are particularly effective in this respect, as their design prioritises rapid content consumption and sustained engagement, often reaching younger audiences at scale.

The progression from exposure to mobilisation now commonly follows a recognisable digital pathway. Initial contact often occurs on open social platforms where extremist narratives, propaganda, or politically manipulative content circulate widely. Individuals who engage with such material may then be drawn into smaller communities through private messaging applications or closed online groups, where relationships can be developed, and ideological reinforcement becomes more intensive. The final stages frequently occur within encrypted communication environments, where coordination, operational planning, or direct tasking can take place with limited visibility to authorities.

# Online radicalisation and recruitment pathway

Threat activity often migrates from open discovery spaces to private and encrypted coordination environments. The pathway is indicative: specific platforms vary by case and jurisdiction.




## Visibility to investigators typically decreases as interaction moves from open platforms to encrypted services.

For counterterrorism and counterintelligence agencies, this migration across platforms creates significant investigative challenges. Evidence relevant to an investigation is rarely located within a single service. Instead, communications, behavioural indicators, and network connections are dispersed across multiple platforms, each operating under different legal jurisdictions and requiring separate access procedures. Establishing a coherent investigative picture, therefore, depends on timely access to data held by several providers, a process that is often slow and legally complex.

The scale of this phenomenon is reflected in arrest patterns across Europe. Europol's Terrorism Situation and Trend Report for 2024 noted that nearly one-third of individuals arrested for terrorism-related offences in EU member states were minors or young adults[1]. The statistic highlights how thoroughly digital environments have become the primary

[1] Europol, June 2025, "European Union Terrorism Situation and Trend Report 2025 (EU TE-SAT)", available at: https://www.europol.europa.eu/media-press/newsroom/news/new-report-major-developments-and-trends-terrorism-in-europe-in-2024

arena for early-stage ideological exposure and recruitment. In many cases, the earliest signs of mobilisation exist only in platform-held data such as account interactions, message histories, and behavioural metadata.

The same digital ecosystems that enable extremist radicalisation are also increasingly exploited by state-linked actors. Online environments enable recruiters to identify potential targets, build trust gradually, and conduct recruitment processes across borders without requiring physical proximity. The absence of direct contact during early stages reduces operational risk and allows recruitment pipelines to develop largely outside the reach of traditional surveillance methods. As a result, the digital terrain in which contemporary threats emerge has shifted significantly faster than the investigative frameworks designed to monitor it.

## 2.1. The Radicalisation-to-Mobilisation Arc

The process through which individuals move from initial exposure to extremist narratives toward operational activity can be described as a radicalisation-to-mobilisation arc. In the digital environment, this progression increasingly unfolds within compressed timelines and across multiple online platforms. Recommendation algorithms play a central role in the early stages of this process. By prioritising emotionally engaging material and surfacing similar content repeatedly to users who have interacted with related themes, these systems expose individuals to ideological material without requiring deliberate searching.

Short-form video platforms are particularly effective at facilitating early exposure. Their design encourages rapid consumption of emotionally charged content and enables ideological messaging to reach younger audiences with little friction. Initial engagement with such material may be casual or exploratory, but repeated exposure can quickly draw individuals into communities where extremist narratives are normalised and reinforced.

As engagement deepens, individuals commonly migrate from open platforms into more private communication environments. Messaging applications and closed online groups allow relationships to form and ideological commitments to strengthen beyond the visibility of public moderation systems. The final stages of the radicalisation arc often occur within encrypted communication channels, where coordination, planning, and direct encouragement of violent action can take place with limited external visibility.

A key feature of this process is the compression of timelines. Where earlier radicalisation pathways often unfolded over extended periods, the digital environment can accelerate progression from ideological exposure to operational intent. Once individuals move into encrypted environments, the observable digital record becomes thinner, and the opportunity for intervention narrows significantly.

Case Study: Vienna Pride Parade Plot, Austria, 2023

In 2023, Austrian authorities disrupted a planned attack targeting the Vienna Pride Parade. Three suspects aged 14, 17, and 20 were arrested days before the event. Investigators determined that the individuals had self-radicalised online and had progressed from ideological exposure to operational planning within a relatively short

period. The suspects initially encountered extremist content on TikTok before migrating to Telegram and the encrypted messaging platform Threema, where they communicated with radical Islamist contacts and discussed the planned attack.

Authorities recovered plans involving an assault rifle, a machete, and the use of a vehicle to target participants in the parade. Throughout the radicalisation process, the suspects were not merely consumers of extremist material but active participants in its dissemination, producing and sharing content within their networks[2]. The case illustrates how platform migration and encrypted communication environments can rapidly reduce the visibility of emerging threats. It also demonstrates how critical early access to platform-held data can be in reconstructing networks, timelines, and contact structures during investigations.

The dynamics visible in the Vienna case are not unique to Austria. Similar platform migration patterns have been observed across multiple European jurisdictions. For investigators, the challenge lies not only in identifying individuals who may be progressing along the radicalisation arc, but also in accessing the digital evidence that documents how that progression occurs.

## 2.2. Foreign Intelligence Exploitation via Online Platforms

The same digital environments that facilitate extremist radicalisation are increasingly exploited by foreign intelligence actors seeking to recruit sources, influence individuals, or coordinate operations. Online platforms provide intelligence services with a recruitment environment that differs fundamentally from traditional approaches. Potential targets can be identified, assessed, and approached without geographic proximity, while relationships can be developed gradually within communities where interaction already appears normal.

Digital platforms also reduce the operational risk traditionally associated with intelligence recruitment. Early contact can occur under pseudonymous identities, allowing recruiters to assess a potential target's background, motivations, and vulnerabilities before revealing any organisational affiliation. Online environments make it possible to build trust incrementally over weeks or months while maintaining a degree of plausible deniability. Only once a relationship is established do interactions typically migrate to more private communication channels.

Gaming communities have proven particularly suitable for such approaches. Military simulation ("MilSim") games create environments where discussions of military equipment, tactics, and geopolitical conflicts are commonplace. Participants often form sustained online relationships, and the collaborative nature of gameplay can facilitate gradual trust-building. These characteristics provide recruiters with an opportunity to identify individuals who display relevant interests, technical skills, or ideological sympathies.

[2] Nicolas Stockhammer, CTC Sentinel (Combating Terrorism Center at West Point), July 2025, "From TikTok to Terrorism? The Online Radicalization of European Lone Attackers since October 7, 2023", available at: https://ctc.westpoint.edu/from-tiktok-to-terrorism-the-online-radicalization-of-european-lone-attackers-since-october-7-2023/

Case Study: Arma 3 Recruitment Pipeline, South Africa and Russia, 2024

In 2024, two South African men in their early twenties were recruited into Russian military service through interactions originating in the MilSim game Arma 3. A recruiter operating under the Discord username @Dash initiated contact within the gaming community and gradually developed a relationship with the individuals over several weeks. Communication subsequently moved beyond the game environment to messaging platforms, where discussions became more explicit.

The recruiter ultimately arranged an in-person meeting in Cape Town and facilitated contact with the Russian consulate. The two men later travelled to Russia via the United Arab Emirates and signed one-year military contracts near St Petersburg. One of the recruits was reported killed in combat in Ukraine's Luhansk region within five months of the initial online contact[3]. The case illustrates how online recruitment pipelines can transition from virtual environments to real-world operational outcomes while passing through multiple jurisdictions and digital platforms.

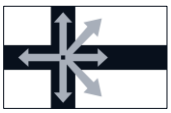
The methods visible in this example are not geographically constrained. The same recruitment model could be applied to targets in other regions where gaming communities and digital social networks are widely used. Nordic societies, characterised by high levels of digital connectivity and strong participation in online gaming cultures, present a comparable environment in which similar approaches could be employed.

Recent incidents in the Nordic region suggest that online recruitment may also play a role in lower-level tasking operations. In March 2026, Finnish media reported a suspected arson attack targeting a residential building in Helsinki that housed a Ukrainian support organisation. Preliminary investigations indicated that the two suspects, both teenagers, may have been recruited through financial incentives offered online. While the investigation was ongoing, the case highlights how digital environments can facilitate recruitment for activities that range from sabotage and harassment to more serious acts of violence[4].

Across both extremist and intelligence recruitment contexts, a common investigative challenge emerges. Online identities are frequently pseudonymous, communication environments are fragmented across multiple platforms, and coordination often occurs within encrypted messaging systems. Establishing the identity of a recruiter, mapping a target's contacts, or reconstructing the sequence of interactions that led to mobilisation requires extensive cross-platform analysis and access to platform-held data. When such access depends on the cooperation of companies operating outside the jurisdiction of investigating authorities, the resulting delays can significantly hinder the ability of security services to detect and disrupt emerging threats.

[3] Bloomberg, January 2026, "Russia Recruited South Africans for Its War Using a Gaming App", available at: https://www.bloomberg.com/news/articles/2026-01-07/russia-recruited-south-africans-for-its-war-using-a-gaming-app

[4] Helsingin Uutiset, March 2026, "Lauttasaarelaisen pyöräliikkeen tulipaloa epäillään tilauskeikaksi", available at: https://www.helsinginuutiset.fi/paikalliset/9284957



## 3. Evidence, Infrastructure, and the Limits of EU Responses

The investigative barriers described in the previous section are not simply operational challenges. They reflect deeper structural constraints within the digital environment in which contemporary security threats develop. European counterterrorism and counterintelligence agencies increasingly depend on information held by private companies operating under foreign legal jurisdictions, while the public institutions that support their work rely on digital infrastructure controlled by the same external actors.

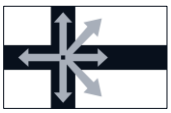
These two conditions represent distinct forms of dependency. The first concerns access to digital evidence held by online platforms, where extremist activity, recruitment, and foreign intelligence interactions frequently occur. The second concerns the technological infrastructure used by public institutions themselves, including cloud services, communications platforms, and administrative systems. Although both forms of dependency arise from the global concentration of digital services among a small number of multinational companies, they present different operational risks and require different policy responses.

European policy initiatives have begun to address aspects of these challenges, but their focus has been uneven. Measures aimed at improving access to electronic evidence attempt to reduce the investigative delays associated with cross-border data requests. At the same time, discussions of technological sovereignty increasingly focus on the risks associated with reliance on foreign-controlled cloud infrastructure. These debates are often treated as part of the same policy problem, yet the mechanisms required to address them differ significantly.

Investigative access to platform-held data depends on legal frameworks that can compel service providers to disclose relevant information in a timely manner. Institutional resilience, by contrast, depends on reducing the exposure of government systems to external legal authorities that could potentially disrupt critical digital services. While both issues involve the intersection of law, technology, and geopolitics, they operate at different layers of the digital ecosystem.

Understanding this distinction is essential for evaluating the effectiveness of current European responses. Policies designed to strengthen technological sovereignty may reduce institutional vulnerability to external pressure but do little to improve investigators' access to the digital environments where radicalisation, recruitment, and influence operations occur. Conversely, legal reforms aimed at improving evidence access do not address the broader infrastructural dependencies that shape how public institutions operate.

The following sections examine these two dimensions in greater detail. The first considers the legal mechanisms through which European authorities attempt to obtain digital evidence from foreign-based platforms and the limitations inherent in those processes. The second examines the implications of relying on foreign-controlled cloud infrastructure for the functioning of European public institutions.



## 3.1. The Evidence Access Problem

A fundamental challenge for European counterterrorism and counterintelligence investigations is that much of the relevant digital evidence is held by private companies operating outside the legal jurisdiction of investigating authorities. Communications data, account activity, and behavioural indicators are typically stored on platforms headquartered abroad, particularly in the United States. Investigators, therefore, cannot compel access to this information directly through domestic legal mechanisms.

Access to data held by U.S.-based service providers generally occurs through Mutual Legal Assistance Treaty (MLAT) procedures. Under this framework, requests for evidence must be transmitted through national justice ministries to the U.S. Department of Justice's Office of International Affairs (OIA). The request is then evaluated against the terms of the applicable treaty as well as U.S. legal standards governing the disclosure of electronic communications data. In many cases, the process requires the requesting authority to demonstrate dual criminality and to meet evidentiary thresholds comparable to those required for search warrants under U.S. law[5].

While the MLAT system provides a formal legal pathway for cross-border evidence gathering, it was designed primarily to support criminal prosecutions rather than time-sensitive security investigations. Requests often require detailed documentation and may involve additional clarification before processing begins. As a result, response times can extend for weeks or months. In counterterrorism and counterintelligence contexts, however, the value of digital evidence is often greatest during the early stages of an investigation, before probable cause has been established and before a threat becomes imminent.

In practice, investigators frequently attempt to obtain information through voluntary cooperation with platform providers. Major technology companies maintain law enforcement response processes and publish transparency reports outlining the number and type of government requests they receive. These channels can sometimes produce faster results than formal MLAT procedures. However, they remain discretionary mechanisms governed by the internal policies of private companies rather than by binding legal obligations. A request that does not meet a platform's internal criteria for voluntary disclosure may simply be declined, and investigators have little recourse when this occurs.

The resulting system, therefore, combines two imperfect mechanisms. Formal legal procedures provide a clear framework but operate slowly and are ill-suited to time-sensitive investigations. Informal cooperation mechanisms may respond more quickly but are inconsistent and ultimately depend on corporate discretion. For security services attempting to reconstruct online networks or identify emerging threats, the combination often produces significant investigative delays.

[5] Official Journal of the European Union, July 2003, "Agreement on Mutual Legal Assistance between the European Union and the United States of America", available at:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22003A0719%2802%29

Example: TikTok's Project Clover and the Limits of Data Localisation

Recent debates surrounding data localisation illustrate the limits of current approaches to the evidence access problem. TikTok's Project Clover, a €12 billion initiative designed to store European user data within dedicated data centres in Europe, was introduced in response to regulatory concerns that Chinese engineers had accessed European user data remotely. Facilities in Norway and Ireland are already operational, and in 2025, the company announced plans to construct a further data centre in Kouvola, Finland[6].

The initiative aims to strengthen protections for European user data by ensuring that information is stored within the European regulatory environment and subject to independent cybersecurity oversight. However, data localisation addresses only one aspect of the broader problem. Relocating servers does not automatically grant European authorities stronger legal powers to compel access to the data stored within them. The corporate entity controlling the platform remains subject to its own national legal framework, and decisions about whether and how to respond to law enforcement requests continue to be governed by that framework.

The distinction between where data is stored and who has legal authority over it, therefore, remains critical. A data centre located within the European Union does not necessarily provide investigators with more reliable access to platform-held evidence if the company operating the platform is headquartered elsewhere and subject to foreign legal obligations. In this respect, data localisation initiatives address concerns about privacy and data protection but do not resolve the investigative challenges faced by counterterrorism and counterintelligence agencies.

## 3.2. Foreign Infrastructure and Operational Risk

The evidence-access problem discussed in the previous section concerns investigators' ability to obtain information from private platforms. A separate but related vulnerability arises from the infrastructure on which European public institutions themselves depend. Across Europe, government administrations increasingly rely on cloud services, communications platforms, and digital productivity tools operated by a small number of multinational technology companies headquartered outside the continent.

In the European cloud infrastructure market, providers such as Amazon Web Services, Microsoft Azure, and Google Cloud collectively hold a dominant position. Estimates vary across market analyses, but these companies together account for a large majority of Europe's commercial cloud services, while European providers represent a comparatively small share of the market[7]. This concentration means that many public institutions store

[6] TikTok Newsroom, 2025, "Project Clover: €1 Billion Investment in Finland for New Data Center", available at: https://newsroom.tiktok.com/en-eu/finlanddatacenter

[7] Synergy Research Group, July 2025, "European Cloud Providers' Local Market Share Now Holds Steady at 15%", available at: https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15

data, manage communications, and operate administrative systems on infrastructure ultimately subject to foreign legal authority.

One important legal framework shaping this environment is the United States' Clarifying Lawful Overseas Use of Data Act (CLOUD Act), adopted in 2018. The legislation enables United States authorities to compel American technology companies to provide data under their control regardless of where that data is physically stored. As a result, information held on infrastructure operated by companies based in the United States may be subject to legal demands issued by U.S. authorities even when the data is located within Europe[8].

The more immediate concern for public institutions, however, is not necessarily the possibility of data access by foreign authorities but the potential for service disruption. If the legal authority governing a technology provider requires the suspension of services to a particular organisation or individual, institutions dependent on those services may find themselves unable to contest the decision or secure an immediate alternative.

Case Study: The International Criminal Court Sanctions Episode, 2025

The experience of the International Criminal Court (ICC) in 2025 illustrates the potential consequences of such dependencies. The Court relied on Microsoft's cloud-based infrastructure to operate its institutional email and communications systems. In 2025, the United States imposed sanctions on certain ICC personnel. As a consequence of these sanctions, individuals designated under the measures lost access to services provided by companies based in the United States, including institutional email accounts.

The impact was immediate and operational rather than purely legal. The Court was forced to undertake an accelerated migration of its communications infrastructure to alternative providers, transferring large volumes of institutional data while simultaneously re-establishing administrative workflows and retraining staff[9]. The episode demonstrated how dependence on foreign-controlled digital services can create institutional vulnerability even in the absence of direct security breaches.

Attempts to develop European alternatives have encountered practical difficulties. The GAIA-X initiative, launched in 2020 as an effort to build a European cloud ecosystem, ultimately evolved into a standards and interoperability framework after major American providers joined the project. While the initiative contributed to discussions on data governance and interoperability, it also illustrated the challenge of establishing a competitive European infrastructure ecosystem in a market already dominated by global providers.

These dynamics have increasingly entered European policy debates under the concept of technological sovereignty. The central question is not merely whether data is stored within

[8] U.S. Congress, March 2018, "Clarifying Lawful Overseas Use of Data Act (CLOUD Act), H.R.4943", available at: https://www.congress.gov/bill/115th-congress/house-bill/4943
[9] Open Source Observatory (OSOR), November 2025, "International Criminal Court switches to open source with openDesk", available at: https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/news/international-criminal-court-invests-open-infrastructure

European territory, but whether public institutions retain control over the digital infrastructure on which their operations depend. While initiatives aimed at reducing such dependencies may strengthen institutional resilience, they do not directly address the separate problem of investigators' access to digital evidence held by online platforms.

## 4. The Nordic Configuration

The structural vulnerabilities described in the previous sections affect European security institutions broadly, but their implications are not uniform across the continent. The Nordic countries present a particularly revealing configuration of risk. Finland, Sweden, Norway, Denmark, and Iceland combine extremely high levels of digital connectivity with relatively small investigative agencies and a complex geopolitical environment. These characteristics make the region both highly exposed to digitally mediated threats and heavily dependent on international technological infrastructure.

Nordic societies consistently rank among the most digitally advanced in the world. Internet penetration is near universal, public services are extensively digitised, and online platforms play a central role in social interaction and information exchange. These conditions create an environment in which extremist propaganda, recruitment efforts, and foreign influence activities can spread rapidly through digital channels. At the same time, the digitalisation of public administration means that government institutions rely heavily on cloud services and digital infrastructure provided by international technology companies.

The region's geopolitical context further amplifies these vulnerabilities. Finland and Sweden have both identified Russian intelligence activity as a persistent concern, particularly following their accession to NATO. Nordic security services regularly report attempts by foreign actors to collect information, influence public debate, or identify potential recruitment targets. In such an environment, the ability to detect and investigate online activity at an early stage becomes particularly important.

At the same time, the Nordic countries occupy different legal positions within the European frameworks designed to improve access to digital evidence. Finland and Sweden participate fully in the European Union's criminal justice architecture. Denmark is a member of the EU but maintains opt-outs from certain justice and home affairs instruments. Norway and Iceland are outside the EU entirely, although they participate in several cooperative arrangements through the European Economic Area and other agreements. These differences affect how each country can access digital evidence held by foreign-based service providers and shape the practical investigative tools available to national authorities.

The Nordic region, therefore, illustrates how the broader European challenges discussed in earlier sections manifest within a specific regional context. Two dimensions are particularly relevant. The first concerns the legal and institutional barriers Nordic investigators face when attempting to obtain digital evidence from foreign-based platforms. The second concerns the emerging political debate within the region about

reducing reliance on foreign-controlled digital infrastructure. The following subsections examine each of these dynamics in greater detail.

## 4.1. Barriers to Digital Evidence Access in the Nordic Region

All Nordic countries rely heavily on cross-border legal cooperation mechanisms to obtain digital evidence held by foreign-based service providers. In practice, this often means relying on Mutual Legal Assistance Treaty (MLAT) procedures when requesting information from companies headquartered in the United States. Requests are typically transmitted from national justice ministries to the U.S. Department of Justice's Office of International Affairs, where they are evaluated under applicable treaty provisions and U.S. legal standards. As discussed earlier, this process can involve significant delays and was originally designed to support criminal prosecutions rather than time-sensitive security investigations.

While this reliance on MLAT procedures is shared across the Nordic region, the five countries occupy different legal positions with respect to emerging European mechanisms intended to improve digital evidence access. Finland and Sweden participate fully in the European Union's criminal justice architecture and are therefore covered by the EU's e-Evidence Regulation, which is scheduled to apply from 2026. The regulation allows judicial authorities within EU member states to issue European Production Orders requiring service providers operating within the EU to disclose certain categories of electronic evidence within specified timeframes[10].

Denmark, although a member of the European Union, maintains opt-outs from several justice and home affairs instruments, including those relating to cross-border criminal procedure. Norway and Iceland, meanwhile, are not members of the EU and therefore fall outside the direct scope of the regulation. As a result, the Nordic countries collectively occupy three different legal positions regarding the framework intended to accelerate evidence access within the European Union.

The e-Evidence Regulation represents a meaningful improvement for those countries able to use it. The mechanism allows authorities to request certain forms of electronic evidence directly from service providers without relying on traditional MLAT channels, potentially reducing response times. The regulation also requires service providers offering services within the EU to designate legal representatives responsible for receiving and responding to such orders. In urgent situations, the framework includes accelerated procedures intended to provide data within hours rather than weeks.

Despite these improvements, the regulation does not resolve the structural challenge discussed earlier in the paper. Its effectiveness depends on the existence of a service provider with a legal presence in the European Union that can be compelled to respond to an order. Many of the platforms most frequently associated with extremist activity,

[10] Official Journal of the European Union, July 2023, "Regulation (EU) 2023/1543 of the European Parliament and of the Council on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings", available at: https://eur-lex.europa.eu/eli/reg/2023/1543/oj/eng

encrypted communications, or emerging online communities operate with minimal formal presence within EU jurisdiction or have historically demonstrated limited responsiveness to regulatory demands.

Furthermore, the uneven applicability of the regulation within the Nordic region creates a potential asymmetry in investigative capabilities. If Finland and Sweden gain faster access to certain forms of digital evidence while neighbouring jurisdictions remain reliant on slower mechanisms, actors seeking to exploit online environments may simply shift activities toward jurisdictions where investigative access remains more constrained. In such circumstances, differences in legal frameworks do not eliminate recruitment pipelines or influence operations but may influence where they emerge and how they evolve.

For Nordic security services, these dynamics underscore the continuing importance of international cooperation and cross-border investigative coordination. While legal reforms may improve access to digital evidence in some jurisdictions, the platforms on which online recruitment and influence operations occur remain global in scope. As a result, investigative effectiveness often depends on the ability of agencies across multiple countries to combine information, reconstruct cross-platform networks, and respond collectively to emerging threats.

## 4.2. Momentum toward Technological Sovereignty

Alongside the challenges associated with access to digital evidence, Nordic governments have increasingly begun to debate a separate issue: the strategic implications of relying on foreign-controlled digital infrastructure. In policy discussions, this concern is often framed in terms of technological sovereignty, referring to the ability of states and public institutions to maintain operational control over the digital systems on which they depend.

These debates focus primarily on the administrative and institutional layers of government. Public administrations across Europe rely extensively on cloud computing platforms, email systems, and digital productivity tools provided by a small number of multinational technology companies. When those services operate under the legal authority of foreign jurisdictions, governments face the possibility that political or legal developments outside their control could affect access to critical digital infrastructure.

Within Nordic policy discussions, the possibility that foreign authorities could disrupt digital services used by public institutions is increasingly treated as a plausible strategic vulnerability rather than a theoretical risk. Governments are therefore exploring ways to diversify suppliers, strengthen domestic infrastructure capabilities, or shift certain functions toward providers operating under European legal frameworks.

Case Study: Denmark's Infrastructure Transitions, 2025

Denmark has moved particularly quickly in this direction. In 2025, the Danish Ministry of Digital Affairs began reducing its reliance on Microsoft Office 365 within parts of the public administration. The transition was motivated by a combination of factors, including concerns about supplier concentration, cost structures, and long-term strategic autonomy. The issue gained additional political attention in early 2026, when public

debate intensified following discussions in the United States regarding the potential acquisition of Greenland.

Danish Digital Minister Caroline Stage Olsen stated publicly that the country's public digital infrastructure had become overly dependent on a small number of foreign suppliers and that this concentration represented a vulnerability. Several municipalities, including Copenhagen and Aarhus, subsequently initiated their own transitions toward alternative digital platforms. During the same period, privacy-focused technology provider Proton reported a sharp increase in Danish users seeking alternatives to established services, based on its own internal user data[11][12].

The Danish case illustrates how technological sovereignty debates can rapidly shift from abstract strategic discussions to concrete policy decisions when geopolitical tensions highlight the potential risks associated with digital dependency.

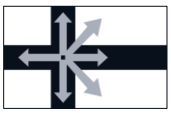
At the same time, it is important to distinguish between the types of systems affected by such transitions. Intelligence and security services generally avoid relying on commercial cloud infrastructure for their most sensitive operational systems. Their exposure to foreign-controlled infrastructure tends instead to occur at institutional interfaces, such as administrative systems, communications platforms used for interagency coordination, or digital services operated at the ministerial level.

For this reason, initiatives aimed at strengthening technological sovereignty may reduce certain institutional vulnerabilities without addressing the investigative challenges discussed earlier in the paper. The core difficulty facing counterterrorism and counterintelligence agencies lies not in where government data is stored but in the platforms where threat activity occurs. Radicalisation networks, recruitment pipelines, and influence operations unfold within digital ecosystems controlled by private companies operating under foreign legal jurisdictions.

Data localisation initiatives illustrate this distinction clearly. Relocating servers to European territory may strengthen data protection and regulatory oversight, but it does not necessarily grant European authorities stronger powers to compel access to platform-held information. The fundamental issue remains one of jurisdiction and corporate control rather than physical infrastructure.

As a result, the technological sovereignty initiatives now gaining momentum across the Nordic region address only one layer of the broader digital dependency described in this paper. While infrastructure diversification may enhance institutional resilience, it does not directly improve investigators' ability to access the online environments where contemporary security threats increasingly emerge.

[11] The Record (Recorded Future News), June 2025, "Danish government agency to ditch Microsoft software in push for digital independence", available at: https://therecord.media/denmark-digital-agency-microsoft-digital-independence
[12] Proton, February 2026, "Europe is ready to ditch US tech for private alternatives", available at: https://proton.me/blog/european-alternative-us-tech-survey



# 5. Recommendations

The analysis presented in this paper highlights two distinct vulnerabilities affecting Nordic counterterrorism and counterintelligence capabilities: dependence on foreign-controlled platforms for access to digital evidence and dependence on foreign-controlled infrastructure for the operation of public institutions. Addressing these challenges requires policy responses that operate at multiple levels, including national institutions, Nordic regional cooperation, and European regulatory frameworks.

## A. Strengthen Nordic Cooperation on Digital Investigations

The Nordic countries share a highly digitalised social environment and face similar threat dynamics in online spaces. At the same time, differences in legal frameworks governing digital evidence access create uneven investigative capabilities across the region. Strengthening operational cooperation between Nordic security services could help mitigate these asymmetries.

Joint analytical capabilities focused on digital environments could enable agencies to combine information about recruitment pipelines, online networks, and emerging threat communities. Shared investigative teams or regional coordination structures could facilitate cross-border analysis of platform-based activity that frequently spans multiple jurisdictions. Such cooperation would also reduce the likelihood that threat actors exploit differences in legal frameworks by shifting activity toward jurisdictions with slower evidence-access mechanisms.

## B. Expand Cross-Platform Digital Investigative Capabilities

Online recruitment pipelines increasingly unfold across multiple digital environments, including social media platforms, gaming communities, and encrypted messaging services. Effective investigation, therefore, requires the ability to reconstruct interactions that span several platforms simultaneously.

Nordic security services should invest in analytical capabilities capable of mapping cross-platform networks, correlating behavioural indicators, and identifying emerging communities in online environments. Open-source intelligence analysis, data science methods, and machine-assisted pattern detection may all contribute to strengthening early-stage detection of recruitment activity and foreign influence operations.

Such capabilities should complement rather than replace traditional investigative methods, enabling agencies to identify potential threats earlier in the radicalisation or recruitment process.

## C. Develop Structured Engagement with Major Digital Platforms

Access to platform-held data remains a central challenge for investigators. While formal legal frameworks such as MLAT procedures provide a structured pathway for obtaining evidence, voluntary cooperation from technology companies continues to play an important role in many investigations.

Nordic governments could benefit from developing more systematic engagement mechanisms with major digital platforms. Dedicated liaison structures, technical contact points, and coordinated communication channels could improve the efficiency of lawful data requests and reduce delays associated with informal cooperation processes.

Such engagement should operate alongside existing legal frameworks rather than replacing them, ensuring that investigative cooperation remains consistent with national and European legal standards.

### D. Support European Efforts to Improve Digital Evidence Access

The European Union's e-Evidence Regulation represents a significant step toward improving cross-border access to electronic evidence within the EU. However, its effectiveness will depend on the extent to which service providers comply with its provisions and the degree to which it can be integrated into existing international legal frameworks.

Nordic governments should support continued development of mechanisms that enable faster and more reliable access to digital evidence, such as the Europol-Eurojust jointly implemented SIRIUS project, particularly in time-sensitive counterterrorism and counterintelligence investigations. At the same time, policymakers should recognise the limitations of purely legal solutions when dealing with global technology companies operating across multiple jurisdictions.

Strengthening cooperation with international partners and encouraging greater transparency in platform responses to lawful requests may help mitigate some of these challenges.

### E. Integrate Security Considerations into Technological Sovereignty Initiatives

Debates surrounding technological sovereignty in Europe have largely focused on administrative resilience and the risks associated with reliance on foreign-controlled cloud infrastructure. While these concerns are legitimate, security-sector implications should also be considered.

Efforts to diversify suppliers or strengthen European digital infrastructure should take into account the needs of law enforcement and intelligence agencies. Secure communications systems, data management environments, and interagency coordination platforms must remain resilient in the face of geopolitical pressures while supporting the operational requirements of security services.

Ensuring that such initiatives incorporate security-sector perspectives from the outset may help prevent future dependencies that limit institutional autonomy.

### F. Maintain a Clear Distinction Between Platform and Infrastructure Dependencies

Finally, policymakers should recognise that the vulnerabilities described in this paper arise from two different layers of the digital ecosystem. Infrastructure diversification may

strengthen institutional resilience, but it does not directly improve investigators' access to the platforms where radicalisation, recruitment, and influence operations occur.

Addressing both issues effectively, therefore, requires distinct policy approaches. Treating them as a single technological sovereignty problem risks overlooking the specific investigative challenges that digital platforms present for counterterrorism and counterintelligence agencies.

## 6. Conclusion

The digital environment in which contemporary security threats emerge has evolved faster than the institutional frameworks designed to address them. Radicalisation pathways, recruitment pipelines, and foreign influence operations increasingly develop within online platforms that operate outside the legal jurisdiction of the authorities responsible for investigating them. At the same time, the public institutions responsible for national security rely heavily on digital infrastructure provided by a small number of multinational technology companies operating under foreign legal authority.

These two conditions represent distinct forms of dependency. Platform dependency concerns the ability of investigators to access digital evidence held by private companies and to monitor the online environments where recruitment and mobilisation occur. Infrastructure dependency concerns the resilience of public institutions whose communications systems, administrative platforms, and digital services rely on external providers. Although both challenges arise from the global concentration of digital services, they affect different layers of the security ecosystem and require different policy responses.

Across Europe, debates about technological sovereignty have begun to address the second issue. Governments are increasingly aware that reliance on foreign-controlled infrastructure can expose public institutions to strategic pressure or disruption. The Nordic countries, characterised by highly digitised societies and strong reliance on digital public services, have become active participants in this debate. Efforts to diversify suppliers and strengthen European digital infrastructure represent an important step toward reducing institutional vulnerability.

Yet these initiatives do not resolve the investigative challenges associated with digital platforms. The environments in which radicalisation, recruitment, and influence operations occur remain largely outside the direct legal reach of European authorities. Access to relevant evidence depends on complex cross-border legal processes and, in many cases, on voluntary cooperation from private companies operating under different legal frameworks.

For counterterrorism and counterintelligence agencies, the consequence is a growing gap between the digital terrain where threats develop and the institutional mechanisms available to monitor and disrupt them. Online recruitment pipelines can span multiple platforms and jurisdictions within days, while legal mechanisms for obtaining evidence often operate on timescales measured in weeks or months. In a security environment

characterised by hybrid pressure, rapid mobilisation, and digitally mediated influence operations, this gap carries increasing strategic significance.

The Nordic region illustrates how these dynamics interact within a highly connected and geopolitically exposed environment. Differences in legal frameworks governing evidence access coexist with shared digital ecosystems and shared exposure to foreign influence activity. As policymakers continue to address questions of technological sovereignty and digital resilience, ensuring that counterterrorism and counterintelligence requirements remain central to these discussions will be essential.

The digital terrain of contemporary security competition will continue to evolve. Whether the institutional frameworks designed to protect democratic societies can adapt at the same pace remains an open question.