Untrusted Streams:

Illegal IPTV, Organised Crime and the Emerging Threat to Nordic Security and Democratic Resilience

Prepared for

Nordic Content Protection

Prepared by

Professor Paul Watters OAM and Associate Professor Joel Scanlan

September 2026

Executive Summary

Illegal IPTV is no longer merely a copyright-enforcement problem. At Nordic scale, it constitutes a parallel, untrusted distribution infrastructure operating outside normal regulatory, security and editorial controls. More than 1.5 million households across Denmark, Finland, Norway and Sweden had access to illegal IPTV in spring 2025, creating a substantial recurring audience beyond the visibility and control of lawful broadcasters. This scale sustains criminal revenue, exposes consumers and devices to measurable cybersecurity risks, and creates an emerging hybrid-threat surface relevant to Nordic security and democratic resilience.

The assessment identifies two established harms and one emerging strategic risk. Organised-crime financing is supported by evidence of professional subscription businesses, reseller networks, fragmented payments, cross-border infrastructure and substantial unlawful revenue. Cybersecurity exposure is likewise well established: illegal streaming sites, applications and devices expose consumers to malware, phishing, credential theft, tracking, botnet activity and residential-proxy abuse. Consumer demand gives both harms scale by sustaining the commercial infrastructure and the large, habitual audience on which the ecosystem depends.

The emerging national-resilience risk arises from the distribution layer itself. Illegal IPTV services can reproduce trusted Nordic channels, programmes, presenters, logos and interfaces while operating outside the broadcaster's authentication, provenance, editorial and incident-response controls. A hostile state, proxy or criminal intermediary could therefore exploit the unauthorised distribution layer to alter the version of a trusted channel received by subscribers without needing to compromise the lawful broadcaster itself. The authentic broadcaster feed could remain intact while an altered version circulates through an illegal service that the broadcaster neither controls nor necessarily observes.

The consequences become most significant during elections, military escalation, major cyber incidents and national emergencies. An altered news segment, false emergency warning, fabricated government or military announcement, deceptive subtitle, overlay or synthetic presenter could create a short period of confusion before authoritative correction reaches the affected audience. The strategic effect need not depend on lasting persuasion: uncertainty, delayed correction and temporary loss of trust during a sensitive event may themselves be consequential. The substantive analysis identifies these as credible manifestations of the emerging pathway.

The central national-resilience finding is that the relevant infrastructure, audience reach, technical capabilities, hostile intent and demonstrated analogue cases already exist. Russian information activity targeting the Nordic-Baltic region is established; audiovisual manipulation techniques are demonstrated; synthetic-media capability is becoming cheaper and more accessible; and uncontrolled IPTV distribution environments already reach substantial audiences. Direct NCP testing and Baltic evidence also show Russian and Kremlin-backed audiovisual content circulating through uncontrolled IPTV and online distribution channels. Their convergence establishes a credible emerging threat pathway through which trusted Nordic broadcaster identities could be exploited, warranting monitoring, preparedness and proportionate intervention before the first documented Nordic incident occurs.

The report draws on 178 research papers, industry reports and other evidence sources, supplemented by direct technical evidence supplied by Nordic Content Protection. Using a structured risk-evidence framework, the overall level of concern is assessed as High Risk. This finding is not based on treating every illegal IPTV service as a national-security threat. Rather, the strategic concern lies in the subset of services where substantial audience reach, criminal monetisation, unsafe technology, opaque control and manipulation capability converge. Russia is the most relevant current state-threat lens for the Nordic region, while the underlying vulnerability is actor-neutral and could be exploited by other state or non-state actors.

The policy implication is clear: reducing illegal IPTV demand also reduces criminal revenue, consumer cyber exposure and the scale of the untrusted audience available for future exploitation.

Nordic governments and industry should, therefore, with urgency:

1. prohibit and proportionately penalise the knowing purchase or acquisition of illegal IPTV access, with clear knowledge thresholds and safeguards;
2. enable rapid and dynamic blocking of illegal services, domains, applications, playlists and replacement infrastructure;
3. strengthen coordinated action against resellers, applications and devices, marketplace pathways and financial infrastructure that enable the ecosystem; and
4. ensure that high-risk illegal IPTV ecosystems are incorporated into relevant cybersecurity, organised-crime, foreign-interference and national-resilience assessments.

These measures should be evidence-led, proportionate and designed to reduce both consumer demand and the operational resilience of the highest-risk services.

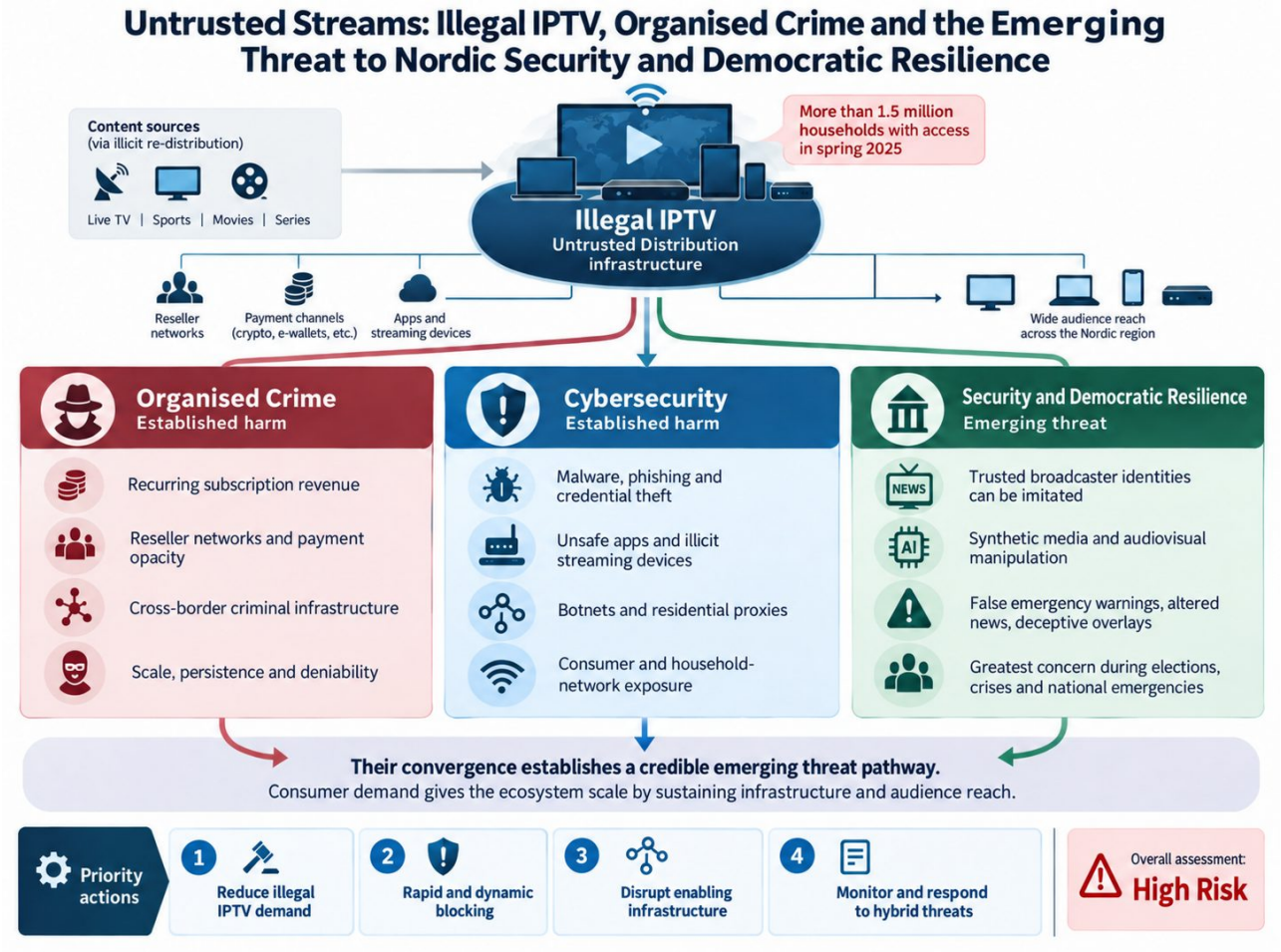

Table of Contents

1. Introduction, Scope and Method

This section defines the report's purpose, scope and methodology, and explains how illegal IPTV and the wider illegal streaming ecosystem create established organised-crime and cybersecurity harms alongside an emerging media-integrity and national-resilience risk.

1.1 Purpose of this report

Illegal IPTV is often treated primarily as a copyright-enforcement and consumer-protection problem. Yet illegal IPTV services, piracy websites, illegal streaming applications and illicit streaming devices also expose users to malware, fraud and credential theft, while unlawful subscription and advertising models generate recurring revenue and sustain criminal commercial infrastructure [CYB-001, CYB-012, OCF-023, OCF-030].

This report examines the security implications of those established harms in a changed regional environment following Russia's invasion of Ukraine and the accession of Finland and Sweden to NATO. It also assesses a distinct emerging risk: whether an untrusted distribution layer that reproduces familiar broadcaster identities could be exploited for altered or synthetic audiovisual content. The central finding is that illegal IPTV creates an untrusted distribution ecosystem combining audience reach, commercial opacity and technical exposure. Illegal IPTV already provides an observed distribution pathway for Russian and Kremlin-backed audiovisual content. The emerging strategic risk is the next step: exploitation of that untrusted distribution layer to manipulate content that viewers believe originates from a trusted Nordic broadcaster. The manipulation pathway is credible and strategically significant.

1.2 Core proposition

The report's central proposition is that illegal IPTV creates an untrusted distribution ecosystem operating outside normal regulatory, security and editorial controls. Organised-crime financing and cybersecurity exposure are established harms; media-integrity and AI-enabled manipulation are emerging strategic risks. Consumer demand provides recurring revenue and audience reach, while unsafe applications, devices and opaque distribution arrangements can provide technical access and concealment [CYB-001, CYB-043, CYB-048, OCF-023, OCF-030, OCF-052–OCF-056].

Real-world analogues illustrate why audience targeting, trusted interfaces and rapid amplification matter, without constituting direct evidence about Nordic illegal IPTV. The Cambridge Analytica controversy showed how audience data and microtargeting could be assembled for tailored political messaging, while the European Commission's 2023 scrutiny of TikTok during the Israel-Hamas conflict focused on crisis-response measures and the risk of amplification of illegal content and disinformation. These examples are used only as analogues for targeting, manipulation and amplification, not as evidence that Nordic illegal IPTV services have been used in the same way (UK House of Commons Digital, Culture, Media and Sport Committee, 2019; European Commission, 2023). Together, these analogues demonstrate how trusted identities, targeted audiences and third-party distribution infrastructure can be exploited; the emerging IPTV risk is that these capabilities could converge within an already-established untrusted audiovisual distribution channel.

In this report, the *Nordic countries* refers to Denmark, Finland, Iceland, Norway and Sweden.

1.3 The three-pillar assessment

The report is organised around three pillars: organised-crime financing as an established harm; cybersecurity exposure as an established harm; and media-integrity and AI-enabled manipulation as an emerging strategic risk. The detailed chapters assess these dimensions separately before considering their convergence.

Organised crime: the established scale and persistence harm

Organised-crime financing (Chapter 5) describes how illegal IPTV and related unlawful streaming markets convert consumer demand into subscriptions, reseller commissions, advertising income and fragmented payments. These mechanisms support professional, cross-border commercial networks and

can obscure operators and beneficiaries [OCF-013, OCF-020, OCF-023, OCF-030]. Where such systems intersect with Russian or other state-exposed criminal networks, they may also acquire strategic utility; such links must be demonstrated rather than assumed [OCF-052–OCF-056].

Cybersecurity: the established access-layer harm

Cybersecurity exposure (Chapter 4) is mature and well established. Piracy sites, illegal IPTV services, streaming applications and illicit streaming devices expose users and networks to malware, phishing, credential theft, tracking and botnet or proxy abuse. Within the compound-risk analysis, these weaknesses form a technical access layer through which compromised devices and infrastructure may support wider criminal or hostile activity [CYB-001, CYB-008, CYB-012, CYB-024, CYB-040, CYB-048].

Media integrity and AI-enabled manipulation: the emerging strategic risk

Media-integrity and AI-enabled manipulation is the report's emerging forward risk. Russian or other hostile actors could in principle exploit unofficial viewing environments to distribute altered broadcasts, overlays, subtitles or crisis messaging, while generative AI lowers the cost of producing and localising synthetic content [DIS-018, DIS-022, DIS-045–DIS-047]. This domain assesses a credible pathway rather than an observed Nordic illegal IPTV harm [DIS-016, DIS-031–DIS-034].

1.4 Scope and Assumptions

This report examines the illegal streaming ecosystem serving Nordic audiences, including illegal IPTV services, piracy sites, illicit streaming devices, streaming applications, cloned interfaces, cyberlockers, advertising networks, reseller systems and related technical and financial services. Its focus is not copyright infringement generally, but the convergence of established cyber and criminal harms with an emerging media-integrity risk.

The assessment focuses on the subset of illegal streaming systems in which criminal monetisation, technical exposure, opaque control or state-relevant capabilities converge. Russian or Russian-aligned activity is assessed where supported by evidence of cyber capability, criminal networks, infrastructure or information operations.

1.5 Method

A purposive evidence-selection strategy was used to identify material relevant to the security risks associated with illegal IPTV and wider illegal streaming infrastructure in the Nordic region. The review was not confined to copyright-piracy research, but extended across three distinct evidence domains: cybersecurity, including malware, compromised devices, botnets, residential proxies and malicious advertising; organised-crime financing, including illegal IPTV markets, reseller structures, payment channels, cryptocurrency and money laundering; and media-integrity risk, including synthetic media, impersonation, broadcast interference, disinformation and crisis communications.

Searches were conducted across major academic databases and open-source repositories, including Scopus, Google Scholar, government and law-enforcement publications, cybersecurity advisories, threat-intelligence reporting and relevant industry research. Search terms combined illegal-streaming concepts, including *illegal IPTV*, *piracy applications*, *illicit streaming devices* and *cyberlockers*, with terms such as *malware*, *residential proxy*, *botnet*, *organised crime*, *criminal financing*, *payment networks*, *synthetic media*, *generative AI*, *broadcast manipulation*, *Russian information operations* and *hybrid threats*.

Sources were selected according to their relevance, credibility, recency and relationship to the identified risk pathways. Peer-reviewed research and authoritative government, law-enforcement and cybersecurity sources were prioritised. Technical and industry reporting was included where it provided observable evidence, documented cases or specialist analysis not yet represented adequately in the academic literature.

Sources are cited throughout using a domain prefix and sequential number: CYB for cybersecurity, OCF for organised-crime financing and DIS for disinformation and AI. Full entries appear in the

corresponding Annotated Bibliographies. The evidence base comprises 178 sources, together with direct technical evidence supplied by Nordic Content Protection [DIS-065].

The report then applies a **standardised risk-evidence framework** across the three domains. Each major risk judgement was assessed against the following dimensions:

1. **Mechanism plausibility** - whether there is a technically, operationally or socially plausible pathway through which the risk could occur;
2. **Capability requirement** - the actors, access, infrastructure or technical capability required for that pathway to be realised;
3. **Evidence strength** - whether the proposition is supported by direct evidence, demonstrated cases, strong analogues, technical plausibility alone, or insufficient evidence;
4. **Case-study and analogue support** - whether comparable real-world incidents or experiments demonstrate the relevant mechanism or pathway;
5. **Nordic relevance** - whether the evidence directly concerns, or can reasonably be applied to, Nordic users, broadcasters, services, infrastructure, markets or public institutions;
6. **Potential impact** - the seriousness and scale of the consequences were the risk to occur; and
7. **Confidence** - the degree of confidence warranted by the quality, directness and regional applicability of the available evidence.

These dimensions were considered together rather than combined through a mechanical scoring formula. The purpose of the framework is to make the evidentiary basis of each judgement explicit and to distinguish established harms from demonstrated capabilities, reasonable inferences and emerging risks. This is particularly important for media-integrity and AI-enabled manipulation, where individual components of a risk pathway may be well demonstrated even though their deliberate convergence within Nordic illegal IPTV has not yet been observed.

The evidence base is organised using the five-level evidence ladder shown in Table 1.

Level	Meaning and Usage	Use in this report
E1	Direct evidence – can support a finding	Project materials, technical artefacts, observed infrastructure, payment flows, application behaviour, OSINT or supplied material.
E2	Actual case study or experiment – can support plausibility and likelihood	Real-world cases or controlled studies showing the relevant risk occurring in piracy, illegal IPTV, cybercrime, fraud, propaganda or adjacent media-manipulation contexts.
E3	Strong analogue or observation – supports reasonable inference	Closely related evidence, including streaming piracy, malicious advertising, botnet monetisation, deepfake fraud, election disinformation or criminal subscription services.
E4	Technically or socially plausible pathway – frame as an emerging or theoretical risk	Feasible pathway for which direct or close case evidence has not yet been identified. Used mainly for emerging AI-enabled manipulation pathways.
E5	Speculative or unsupported – exclude from findings	Propositions without sufficient evidence or mechanism. Not relied on for core judgements.

Table 1. Evidence ladder

The evidence ladder governs the strength of the claims made in the report. E1 evidence can support direct findings; E2 evidence demonstrates that a mechanism or risk has occurred in practice; E3 evidence supports reasonable inference from closely related contexts; E4 evidence supports cautious treatment as an emerging or theoretical risk; and E5 propositions are not relied upon for substantive findings. The three

risk domains are assessed separately using this framework before their potential convergence is considered in Chapter 7.

The Annotated Bibliographies provide an extract of the underlying evidence record, including source classification and evidentiary contribution; they do not reproduce every analytical dimension considered in applying the risk-evidence framework to each domain judgement.

1.6 Terminology

Illegal streaming ecosystem and untrusted distribution infrastructure refer to the technical, commercial and operational systems enabling unauthorised audiovisual distribution, including websites, applications, streaming services, devices, reseller networks, payment channels, advertising, hosting and related services. The term piracy is retained where it is legally or technically precise, including when describing evidence sources, copyright infringement categories or broader piracy-site research.

Illegal IPTV refers to subscription or streaming services providing unauthorised television, sports, film or other audiovisual content through applications, portals, playlists or dedicated devices.

Illicit streaming devices are devices configured, marketed or used to access unauthorised services, including modified set-top boxes, sideloaded applications and devices bundled with illegal IPTV access.

Disinformation is deliberately created or distributed to deceive or influence.

Russian-aligned organised crime refers to criminal actors or service providers based in Russia, connected to Russian-speaking criminal ecosystems, exposed to Russian state influence. The term does not imply formal Kremlin direction in every case [OCF-035].

1.7 Limitations

This report is a forward-looking security assessment examining the convergence of established cybersecurity exposure, professionalised illegal-streaming markets, documented state use of criminal networks, hostile information operations and synthetic-media capability. It establishes the strength of the relevant risk pathways and their significance for Nordic security and national resilience.

The principal area requiring further investigation is the relationship between particular Nordic-facing illegal IPTV services and state-aligned criminal or influence networks. Resolving those relationships requires targeted forensic, financial, ownership and supply-chain investigation. The evidence already supports action against established cyber and criminal harms and proportionate monitoring and preparedness for the emerging media-integrity pathway.

The assessment therefore provides a basis for identifying, prioritising and investigating high-risk services while maintaining evidentiary discipline around specific actors and relationships.

2. Strategic Context: Hybrid Threats and Nordic Exposure

This section situates the assessment within the changed Nordic security environment and explains why hybrid activity, deniable proxies and regional digital dependence make untrusted illegal-streaming infrastructure relevant to national resilience.

2.1 A changed Nordic security environment

Russia's 2022 invasion of Ukraine and Finland's and Sweden's subsequent NATO accession increased the strategic importance of Nordic infrastructure, audiences and information systems. In the region's highly connected societies, cyber resilience and information integrity are central to security across NATO's northern flank, the Baltic Sea and the High North. High-risk illegal streaming infrastructure should therefore be assessed within a broader hybrid-threat environment encompassing cyber operations, sabotage, disinformation, organised crime and deniable proxies [DIS-016, DIS-031–DIS-034, OCF-052–OCF-056]. Nordic and NATO resilience literature similarly situates the region within a grey-zone environment combining cyber, information, economic and other forms of pressure [OCF-036, OCF-037].

2.2 Hybrid threats and the use of deniable infrastructure

Hybrid threats exploit ambiguity below the threshold of armed conflict through cyberattacks, disinformation, sabotage, illicit finance, criminal proxies and attacks on public trust. Criminal networks offer hostile states useful capabilities, including malware, compromised systems, laundering, local access and deniable operational structures [OCF-052–OCF-056, CYB-043, CYB-048]. They may serve as facilitators, intermediaries or service providers, complicating attribution and response. High-risk illegal streaming infrastructure is therefore strategically relevant even without formal state ownership because insecurity, opacity, criminal financing and audience reach may make parts of it exploitable by hostile actors [CYB-026–CYB-031].

2.3 Russia as the primary Nordic threat lens and the wider state-crime mechanism

Russia remains the most relevant current state-threat lens for this assessment. Russian organised crime can advance state interests without direct Kremlin control, through relationships based on tolerance, coercion, protection and mutual utility [OCF-052, OCF-053]. Where illegal streaming systems intersect with Russian or Russian-aligned criminal networks, existing hosting, reseller systems, compromised devices and other infrastructure may provide access, capability and deniability without requiring direct state ownership or control [OCF-052–OCF-056].

The mechanism is not unique to Russia. In 2024, the Swedish Security Service stated that Iran was using criminal networks in Sweden as proxies and separately attributed a cyber-enabled influence campaign to an Iranian group that had compromised an existing commercial bulk-messaging service [OCF-061, DIS-064]. These cases demonstrate that hostile states can exploit criminal intermediaries and civilian communications infrastructure without owning the underlying delivery system.

A July 2026 UK conviction provides a further cross-border example. A Norwegian teenager was convicted of conspiracy to murder after being recruited on behalf of the Swedish Foxtrot Network, an organised-crime group with reported links to the Iranian regime [OCF-019]. The conviction does not establish that Iran directed that specific plot, but it demonstrates the reach of a Nordic criminal network with a documented foreign-state nexus.

These cases do not themselves involve illegal IPTV. Rather, they demonstrate a broader mechanism relevant to this assessment: hostile states can exploit criminal intermediaries and civilian communications infrastructure without owning or directly controlling the underlying delivery system. Separately, Russian and Kremlin-backed audiovisual content is already distributed through illegal and uncontrolled IPTV environments relevant to the Nordic region. The emerging strategic risk is that the same untrusted distribution layer could be exploited to alter, substitute or insert content presented under the identity of trusted Nordic broadcasters, allowing a hostile actor to reach established audiences without compromising the lawful broadcaster itself.

2.4 Untrusted distribution infrastructure as an attractive hybrid-threat surface

Many users return to the same illegal IPTV service, application or reseller for regular viewing, particularly for live sport and television. Mediavision reported in May 2025 that more than 1.5 million households across Denmark, Finland, Norway and Sweden had access to illegal IPTV, demonstrating the scale of the recurring audience. Consumer research also shows that users often underestimate piracy-related cyber risk [OCF-013, CYB-002, CYB-005]. Repeated use can therefore create familiarity and behavioural trust.

Unauthorised services do not need to create credibility from scratch. They appropriate the channels, programmes, presenters, logos, graphics and electronic programme guides of lawful public-service and commercial broadcasters. A user may distrust the operator yet still trust what appears to be a familiar broadcaster or programme. That borrowed brand integrity can lower scrutiny of altered segments, overlays or prompts, even though the distribution environment lacks the editorial oversight, security assurance, incident response and consumer redress of lawful media [CYB-001, CYB-008, CYB-048, DIS-039, DIS-052].

The infrastructure is also resilient. Domains, servers and access arrangements can be replaced after disruption, while opaque ownership and payment structures make responsible actors difficult to identify [OCF-011, OCF-018, OCF-023, OCF-030]. During a crisis, piracy may therefore provide hostile actors with a persistent and difficult-to-disrupt channel that often sits outside effective editorial, provenance and incident-response governance.

2.5 Compromised consumer infrastructure has crossed the national-security boundary

The national-security relevance of illegal streaming infrastructure is demonstrated by the existing use of consumer devices as covert infrastructure. BADBOX identified more than 192,000 infected TV boxes, smartphones and other devices containing preinstalled malware [CYB-040]. Russia was the most affected country, indicating market exposure but not necessarily origin. Its significance is that ordinary household devices can be repurposed at scale for proxying, botnet activity and traffic relay. More recent evidence places BADBOX 2.0 above 10 million affected devices and identifies state-sponsored actors among the extensive criminal and espionage groups using residential-proxy services [CYB-048].

The NetNut disruption shows how this device layer can be monetised. At least two million home devices, including smart TVs and streaming boxes, were converted into residential proxy nodes that concealed malicious traffic behind consumer IP addresses. Related reporting on H96 streaming devices found coordinated advertising fraud and residential proxying continuing even when the devices appeared inactive [CYB-042, CYB-046, CYB-048].

A clearer state-linked precedent comes from the GRU's exploitation of vulnerable home and small-office routers for DNS hijacking, traffic interception and adversary-in-the-middle activity. Allied reporting on China-linked actors similarly shows that compromised routers and smart devices can provide low-cost, deniable infrastructure for cybercrime and espionage [CYB-043, CYB-044, CYB-048].

These cases place illicit streaming devices within a wider covert-infrastructure problem. They also expose a jurisdictional asymmetry: a Nordic consumer may use a local reseller to access an application, authentication service, stream, payment channel and backend infrastructure located across several foreign jurisdictions. The affected household and broadcaster can therefore be Nordic while key operators, evidence and technical control points sit outside effective Nordic jurisdiction. The unresolved question is whether Nordic piracy services, supply chains, resellers or payment flows intersect with Russian or Russian-aligned criminal networks in ways that make this infrastructure available for state or state-tolerated exploitation.

2.6 The role of generative AI

Generative AI reduces the cost and expertise required to produce convincing synthetic media. Experimental evidence shows that AI-generated propaganda can approach the persuasiveness of authentic

foreign propaganda, particularly after limited human editing [DIS-018]. Voice-cloning tools can now generate credible impersonations from short recordings, with documented fraud losses including a EUR 220,000 transfer induced through executive impersonation [DIS-045]. Synthetic speech has also reached a level at which human listeners may struggle to distinguish it from genuine audio [DIS-022].

The greater risk lies in combination with established techniques. Edited footage, false subtitles, selective translation, forged documents and cloned interfaces remain effective, and recent elections have featured more cheap fakes than fully AI-generated content [DIS-023, DIS-051]. Generative AI nevertheless makes such material easier to produce, localise and adapt. When distributed through unofficial services that lack editorial oversight and reliable correction mechanisms, manipulated content may reach audiences through channels they already use. AI-enabled manipulation is therefore best understood as an emerging risk that builds on existing weaknesses in piracy distribution.

2.7 Mature harms and emerging risk

It is important to distinguish established harms from prospective risk. Cybersecurity exposure and organised-crime financing are well documented in the Nordic region and elsewhere, as set out in Chapters 4 and 5 [CYB-001, CYB-012, OCF-013, OCF-020, OCF-023, OCF-030]. The media-integrity dimension is different: it is an emerging strategic risk rather than an established Nordic harm. Russian information operations already target the region; uncontrolled IPTV distribution is established; consumer infrastructure can be compromised at scale; audiovisual manipulation techniques are demonstrated; and synthetic media has become cheaper and more accessible. Their convergence creates a credible pathway for future exploitation [DIS-016, DIS-031–DIS-034, CYB-040–CYB-046, CYB-048, DIS-018, DIS-022, DIS-045–DIS-047].

High-risk illegal streaming infrastructure should therefore be incorporated into relevant cybersecurity, organised-crime, foreign-interference and national-resilience analysis before a major incident occurs. The case for action rests on established cyber and criminal harms combined with a plausible, high-consequence media-integrity escalation pathway.

2.8 Strategic implication

Scale makes the governance problem strategically significant. Mediavision's Spring 2023 survey found approximately 1.15 million subscribing households and 4.4 million people aged 15–74 who had used a piracy service in the previous month across Denmark, Finland, Norway and Sweden [OCF-013]. Its May 2025 update reported more than 1.5 million households with access to illegal IPTV across the same four markets. Responsibility, however, is split across institutions whose mandates capture only part of the problem: cyber agencies see malware and proxy infrastructure; financial-intelligence units see suspicious transactions; regulators and rights holders see unlawful distribution; consumer agencies see complaints; and security services see foreign influence. A single high-risk illegal IPTV operation can generate activity in several domains at once, yet no institution is positioned to assemble the full evidentiary picture. Organised-crime research likewise stresses shared intelligence, anti-money-laundering capability and cross-agency partnership [OCF-029].

3. Untrusted Distribution Infrastructure as a Shared Attack Surface

This section explains how the illegal streaming ecosystem creates a shared attack surface linking established cybersecurity and organised-crime harms with an emerging media-integrity risk.

3.1 Overview

The illegal streaming ecosystem comprises interconnected services, devices, applications, resellers and hosting arrangements that reach substantial and often habitual audiences outside lawful security and editorial controls. This untrusted distribution infrastructure creates a shared attack surface through which technical compromise, criminal monetisation and information manipulation can reinforce one another. Figure 1 illustrates how these interactions can transform otherwise distinct harms into a compound strategic risk.

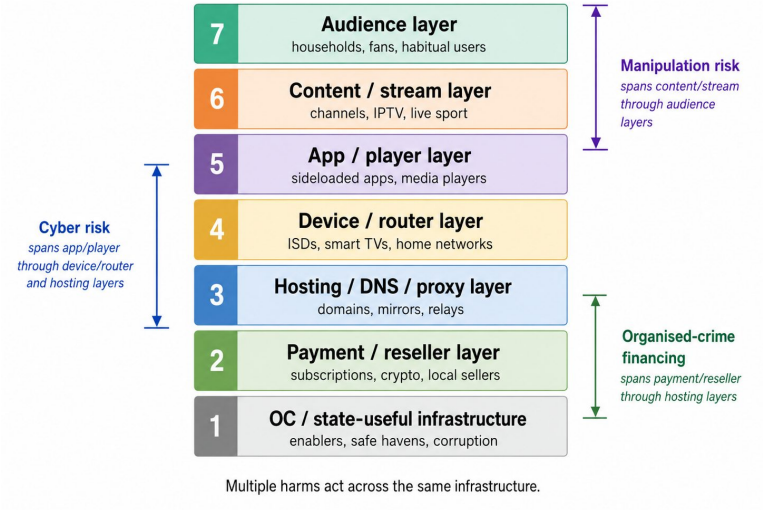

Figure 1. An idealised view of the illegal streaming infrastructure stack

3.2 Illegal streaming infrastructure is more than content theft

Illegal streaming is often framed primarily as unauthorised access to content, but its operation depends on a wider technical and commercial ecosystem. Opening an application, purchasing an illicit subscription or installing a set-top box may engage hosting, credential distribution, payment processing, advertising, reseller networks and domain migration.

Each layer introduces distinct risks. Applications and devices may enable tracking, malware or covert network activity; websites may facilitate scams and credential theft; payments may obscure beneficiaries or expose users to fraud; and streams or interfaces may be altered without effective oversight. Resellers can provide local familiarity while distancing customers from the underlying operator. Piracy should therefore be assessed as infrastructure rather than infringement alone, because its technologies, payment systems and distribution relationships create capabilities that may be exploited by criminal and hostile actors [CYB-001, CYB-008, CYB-019, CYB-021, OCF-023, OCF-030, DIS-043].

3.3 The shared attack surface

The shared attack surface shown in Figure 1 comprises five operational layers and a cross-cutting governance gap. Their boundaries are not fixed, particularly where applications and devices operate as an integrated system.

The technical layers comprise distribution, applications and devices. The distribution layer governs what users see and hear through streams, websites, portals and playlists, creating opportunities for content substitution, false captions, deceptive overlays and cloned channels. The application layer includes unofficial media players, browser extensions and sideloaded software that may collect data, steal credentials, manipulate traffic or enrol devices in proxy and botnet activity. The device layer extends these

risks to streaming boxes, smart televisions and routers, where compromise may provide persistent access to residential networks and trusted domestic traffic [CYB-001, CYB-008, CYB-024, CYB-048, DIS-043].

The commercial layer sustains the ecosystem through subscriptions, resellers, advertising, payments and laundering mechanisms, while obscuring ownership and attracting criminal intermediaries. The audience layer gives the infrastructure its reach: repeated use, particularly for live sport and culturally specific content, can create familiarity and reduce perceptions of risk [OCF-017, OCF-023, OCF-030].

The final element is a governance gap rather than a separate operational surface. Responsibility is divided among institutions, none of which necessarily sees the full relationship between technical compromise, criminal monetisation and manipulated content. This fragmentation allows multiple harms arising from the same ecosystem to be treated as unrelated problems.

3.4 The distribution surface: untrusted channels and content control

Licensed broadcasters operate within systems of editorial responsibility, technical assurance and regulatory accountability. Content can be authenticated, incidents investigated, false information corrected and compromised transmissions interrupted. Unauthorised services can reproduce the broadcaster's outward identity while discarding those controls, leaving the provenance and integrity of redistributed content uncertain.

Familiar channels, presenters, graphics and interfaces may therefore conceal unauthorised restreaming, cloned portals or compromised backend systems [DIS-039, DIS-052, DIS-061]. A viewer may recognise and trust the lawful broadcaster even though the delivery path is controlled by an unrelated unauthorised service. This creates a particular risk for live and crisis-sensitive content, where altered captions, false announcements, synthetic clips or deceptive overlays may circulate before viewers can verify them through lawful sources.

Repeated delivery of genuine sport, news and entertainment can make an untrusted distribution environment appear routine and reliable. That accumulated familiarity can then lend credibility to a malicious insertion, allowing hostile content to borrow both the broadcaster's reputation and the user's established viewing habit.

This is the 'Trojan horse' characteristic of illegal IPTV. Unlike an overt propaganda channel, the potentially hostile distribution mechanism is largely invisible to the viewer because it normally delivers the content the viewer expects. Genuine news, sport and entertainment can establish months or years of routine use before any malicious intervention occurs. If the intermediary later substitutes a short segment, changes a caption, inserts a breaking-news banner or displays an emergency-style message, the manipulation arrives inside an already trusted viewing environment rather than as an obviously foreign communication.

At sufficient scale, this becomes more than a weakness within individual illegal streaming services. It creates a governance problem for the wider media environment because neither the broadcaster nor the state necessarily controls, authenticates or even observes the version of a trusted channel received through the unauthorised distribution layer. As more habitual viewing moves into these environments, a larger share of the audience sits outside normal mechanisms for provenance, editorial accountability, incident response and correction.

3.5 The application and device surface: access into the household network

Illegal streaming applications and devices create risks that extend well beyond unlawful viewing. Sideloaded players, modified set-top boxes and illicit streaming devices may introduce untrusted code, weak update mechanisms, excessive permissions and insecure network behaviour into domestic environments. As discussed in Chapter 4, BADBOX, residential proxy networks and compromised-router campaigns show that consumer hardware can be repurposed as botnet nodes, proxy exits, traffic relays and persistent access points [CYB-001, CYB-008, CYB-024, CYB-046, CYB-048]. The same application or device may simultaneously provide trusted-looking broadcaster content and retain control over updates, overlays, programme guides, traffic and network permissions.

For consumers, the consequences include malware, credential theft, privacy loss and fraud. For attackers, the greater value lies in residential connectivity: a compromised device can provide a local IP address, trusted domestic traffic and concealment within a home network. Malicious activity routed through a household in Oslo or Copenhagen may therefore appear to originate from an ordinary user [CYB-040–CYB-045, CYB-048].

Illegal-streaming device exposure consequently forms both a technical and a trust surface. A device that reliably delivers genuine broadcaster content for months can condition the user to trust the environment through which a later malicious update, overlay or manipulated segment is delivered. Trusted content and untrusted distribution therefore share the same attack surface: the viewing device is no longer merely a receiver, but infrastructure available for third-party exploitation and content intervention.

3.6 The commercial surface: monetisation, resilience and opacity

The illegal streaming ecosystem is sustained by organised commercial systems that generate recurring revenue and allow services to recover after disruption. Consumers often interact only with a reseller, application or payment instruction, while the underlying operators and beneficiaries remain concealed. This separation supports continuity, limits accountability and provides access to users, devices, payment channels and technical services [OCF-011, OCF-018, OCF-023, OCF-030].

Where these systems intersect with Russian or Russian-aligned organised crime, their significance extends beyond profit. Criminal networks may be tolerated, protected, coerced or purchased in ways that preserve operational distance from the state. Such arrangements provide persistence and strategic deniability without requiring direct state ownership or control [OCF-052–OCF-056].

3.7 The audience surface: routine trust in unlawful environments

The illegal streaming ecosystem depends on operational trust and sustained demand. Users may recognise that a service is unlawful while still expecting its streams, applications, payments and reseller support to function predictably. More importantly, the service borrows trust from the lawful content it redistributes. A familiar public-service channel, sports broadcast, presenter or programme guide can reduce scrutiny of the unauthorised distribution layer. Consumer research shows that piracy-related risks are frequently underestimated [CYB-002, CYB-005].

Demand is reinforced through friends, family, resellers and language or fan communities, and by the economic value proposition offered to consumers. The 2023 Mediavision evidence identifies paid access to streaming services, live sport and foreign channels as important purchase drivers in Nordic markets [OCF-013]. Broader live-sports research likewise identifies price, availability, convenience and social normalisation as persistent drivers [OCF-021]. These incentives sustain subscriptions and renewals, generate recurring criminal revenue and create habitual viewing environments in which AI-enabled manipulation can exploit familiar interfaces, voices and localised content [DIS-018, DIS-022, DIS-039, DIS-045, DIS-052]. The intended effect need not be lasting persuasion; brief confusion, delay or loss of confidence during a crisis may be sufficient.

3.8 Conclusion

The shared attack surface is difficult to govern because responsibility is divided across institutions with different mandates. Broadcasters address unauthorised distribution; cyber agencies investigate malware and proxy abuse; financial-intelligence units examine suspicious payments; consumer agencies respond to scams; and national-security agencies assess hostile influence. Each sees a valid but incomplete part of the same ecosystem.

This fragmentation creates a structural blind spot. A single illegal IPTV operation may combine copyright infringement, fraud, technical compromise, criminal revenue and information manipulation, yet no institution necessarily receives or integrates the full evidentiary picture. The term *shared attack surface* is therefore literal: the same infrastructure, devices, users and financial arrangements may support several forms of harm simultaneously.

Chapters 4 and 5 examine the established cyber and financial dimensions of this risk, while Chapter 6 assesses the emerging potential for AI-enabled manipulation. The concern is not that every illegal service exhibits all three characteristics, but that a strategically significant subset may do so. Identifying that subset should be a priority for Nordic monitoring, investigation and coordinated response.

4. Cybersecurity Exposure: A Mature Access-Layer Risk

This section assesses the established cyber risks associated with piracy sites, illegal IPTV applications and illicit streaming devices, and explains how persistent device compromise can create an access layer for broader criminal or state-linked activity.

4.1 Overview

Cybersecurity exposure is the most mature harm examined in this report. That piracy sites are dangerous places has been measured repeatedly, in many countries, using several different methods, and the answer keeps coming back the same. However, what is notable about the piracy examined in this study, is that it is the device layer. A dangerous website harms whoever visits it. A compromised set-top box stays in the house afterwards: connected, unattended, and useful to bad actors.

In the compound-risk model, this exposure forms the access layer. Compromised devices may become botnet nodes, covert relays, residential proxies or footholds in home networks, while unsafe applications may collect data, manipulate traffic or install malicious components.

These harms affect consumers, businesses, broadcasters and public agencies. More broadly, compromised devices and networks can create technical access that organised crime or hostile state actors may exploit. Illegal-streaming cyber risk is therefore measurable, serious and substantially under-controlled; direct hostile-state use of a particular Nordic IPTV service remains a separate attribution question.

4.2 Core Findings

Evidence combines Nordic studies, international comparisons, device experiments, botnet research, surveys and intervention evidence, as shown in Table 2.

Evidence group	Evidence IDs	Contribution
Nordic baseline	CYB-012, CYB-013	Direct evidence of elevated cyber risk across Nordic P2P, streaming, scam and IPTV services.
Site and consumer risk	CYB-002–007, CYB-009, CYB-011, CYB-034, CYB-036, CYB-037	Evidence of malware, scams, tracking, deceptive downloads, fake files and consumers' tendency to underestimate exposure.
Illicit streaming applications and platforms	CYB-016, CYB-019–023	E2 case and experimental evidence showing how piracy applications and services may expose users to malicious, deceptive or unauthorised activity. The evidence has Medium Nordic relevance because the observed mechanisms are not confined to a single jurisdiction.
Devices and covert infrastructure	CYB-001, CYB-008, CYB-024, CYB-040–045, CYB-048	Direct device testing and evidence of device compromise, residential-proxy abuse, botnet monetisation, criminal revenue and state-sponsored use of consumer infrastructure.
Intervention	CYB-010	Evidence that rapid blocking can reduce traffic to harmful services and limit user exposure.

Table 2. Nordic evidence base

The overall risk is **High**. Evidence is strongest for consumer exposure, device compromise, malware, scams and proxy abuse.

4.3 Nordic empirical baseline

The Nordic study found substantially elevated cyber risk across all piracy categories, as shown in Figure 2. For P2P, streaming and fraudulent sites, the reported ranges reflect variation both between Nordic countries and between the study's conservative best-case and less conservative worst-case detection assumptions. IPTV subscription services were assessed separately using a Swedish sample because of the substantial overlap in services used across the Nordic region. Their landing pages produced

a relative-risk estimate of 2.33 to 4.0 times that of mainstream sites. These figures measure exposure at the website level and should not be interpreted as the total risk associated with using an IPTV service [CYB-012], as shown in Table 3.

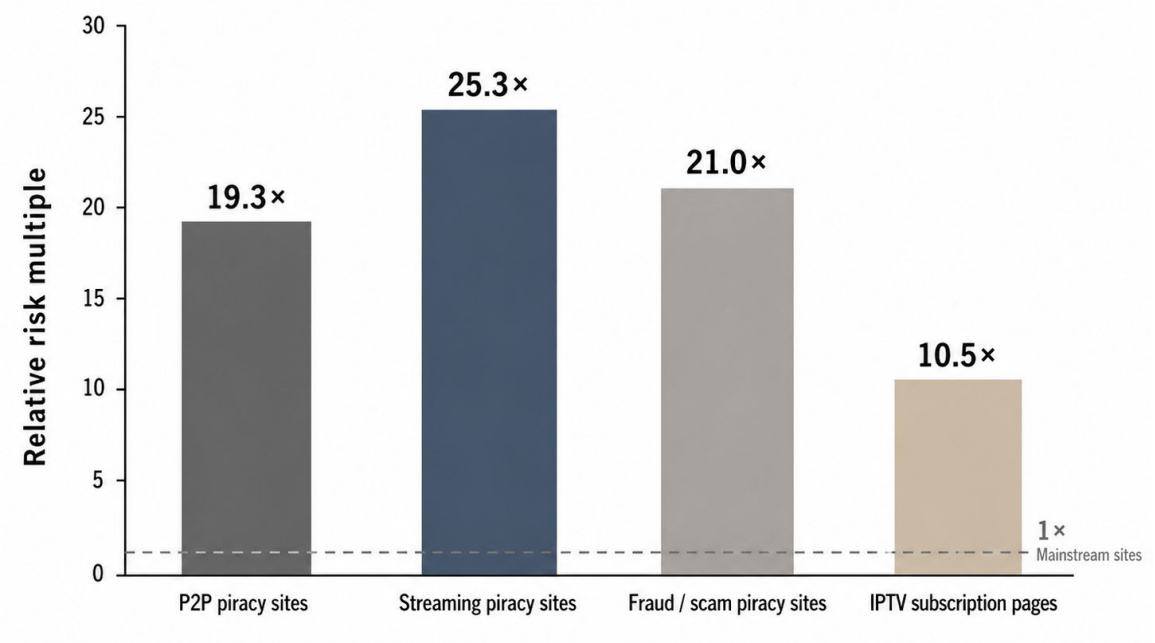

Figure 2. Nordic piracy cyber risk multiples.

The same Nordic study separately analysed 14 IPTV client applications advertised by or linked from the sampled services. These applications produced an average of 1.50 malware detections or intrusion-detection rule matches per application and contained 63 MITRE ATT&CK tactic instances, including behaviours associated with command and control, system and network discovery, data collection, persistence and evasion. This provides direct Nordic-relevant evidence that the principal IPTV risk may extend beyond the subscription landing page to the software installed on the consumer's device and the network to which it is connected [CYB-012].

Independent experimental evidence reinforces this finding. CYB-020 tested 60 URLs drawn from illegal IPTV websites, application stores and software using a specialist malware-analysis framework. It classified 32 of 60 as malicious, compared with 23 of 60 identified through VirusTotal, and found malicious URLs or files associated with 31 sampled websites. The study is not Nordic-specific, but the technical mechanisms are directly applicable because illegal IPTV services rely on the same types of websites, applications and installation pathways across jurisdictions. Together, CYB-012 and CYB-020 show that conventional landing-page and antivirus screening captures only part of the exposure associated with illegal IPTV.

The evidence therefore supports two related but distinct conclusions. Piracy websites expose Nordic consumers to materially greater cyber risk than mainstream services, while IPTV applications can create a deeper device- and network-level foothold that is not adequately represented by website risk scores alone.

Historical NCP trend evidence remains useful for showing the transition from card-sharing to IPTV, but it should not be read as the current market scale. Since 2015, active card-sharing servers fell markedly while the number of IPTV websites on the NCP blacklist increased; only 4.5% of identified card-sharing servers were hosted within the Nordic countries [CYB-013]. This established early that services targeting Nordic consumers were supported largely by infrastructure outside the region.

Current regional weight should instead rest on the direct Nordic cyber-risk study [CYB-012] and newer Mediavision consumer evidence. The 2023 Mediavision study found approximately 1.15 million

subscribing households and 4.4 million monthly piracy users across Denmark, Finland, Norway and Sweden [OCF-013], while its May 2025 public update reported more than 1.5 million households with access to illegal IPTV across those four markets. The older NCP 2020 blacklist finding, including a 358% increase since 2016 and strong Nordic-content targeting, is retained as longitudinal context rather than a current prevalence estimate [OCF-020].

Piracy category	Relative risk
P2P sites	11.8 to 19.3 times
Streaming sites	16.5 to 25.3 times
Fraudulent or scam sites	15.0 to 21.0 times
IPTV subscription sites	4.0 (in Sweden)

Table 3. Nordic piracy cyber risk data

4.4 Piracy sites, malware and scams

International studies confirm that the Nordic findings reflect a consistent global cyber-risk pattern. Across multiple methods and markets, piracy services show substantially higher malware, scam, phishing, tracking and fake-file exposure than mainstream sites. Worst case data is shown in Table 4.

Study	Design	Key result	Evidence
Philippines, 2023	100 piracy sites compared with 50 mainstream sites	Torrent and streaming risk scores were 16.66 and 21.66 times higher than controls.	CYB-004
Thailand sports streaming, 2024	25 illicit domains	Threats were detected on 20% of sites; scam risk was 5.9 times higher than controls.	CYB-006
Indonesia sports streaming, 2024	25 illicit domains	Threats were detected on 20% of sites; scam risk was 3.21 times higher than controls.	CYB-007
Philippines, 2024	180 piracy URLs compared with 30 lawful sites	P2P and streaming risk were approximately 33 and 32 times higher than controls.	CYB-009
Malaysia, 2025	25 piracy and 25 mainstream sites	Piracy sites recorded 12.81 times the mainstream scam-risk score, with a large, significant effect.	CYB-011
BitTorrent/TorrentGuard, 2011	Fake-file ecosystem analysis	Fake files comprised about 35% of content; over 99% were linked to malware or scams, noting that consumption has since shifted to include streaming, IPTV and messaging platforms.	CYB-037

Table 4. Global cyber and piracy study results

Pirated-software research in Southeast Asia provides a related malware-bundling analogue, identifying adware and trojans associated with unlawful software [CYB-035]. Common pathways include malicious advertising, phishing pages, fake downloads, forced redirects, notification abuse and fraudulent player or codec updates. Free sports streaming is especially relevant because time-sensitive demand encourages users to tolerate poor security and intrusive advertising [CYB-034]. A smaller Philippine study likewise found malware or attack indicators on most of nine tested illegal-streaming sites, while 70% of surveyed users said they would continue using them despite the risk [CYB-017].

Cyber exposure is therefore structural, piracy operators monetise traffic through subscriptions, advertising, tracking, scams, credential capture, malware and compromised devices. Users are not merely accessing unlawful content, but entering an ecosystem designed to exploit attention, trust, devices and data.

4.5 Illicit streaming devices and unsafe applications

Illicit streaming devices and piracy apps extend cyber risk into household networks, as documented in Table 5. Unlike a malicious website, a compromised device may remain connected, execute code and interact continuously with domestic traffic. Compromise may arise from the device itself or during ordinary setup. Streaming hardware has been documented with pre-installed residential-proxy software active before any user interaction [CYB-046], while other devices direct users to piracy application portals containing malware [CYB-008].

Evidence	Key finding	Implication
Proxy analysis	Seven illicit streaming APKs and three devices exhibited behaviour consistent with residential proxying. The clearest device example was UnblockTech 10, which generated 6,895 SOCKS5 handshake indicators, nine HTTP CONNECT signals, 102 common-proxy-port events and fan-in from 2,016 distinct client IP addresses. Traffic was also linked to infrastructure associated with banking trojans and ransomware [CYB-001].	Household devices may route third-party traffic, conceal malicious activity and connect to wider command-and-control infrastructure.
Taiwan device study	Four devices averaged 7.75 vulnerabilities, including exposed web services and Android Debug Bridge access. During normal setup, users were directed to a portal distributing 67 APKs, of which 49% received at least one malware detection. The set produced 157 detections in total, with up to 20 detections for a single file [CYB-008].	Risk arises both from device vulnerabilities and from the applications consumers are instructed to install during setup.
EVPAD ecosystem	EVPAD provided 1,260 live channels and 24,934 titles through an ecosystem comprising 131,175 identified users and 78 operational servers. Its P2P architecture used participating devices to redistribute content to other users rather than merely receive streams [CYB-024].	Consumer devices can become active distribution nodes within a large piracy ecosystem.
VSeeBox and SuperBox S6	Recent test purchases provide independent corroboration of these risks. A VSeeBox V5 Pro purchased through a mainstream US retailer contacted a Chinese server every 60 seconds and accepted remote commands, including application installation, reboot and factory reset. A SuperBox S6 Max transmitted its IP address, location and proxy status, obtained applications through a Google-spoofing domain and connected to a BitTorrent tracker [CYB-048]. The findings demonstrate that piracy-oriented devices with unsafe remote-control and telemetry behaviour can enter mainstream retail supply chains.	Piracy-oriented devices sold through mainstream retail channels may contain unsafe remote-control, telemetry and application-distribution functions, extending supply-chain risk beyond grey-market sellers and enabling persistent third-party access to household networks.

Table 5. Illicit streaming devices and unsafe applications

These findings show that illicit streaming devices are active infrastructure rather than passive receivers. They may expose network services, install or execute unsafe applications, connect to backend systems, redistribute content to other users and route third-party traffic. In the compound-risk model, this transforms consumer exposure into an access-layer risk. Compromised devices may persist within home

networks, support proxy or P2P activity, observe network behaviour and provide infrastructure that can be repurposed or exploited at scale.

4.6 Botnets, residential proxies and covert infrastructure

The strongest cyber evidence concerns the conversion of consumer devices into botnet, proxy and relay infrastructure, as shown in Table 6. This is where piracy-related risk becomes a national-security concern.

Evidence	Key finding	Strategic relevance
BADBOX	Bitsight identified over 192,000 infected Android devices, including Yandex smart TVs and Hisense phones. Russia was the most affected country [CYB-040].	Streaming devices can be compromised at scale within Russian-market ecosystems.
BADBOX 2.0	The FBI warned that more than one million IoT devices, including TV streaming devices, were being used in botnets [CYB-041]. Later reporting placed the wider BADBOX 2.0 infection above 10 million devices. Google's disruption of the associated IPIDEA proxy network reduced its pool by approximately 40%, but several million devices continued connecting, and the same infrastructure was subsequently exploited by the Kimwolf botnet [CYB-048].	Free-content devices can expose home networks to criminal infrastructure.
NetNut / Popa	Google estimated at least two million devices were enrolled as residential proxies. In one week, 316 threat clusters used suspected exit nodes [CYB-042].	Home devices can provide residential IP space and conceal criminal or espionage activity.
Fengwo / H96	Generic H96 streaming devices shipped with pre-installed proxy software and were centrally tasked by a named China-based operator. This included ad-click fraud while the television was off and serving as a residential proxy while in use. One expired telemetry domain revealed about 38,000 devices [CYB-046].	Device-fleet monetisation has an identifiable commercial operator with shell companies, making supply-chain investigation practical.
Russian GRU routers	The FBI attributed compromised routers used for DNS manipulation, credential theft and traffic interception to APT28 [CYB-043].	Russian state actors already exploit consumer and edge infrastructure.
China-nexus networks and RSOCKS	Allied advisories and the RSOCKS case confirm state and Russian cybercriminal use of compromised devices and residential proxies [CYB-044, CYB-045].	Consumer devices are now a recognised covert-infrastructure class.
Residential-proxy market	Approximately 26 million unique US residential IP addresses were observed over 30 days, with more than 20 million connections estimated to enter proxy pools annually. Across seven services, an average of 85% of connections were flagged for fraud or abuse [CYB-048].	Demonstrates the scale and predominantly abusive use of residential-proxy infrastructure

Table 6. Botnets and residential proxy evidence

These cases show that compromised consumer devices can provide botnet capacity, traffic relaying, residential IP addresses, access to domestic networks and operational deniability. The Fengwo case adds an orchestration layer, demonstrating that fleet monetisation can be centrally managed by an identifiable commercial operator [CYB-046]. More directly, analysis of illicit streaming devices found traffic connecting to command-and-control infrastructure associated with the GandCrab and REvil/Sodinokibi ransomware families and the Chapak, Glupteba and Kryptik banking trojans [CYB-001]. REvil is also identified among Russian-linked ransomware groups operating as state-tolerated cyber proxies [CYB-025]. This provides a concrete link between illicit streaming devices and criminal infrastructure with a documented Russian nexus. Combined with evidence that state-sponsored actors use residential-proxy infrastructure, it places illicit streaming devices and piracy applications within a broader class of infrastructure relevant to both organised cybercrime and state-linked activity. Specific state direction remains an attribution question for targeted investigation.

CYB-048 also provides a direct link between device compromise and criminal revenue. The 911 S5 botnet monetised more than 19 million compromised IP addresses, generated approximately US$99 million for its operator and enabled an estimated US$5.9 billion in fraudulent pandemic-related claims. The same report identified more than 550 threat groups using residential proxies during a single week, including state-sponsored actors associated with Russia, China, Iran and North Korea [CYB-048]. These US-centred findings do not measure Nordic prevalence, but demonstrate that residential proxy infrastructure is used systematically for both organised cybercrime and state-sponsored activity.

The strategic value of this infrastructure is established. The next Nordic research priority is to determine the extent to which piracy services, supply chains, reseller networks and payment flows intersect with Russian or Russian-aligned organised crime in ways that enable state, state-tolerated or state-sponsored exploitation.

4.7 Privacy, tracking and data harvesting

Piracy services also create significant privacy risks by collecting behavioural and technical data that may support profiling, advertising and fraud. Users may regard piracy primarily as a legal risk, yet the information collected can reveal location, language and viewing patterns useful for phishing, account takeover and social engineering.

Evidence suggests that such tracking is widespread. Studies of live-sports piracy in Thailand, Indonesia and Malaysia identified intrusive advertising, malicious redirects and elevated scam indicators [CYB-006, CYB-007, CYB-011]. Separate research found third-party trackers on more than 95% of illegal movie-streaming services and fingerprinting on more than 70%, including services accessed from Sweden [CYB-019]. A larger study of 151,661 stream URLs across 467 provider domains identified canvas fingerprinting on 237 providers and WebRTC fingerprinting on 164, with illegal sports-streaming services tracking users more aggressively than lawful services [CYB-021].

These data may also increase manipulation risk by enabling content to be tailored to users' language, location and viewing habits, including Nordic audiences.

4.8 Infrastructure and content-protection exposure

Piracy services rely on unstable backend infrastructure, including domains, DNS, hosting, cyberlockers, Telegram channels, playlists, peer-to-peer systems, proxies and mirror sites. These mechanisms support enforcement evasion but also create substantial cyber risk, with the evidence summarised in Table 7.

Infrastructure pathway	**Key finding**	**Evidence**
High-risk sites	Torrent and streaming sites recorded 16.66 and 21.66 times the mainstream risk.	CYB-004

Infrastructure pathway	Key finding	Evidence
Piracy categories	P2P, streaming, scam, proxy and IPTV sites all exceeded lawful controls.	CYB-009
Scam ecosystem	Malaysian piracy sites recorded 12.81 times the mainstream scam-risk score.	CYB-011
Fake files	About 35% of BitTorrent files were fake, with over 99% linked to malware or scams.	CYB-037
Platform distribution	Cyberlockers and Telegram enable automated distribution beyond conventional websites.	CYB-038, CYB-039

Table 7. Infrastructure evidence

This infrastructure is resilient and difficult to govern. Removing a domain may not disrupt the service, payments or compromised devices, while app removal may encourage sideloading. Cyber exposure is therefore an enduring ecosystem condition rather than a single event.

4.9 Consumer perception and behavioural risk

Consumers often recognise piracy risk but underestimate its scale. A YouGov survey of 6,407 adults across five Asian markets ranked piracy websites as the second-leading perceived malware source, while piracy exposure, risk perception and demographics explained 31% of reported infection experience [CYB-002]. Broader behavioural research also found that digital piracy frequently co-occurred with hacking, cyberfraud and other cyber-deviance in an Australian adolescent sample [CYB-032].

The gap is clearest in India. Among 1,037 respondents, piracy sites were perceived as the leading malware vector, yet their estimated risk was only 2.03 times that of mainstream sites. VirusTotal analysis found substantially higher exposure: the Top 30 piracy sites carried 10.5 to 15 times the risk of mainstream controls, while the Top 30 fraudulent or scam piracy sites carried 15.5 to 27 times the risk [CYB-005]. This distinction is important because scam piracy sites combine the appeal of unauthorised content with deliberate deception and may warrant priority enforcement. Consistent with this finding, CYB-009 also recorded the highest malicious-detection count among fraudulent piracy sites.

Controlled testing demonstrated rapid compromise. A Windows device became unusable within 42 seconds, with 33 trojan command-and-control download attempts recorded in one hour. Android malware appeared 78 seconds after installation [CYB-003]. User behaviour therefore forms part of the attack surface. Pop-ups, redirects, permissions and device prompts may be normalised, while familiar devices or recommended resellers may appear trustworthy.

Consumer messaging should be about household security: malware, fraud, privacy, and the possibility that a device in the living room is quietly working for somebody else. In a sad irony, copyright may be the least persuasive part to lead with to enact change in consumer behaviour.

4.10 Intervention evidence

The evidence identifies speed as an important factor in effective intervention. A quasi-experimental study across six Asian markets found that Indonesia's 24-hour administrative blocking model was associated with a 58.8% reduction in piracy traffic, compared with 9.5% under Singapore's judicial model. Blocking was also associated with increased lawful OTT use in Indonesia and Malaysia [CYB-010]. These findings support the operational value of rapid and updateable intervention, although the Asian legal models should not be mapped directly onto Nordic arrangements.

For illegal IPTV and copyright infringement, blocking in Denmark, Finland, Norway and Sweden is principally court-based. Denmark supplements court orders through voluntary ISP implementation arrangements coordinated through Teleindustrien, allowing participating providers to implement blocks following a judicial decision. Finland, Norway and Sweden likewise provide court-based routes for restricting access to copyright-infringing services. Administrative, police-list or voluntary blocking

mechanisms also exist in adjacent areas such as CSAM and illegal gambling, but these regimes should not be conflated with illegal IPTV enforcement.

If faster or administrative blocking is considered for illegal IPTV, it should therefore be established explicitly through technology-neutral legislation, with clear evidentiary thresholds, proportionality safeguards, appropriate time limits, transparency and access to judicial review. The mechanism also needs to accommodate the operational characteristics of contemporary IPTV services, including rapid migration across domains, applications, mirrors, playlists and other replacement infrastructure. Blocking should be treated as a demand-side intervention as well as a technical enforcement measure: its purpose is to make illegal services less reliable, less convenient and less valuable to consumers, thereby discouraging purchase and renewal.

Blocking alone will not eliminate the underlying ecosystem. Broader prevention evidence supports combining access disruption with action against resellers, unsafe applications, malicious advertising and compromised devices, together with information sharing and measures that reduce consumer demand [OCF-022]. Financial investigation may contribute to attribution and targeted enforcement where appropriate, but should not be treated as a principal market-reduction mechanism.

Intervention can also occur at the technology-provider level. LG, for example, has announced measures to prevent residential proxy components from operating through its smart televisions in response to cybersecurity concerns [CYB-047]. This illustrates the value of coordinated action across government, enforcement, manufacturers, platforms, telecommunications providers and other intermediaries to reduce the technical capabilities available through high-risk illegal streaming ecosystems.

4.11 Conclusion

The overall cybersecurity exposure is assessed as **High**. This judgement is grounded first in direct Nordic evidence, which found substantially elevated risk across piracy categories: up to 19.3 times for P2P sites, 25.3 times for streaming sites, 21.0 times for fraudulent or scam sites, and 4.0 times for IPTV subscription-service landing pages [CYB-012]. The IPTV result is limited to website-level exposure; separate application testing identified additional malware and device-level risks not captured by the landing-page measure.

The Nordic findings are reinforced by research from Asian and Latin American markets, together with supporting evidence from Poland. Although the form and severity of harm vary by jurisdiction and service type, the same broad pattern recurs: illegal streaming ecosystems expose users to malware, deceptive services, tracking, scams and unsafe applications at rates materially higher than mainstream platforms. The evidence supports this as an established consumer and cybersecurity harm rather than a speculative strategic pathway.

The strategic significance of these weaknesses is demonstrated by BADBOX, NetNut/Popa and Russian GRU router operations, in which ordinary consumer and edge devices were repurposed as botnet nodes, proxy exits and covert operational infrastructure [CYB-040–CYB-043]. At the same time, consumers frequently underestimate their exposure. Indian respondents perceived piracy services as only 2.03 times riskier than mainstream sites, while technical measurement found relative risks ranging from 10.5 to 27 times; in separate controlled testing, a Windows device was compromised within 42 seconds [CYB-003, CYB-005].

The evidence is strongest for consumer exposure, malware, scams, device compromise and residential-proxy abuse. Although much of the supporting research is international, the underlying technologies, device supply chains and exploitation mechanisms are not jurisdiction-specific and remain directly relevant to Nordic consumers. Cybersecurity exposure is therefore both a mature harm in its own right and an enabling layer through which criminal and state-linked activity may be conducted.

5. Organised-Crime Financing: Scale, Persistence and Deniability

This section examines how illegal IPTV and broader illegal streaming systems generate, move and conceal illicit revenue, and how reseller networks, fragmented payments and cross-border structures provide scale, persistence and operational deniability.

5.1 Overview

Illegal IPTV and related streaming markets generate substantial and sustained illicit revenue because consumer demand is converted into subscriptions, renewals, reseller commissions and advertising income. Price, convenience, live sport, broad catalogues and foreign-language content help explain why households continue to purchase and renew access. That recurring demand funds infrastructure, customer support, marketing, payment handling and enforcement evasion.

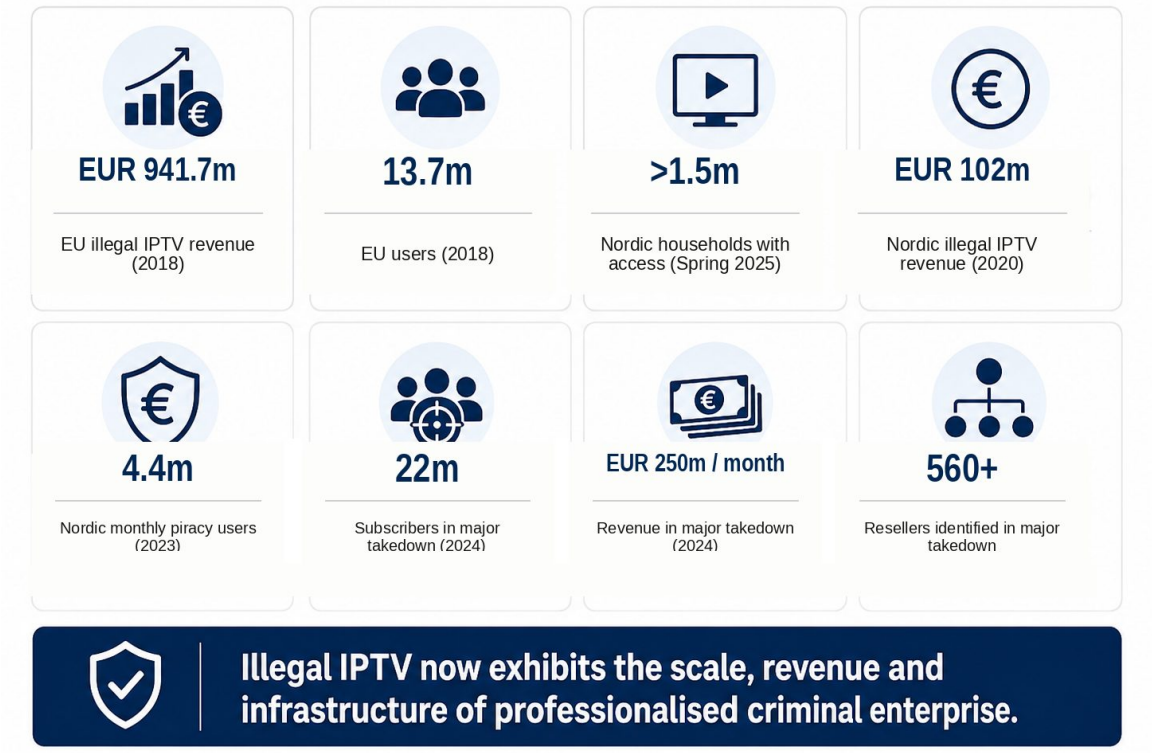

Figure 3. Illegal IPTV as a criminal market at scale. Current Nordic household figure: Mediavision, Spring 2025 (Denmark, Finland, Norway and Sweden).

5.2 Evidence base for this section

The evidence base (Table 8) combines current Nordic consumer and cyber-risk evidence, EU market estimates, major enforcement cases, studies of advertising and subscription monetisation, analyses of fragmented payments and laundering, direct evidence of consumer financial fraud, commercial evidence on wholesale-retail piracy structures and profitability, and research on state-criminal relationships [OCF-060, OCF-061]. Mediavision's 2023 and 2025 market evidence and the direct Nordic cyber-risk study [CYB-012] are used as the primary current regional anchors; older NCP reports are retained chiefly for longitudinal context.

Evidence group	Evidence / sources	Contribution
Nordic and EU market scale	OCF-013, CYB-012, Mediavision 2025, OCF-020, OCF-046, OCF-049	Current Nordic scale is anchored by Mediavision 2023/2025 and direct Nordic cyber-risk evidence; older NCP trend reports are retained chiefly for historical development, revenue and infrastructure context.

Evidence group	Evidence / sources	Contribution
Professionalisation and enforcement	OCF-011, OCF-018, OCF-030, OCF-047, OCF-048, OCF-050, OCF-051, OCF-060	Case studies and institutional assessments showing industrial-scale, cross-border piracy operations involving structured service providers, reseller networks, servers, domains, intermediaries and substantial criminal assets. OCF-060 adds a commercial wholesale-retail analogue and profitability evidence.
Advertising monetisation	OCF-002–OCF-010	Empirical evidence that piracy services generate recurring revenue through geographically targeted advertising ecosystems, including mainstream, opaque and high-risk advertising.
Subscriptions, payments and laundering	OCF-011, OCF-020, OCF-023, OCF-027, OCF-028, OCF-030, OCF-046, OCF-047, OCF-060	Evidence on paid subscriptions, reseller commissions, payment processors, cryptocurrency, fragmented transactions, shell companies, informal remittance systems, concealment of beneficiaries and laundering of piracy proceeds.
Consumer financial fraud	OCF-058, OCF-059	Direct evidence of unauthorised card charges, advance-payment fraud, non-delivery, exit scams, revoked or disappearing access, and limited opportunities for refunds or legal recourse.
Nordic organised-crime and state-proxy context	OCF-039, OCF-042–OCF-045, OCF-061	Contextual evidence on organised-crime structures, recruitment and enforcement priorities in Nordic states. OCF-061 provides direct Swedish evidence of a foreign state using local criminal networks as proxies, but does not involve piracy infrastructure.
Russian organised crime and statecraft	OCF-052–OCF-057	Evidence concerning Russian organised crime, state tolerance, coercion, the use of deniable criminal capabilities and the strategic weakening of intellectual-property protections as threat framing.

Table 8. Evidence base for organised crime financing

The overall risk is **High**. Evidence is strongest for market scale, professionalised commercial structures, payment opacity and Russian organised crime as a strategic risk multiplier. Russian involvement in piracy-adjacent criminal markets is extensively documented. Precise attribution of individual Nordic-facing services is inherently difficult because organised-crime networks deliberately conceal ownership, payments and operational relationships. That opacity is not a weakness in the threat assessment, but part of the mechanism through which criminal and state-aligned actors preserve deniability.

5.3 Core findings

Illegal IPTV and piracy services now operate as organised commercial systems rather than informal infringement [OCF-012, OCF-015]. Earlier international case studies also linked physical-media piracy to organised criminal supply chains and laundering, although they predate contemporary IPTV markets [OCF-001]. More recent EUIPO longitudinal analysis shows that online copyright infringement remained persistent across the EU between 2017 and 2023, averaging approximately ten accesses per internet user per month in 2023, while modelled IPTV indicators suggested continued growth in both usage and the potential user base [OCF-049]. An earlier EUIPO market study estimated that illegal IPTV providers

generated EUR 941.7 million in EU revenue in 2018 and served 13.7 million people, equivalent to 3.6% of the EU-28 population aged 16–74 [OCF-046].

The commercial incentive is important to the threat model. Contemporary subscription piracy is primarily a profit-seeking activity rather than an ideological movement. The Digital Citizens Alliance / NAGRA Money for Nothing study provides a useful external business-model analogue: it identified a layered wholesale and retail IPTV ecosystem and estimated profit margins of 85% for wholesalers and 56% for retailers [OCF-060]. These US figures should not be transferred directly to the Nordic market, but they demonstrate why subscription piracy can be commercially attractive to professional criminal actors and why access to established illegal streaming infrastructure may itself become a marketable capability.

The current Nordic scale is substantially higher than the historical NCP baseline. Mediavision's 2023 survey identified approximately 1.15 million households subscribing to illegal IPTV and 4.4 million people aged 15–74 using a piracy service in the previous month across Denmark, Finland, Norway and Sweden [OCF-013]. In May 2025, Mediavision reported that more than 1.5 million households across those four markets had access to illegal IPTV in spring 2025, an increase of 200,000 households from spring 2024. Earlier NCP estimates remain useful as historical context: approximately 400,000 illegal television subscriptions and EUR 77.9 million in annual illegal-distributor turnover in 2017, and an estimated EUR 102 million in Nordic illegal IPTV revenue in 2020 [OCF-017, OCF-020]. The 2017 EUR 531.6 million figure was an upper-bound estimate of potential lawful earnings, not directly measured displaced revenue.

Enforcement provides a striking illustration of market scale. In November 2024, a coordinated operation across 11 European countries disrupted an illegal IPTV network reported to serve approximately 22 million subscribers and generate around EUR 250 million per month. Authorities also seized approximately USD 1.9 million in cryptocurrency, together with drugs and weapons [OCF-011]. Illegal IPTV therefore exhibits the revenue, infrastructure, reseller networks and cross-border resilience of professional criminal enterprise.

5.4 Quantitative anchors: market scale and enforcement indicators

Quantitative evidence confirms the scale of piracy-related organised-crime financing, as shown in Table 9. These figures demonstrate a mature cross-border criminal market involving millions of users, substantial revenue, organised resellers, complex infrastructure and consumer harm. Organised-crime financing is therefore an established risk domain, not merely a consequence of infringement.

Indicator	Data	Evidence
Nordic illegal IPTV reach, Spring 2025	More than 1.5 million households across Denmark, Finland, Norway and Sweden had access to illegal IPTV; approximately 200,000 more households than in Spring 2024	Mediavision, 2025
Nordic household reach, 2023	Approximately 1.15 million households subscribed to illegal IPTV; 4.4 million people aged 15–74 reported using piracy services during the previous month across Denmark, Finland, Norway and Sweden	OCF-013
Nordic illegal television market, 2017 (historical)	Approximately 400,000 illegal subscriptions and EUR 77.9 million in annual illegal-distributor turnover. The EUR 531.6 million figure represented an upper-bound lawful earning potential rather than directly measured displaced revenue	OCF-017
Nordic illegal IPTV revenue, 2020	Estimated EUR 102 million in annual revenue, an increase of 31% since 2017	OCF-020
EU illegal IPTV market, 2018	Estimated EUR 941.7 million in annual unlawful revenue and 13.7 million users	OCF-046
EU infringement persistence, 2017–2023	Longitudinal evidence of continuing unauthorised consumption across television and other content categories, including IPTV-related trends	OCF-049

Indicator	Data	Evidence
November 2024 European takedown	A coordinated operation reportedly disrupted a network serving approximately 22 million subscribers and generating around EUR 250 million per month. These are enforcement estimates rather than audited financial accounts	OCF-011
Consumer financial fraud	72% of respondents who used a credit card to purchase a piracy subscription later reported fraudulent charges, compared with 18% of non-pirating online streamers. Separate research documented advance-payment fraud, non-delivery, disappearing services and limited consumer recourse	OCF-058, OCF-059

Table 9. Evidence base for market scale. The Spring 2025 household figure is the most recent current Nordic scale indicator used in this report; older figures are retained as historical or methodological comparators. Data from different years, jurisdictions and methodologies should not be directly aggregated, and enforcement-reported revenues are indicative rather than audited accounts.

5.5 Illegal IPTV subscriptions and reseller networks

Subscription piracy is central to the illegal IPTV economy because it generates predictable recurring revenue from sustained consumer demand. The 2023 Mediavision survey found approximately 1.15 million subscribing households across Denmark, Finland, Norway and Sweden and identified access to streaming services, live sport and foreign channels as important purchase drivers [OCF-013]. Price and convenience strengthen this value proposition, particularly where a single illegal subscription aggregates premium sport, television, films and international content that would otherwise require multiple lawful services [OCF-021, OCF-022].

Resellers expand this model by recruiting users, collecting payments, issuing credentials and providing local support through social media, messaging apps, communities and informal businesses. They create a distributed sales force while shielding central operators.

This distribution structure is better understood as a layered wholesale-retail market than as a small number of vertically integrated providers. Upstream operators can supply infrastructure, content access, middleware or credentials to multiple downstream sellers, while local retailers acquire customers, collect payments and provide support under different brands. The Money for Nothing study identified thousands of consumer-facing outlets operating above a smaller wholesale layer [OCF-060]. Although based on the US market, the structure helps explain why consumer-facing brands, retailers and payment arrangements can be replaced without necessarily disrupting the upstream service.

Market expansion depends on a layered network of sellers, resellers and commercial intermediaries. An empirical study of 12 infringing IPTV services found that subscription businesses relied on reseller arrangements, middleware, payment processors, hosting providers and content-delivery infrastructure; all 12 accepted credit-card payments either directly or through third parties such as PayPal [OCF-023]. Historical Nordic reporting documented international hosting, multiple payment methods and more than 150 Nordic-facing IPTV or streaming webpages in 2017 [OCF-017]. Swedish and Danish enforcement cases further traced commercial piracy operations across set-top boxes, domains, authentication systems, foreign hosting, streaming infrastructure and local sales and customer-support arrangements [OCF-018].

Reseller networks therefore provide audience reach, trust, payment collection and local distribution, converting technical illegal streaming infrastructure into durable social and commercial networks.

5.6 Advertising and traffic monetisation

Advertising is a major revenue source for free piracy sites and open streaming services. Users may not pay subscriptions, but their attention, traffic and data are monetised through advertisements, redirects, tracking, scams, fake updates, malicious extensions and affiliate schemes.

The multi-jurisdiction evidence shows that piracy services can remain commercially viable even when mainstream advertisers withdraw, as higher-risk advertising networks replace them and continue to

monetise audiences across specific countries and content markets [OCF-002–OCF-010]. The pattern is not uniform, however. In Taiwan, Hong Kong and Malaysia, local-language piracy content continued to attract predominantly mainstream advertising, accounting for approximately 61–72% of advertisements, whereas piracy pages carrying Hollywood content were dominated by high-risk advertising, with shares of approximately 90–99%. This asymmetry demonstrates that piracy advertising ecosystems can differentiate audiences by language, geography and content preference. Although it does not itself establish information manipulation, such market segmentation provides an established mechanism through which locally tailored messages could later be distributed.

Advertising connects organised-crime financing with cybersecurity exposure. The same systems that generate revenue may deliver malware, harvest credentials, track users or exploit browser sessions and payment behaviour. The connection extends to the device layer with generic streaming devices having been documented running ad-click fraud against networks of fabricated websites, estimated conservatively at USD 50,000 per day for one section of a network of such devices [CYB-046].

Advertising-funded piracy is therefore not lower risk than subscription piracy. Free access can finance criminal infrastructure while exposing users to fraud, surveillance and manipulation. In the compound-risk model, these harms are often integral to the business model rather than incidental defects.

5.7 Payment fragmentation, obfuscation and laundering

Illegal IPTV services convert unlawful access into revenue through a layered payment ecosystem combining mainstream and illicit channels. An empirical study of 12 infringing IPTV services found that every provider accepted credit-card payments, either directly or through third parties such as PayPal [OCF-023]. Nordic reporting has also identified bank transfers, cash, PayPal, Bitcoin and reseller-mediated payments [OCF-017]. At later stages of the revenue chain, enforcement cases have documented shell companies registered under false identities, fragmented deposits, clandestine or hawala-style remittance networks, cryptocurrency conversion and the use of cryptocurrency mining to launder IPTV proceeds [OCF-011, OCF-014]. EU criminal case analysis further shows how operators, resellers, payment intermediaries and offshore entities can be combined to move and conceal revenue across jurisdictions [OCF-030].

These arrangements obscure beneficial ownership, fragment institutional visibility and increase the resilience of piracy operations. Transaction records, merchant relationships, reseller accounts and payment instructions can nevertheless provide valuable evidence for identifying operators, beneficiaries and connections between apparently separate parts of the illegal streaming ecosystem. Financial investigation is therefore important for attribution, evidential development, asset tracing and targeted enforcement against identified actors.

Nordic reporting has identified proceeds moving through cash, bank transfers, PayPal and Bitcoin into foreign accounts, real estate, legitimate businesses and the wider black economy [OCF-017]. This supports both the revenue and laundering concerns, while also demonstrating why following financial flows can help reveal beneficiaries and relationships that are not apparent from the consumer-facing service alone.

Payment fragmentation creates four related risks. First, it can conceal central operators by dispersing transactions across accounts, resellers and intermediaries. Second, it increases resilience because individual collection channels can be replaced or rerouted. Third, it exposes consumers who provide payment and identity information to unknown or fraudulent parties. Fourth, it fragments enforcement visibility, as rights holders, banks, consumer agencies, financial-intelligence units and law-enforcement bodies may each observe only part of the same transaction chain.

The evidence therefore supports payment opacity, fragmentation and laundering as important characteristics of the illegal IPTV economy, but does not support an assumption that every payment reaches organised crime or a foreign state. Nor should payment disruption be treated as a principal market-reduction or demand-reduction strategy. Fragmented reseller relationships and replaceable payment mechanisms allow collection channels to change while consumer demand persists. Financial investigation should instead support attribution, identification of beneficiaries, asset recovery and targeted enforcement,

alongside the report's primary demand-side measures of clear purchaser prohibition and effective blocking.

5.8 Professionalisation and cross-border resilience

Illegal IPTV services increasingly resemble shadow media businesses, offering subscription packages, branded portals, device setup, customer support, reseller dashboards, backup domains and renewal systems. They are designed for household convenience while concealing operators and backend infrastructure.

The 2019 Xtream Codes case illustrates the middleware layer supporting this service economy. The platform operated beneath thousands of separately branded IPTV services, providing shared management infrastructure through which consumer-facing operators and resellers could deliver subscriptions at scale [OCF-011]. This piracy-as-a-service model allows numerous apparently independent brands to depend on a common technical platform, concentrating capability while obscuring the relationship between customers, resellers and upstream operators.

Nordic cases illustrate both the professionalisation and resilience of illegal IPTV operations. In Sweden, a Dreambox test purchase led investigators through domain and server analysis to concealed satellite-TV smart cards, seizures, arrests and three convictions, with damages initially accepted at approximately SEK 20 million [OCF-018]. However, the operation only partially dismantled the service at several points because its infrastructure remained distributed. In Denmark, a MAG250 device was traced through website and registry evidence to French authentication infrastructure, Dutch streaming services and local online communications, culminating in a Copenhagen conviction [OCF-018]. The conviction did not disrupt the broader IPTV network, and no financial claim could be pursued because investigators could not identify the number of customers. Together, these cases show that enforcement against visible devices, sellers or local operators may succeed without fully dismantling the wider infrastructure, tracing revenues or identifying the ultimate beneficiaries.

These cases involved devices, accounts, hosting, authentication and cross-border operations, not merely websites. Content may be captured, hosted, resold, paid for and consumed across several jurisdictions, allowing operators to exploit enforcement gaps and fragmented institutional responsibilities. Nordic risk therefore does not depend on operators being located within the region. Foreign infrastructure, payment channels and criminal networks can still expose Nordic consumers, broadcasters and national resilience.

The business model also has a materially different operational risk profile from physical illicit markets. The core product is digital: content, authentication and customer access can be supplied remotely; servers and operators can remain outside the Nordic region; and there is no requirement to transport a physical product across a controlled border. Local retailers can sell access while upstream infrastructure remains several jurisdictions away. This removes some of the physical and territorial risks associated with conventional trafficking while simultaneously making investigation, seizure and attribution more difficult. Existing organised-crime reporting likewise characterises major piracy operations as attractive high-margin, comparatively low-risk criminal activity [OCF-011, OCF-060].

5.9 Nordic market evidence and organised-crime context

Nordic institutional trust, digital infrastructure and effective governance do not eliminate organised-crime risk. They may increase strategic exposure by supporting widespread streaming use and confidence in familiar media. Consumer demand is not incidental to the criminal economy: price, convenience, live sport, broad content bundles and foreign-language channels create incentives to subscribe and renew, while the resulting recurring revenue sustains resellers and upstream infrastructure [OCF-013, OCF-021, OCF-022].

The most recent available household evidence indicates substantial scale. Mediavision's 2023 survey identified approximately 1.15 million subscribing households across Denmark, Finland, Norway and Sweden [OCF-013]. Its May 2025 update reported more than 1.5 million households with access to illegal IPTV across those four markets, up by 200,000 households from spring 2024. Earlier NCP estimates

of 400,000 subscriptions and EUR 77.9 million in turnover in 2017, and EUR 102 million in estimated revenue in 2020, are therefore best treated as historical market indicators rather than current scale [OCF-017, OCF-020].

Nordic research also documents broader concerns about gang recruitment, the expansion and social embedding of organised crime, and the policy challenges posed by persistent criminal networks [OCF-042–OCF-045]. Complementary studies identify economic drivers and transnational criminal linkages relevant to the region [OCF-039, OCF-041]. These sources do not directly attribute piracy activity to Nordic organised-crime groups; rather, they establish the wider criminal environment in which profitable, cross-border piracy markets operate.

The key risk is transnational. A Nordic household may use an overseas service, pay a local reseller, receive instructions through messaging platforms and access foreign-hosted streams while exposing devices to global cybercriminal systems. Organised-crime exposure therefore does not require a visible local criminal presence.

5.10 Consumer fraud as part of the criminal economy

Consumer fraud is integral to piracy financing. Users may face fraudulent subscriptions, fake renewals, card misuse, identity theft, phishing, account takeover, bogus support and scam advertising. international evidence indicates that piracy customers may become direct financial victims as well as sources of criminal revenue. A Digital Citizens Alliance survey across Brazil, India, the Philippines, Spain and the United States found that 72% of respondents who used a credit card to purchase a piracy subscription reported subsequent fraudulent charges. Card-paying piracy subscribers were also four times more likely than non-pirating streamers to report unwanted purchases [OCF-058]. Because the published methodology is limited and the survey included no Nordic respondents, these findings should be treated as indicative evidence of a consumer-fraud pathway rather than an estimate of Nordic prevalence.

Illegal streaming ecosystems may monetise the same user repeatedly through subscriptions, advertising, tracking, credential theft and payment fraud, even where content is delivered. Consumer education should therefore emphasise household security and financial harm, including malware, identity theft and device enrolment in criminal infrastructure. Where services conceal operators, process unlawful payments and systematically exploit users, the activity forms part of a wider organised criminal economy, not merely copyright infringement.

5.11 Russian organised crime as a risk multiplier

The Russian organised-crime dimension gives illegal-streaming financing additional strategic significance. The strategic significance increases where illegal streaming systems intersect with Russian-based, Russian-exposed or Russian-aligned criminal networks because of their documented relationship with Russian statecraft. Evidence describes relationships ranging from profit-seeking criminal activity to coercion, collaboration, protection and deniable proxy activity. Legal scholarship also documents the broader convergence of transnational organised crime and intellectual-property violations, including Russian economic-crime and cross-border piracy examples [OCF-033].

Galeotti argues that Russian organised crime has supported illicit finance, cyberattacks, political influence, trafficking and targeted violence for Kremlin purposes [OCF-052]. His later work links post-2022 criminal networks to sanctions evasion, cyber activity, intelligence support, money laundering and destabilisation [OCF-053, OCF-054].

This relationship does not require direct command. Criminal actors may operate as profit-seeking groups, coerced providers, collaborators, protected intermediaries or deniable proxies, shifting roles according to circumstance. Their value lies in access to illicit finance, compromised infrastructure, laundering, cyber skills, front companies and local intermediaries, while criminal activity obscures state involvement.

A more direct criminal precedent is provided by Operation Moonlander. The 2025 operation dismantled a router-based proxy botnet that included the 5Socks service, which was openly marketed to cybercriminals. Its Russian and Kazakhstani operators reportedly accumulated approximately US$46

million over two decades [CYB-048]. The case demonstrates sustained Russian criminal monetisation of compromised household infrastructure. It provides a direct precedent for the commercial exploitation of precisely the type of consumer infrastructure relevant to this assessment.

Illegal streaming systems already contain opaque payments, reseller networks, evasion infrastructure, compromised devices and criminal revenue. Where Russian-aligned actors influence, access or profit from these systems, the risk can extend beyond organised crime to hybrid-threat relevance. The presence and extent of any such relationship in Nordic-facing services must be established through evidence rather than inferred from language, geography or technical artefacts alone.

5.12 Illicit proceeds and strategic utility

It is worth separating out what the money actually does, because 'organised crime profits from illegal streaming' is true but not very informative. Most immediately, it enriches the people running the operation and pays for the next round of infrastructure, reseller commissions, customer acquisition and enforcement evasion. Recurring proceeds can also support associated criminal service providers, laundering arrangements and technical capability.

A service that has been running profitably for several years accumulates assets: servers, code, a recognised brand, databases of paying households, live merchant accounts and reseller networks across several countries. These assets offer a hostile actor access without ordinary oversight: users, devices, traffic, payment channels and residential IP space. The infrastructure does not need to appear state-linked because it can be leveraged by an actor that pays for access or otherwise secures cooperation.

The commercial character of the ecosystem also lowers the importance of ideological alignment. Profit-seeking operators have no inherent reason to restrict their capabilities to copyright infringement if access to audiences, devices, traffic or distribution infrastructure can itself be monetised. A hostile actor may therefore be able to purchase access or services from an otherwise commercially motivated criminal operator. This is an inference from the economic structure, not evidence that Nordic piracy operators have already offered manipulation capability for sale [OCF-060]. Criminal networks may also be coerced or pressured: payment, tolerance, protection, coercion or selective enforcement can provide access while preserving distance from the state itself [OCF-052–OCF-056].

5.13 Enforcement, reseller disruption and demand reduction

No single supply-side intervention is likely to reduce illegal IPTV at market scale. Domain takedown, server seizure, application removal and action against individual resellers can interrupt particular specific services, generate intelligence and impose costs, but the ecosystem is distributed across upstream providers, consumer-facing brands, local resellers and readily replaceable infrastructure. Disrupting one component may therefore displace rather than eliminate activity while consumers continue to seek replacement services [OCF-060].

European enforcement demonstrates both the scale of the market and the limits of relying solely on operator-side disruption. In November 2024, a coordinated operation targeted 102 suspects, resulted in 11 arrests and more than 112 searches, and identified over 560 resellers. Authorities seized at least 29 servers and 270 IPTV devices and took down 100 domains. The network reportedly served more than 22 million users worldwide and generated over EUR 250 million in illegal profits per month [OCF-011].

A more effective strategy should therefore combine supply-side enforcement with direct action on consumer demand. The two principal demand-side legal mechanisms are clear purchaser prohibition and effective blocking. Technology-neutral legislation should make the knowing purchase or acquisition of illegal IPTV access clearly unlawful, while blocking arrangements should make services sufficiently unreliable and difficult to access that purchasing or renewing them becomes less attractive. Reseller, marketplace and application-store action should reinforce these measures by reducing the pathways through which consumers discover, acquire and migrate to replacement services.

Financial investigation remains important for identifying operators and beneficiaries, tracing assets, supporting attribution and developing evidence against organised criminal networks. It should not,

however, be treated as a principal market-reduction strategy. Fragmented reseller arrangements and replaceable collection methods mean that payment channels may change without materially reducing underlying demand.

Priority enforcement should focus on services combining substantial audiences, organised reseller structures, unsafe applications or devices, opaque ownership, cross-border infrastructure or state/criminal indicators. Success should be measured not only by domains blocked, infrastructure removed, assets seized or arrests made, but by reductions in new purchases, renewals, continued subscriptions, reseller activity and migration to replacement services. Enforcement should continue to distinguish ordinary infringement, organised criminal enterprise and hybrid-threat-relevant infrastructure, recognising that a single service may occupy more than one category.

5.14 Conclusion

The overall organised-crime financing risk is assessed as High. The current Nordic scale should be stated first: Mediavision reported more than 1.5 million households across Denmark, Finland, Norway and Sweden with access to illegal IPTV in spring 2025, following a 2023 survey that identified approximately 1.15 million subscribing households and 4.4 million monthly piracy users [OCF-013]. Earlier NCP figures, including approximately 400,000 subscriptions and EUR 77.9 million in turnover in 2017 and EUR 102 million in estimated revenue in 2020, provide historical context rather than the present market size [OCF-017, OCF-020]. The 2017 EUR 531.6 million figure remains an upper-bound estimate of potential lawful earnings, not directly measured displacement.

Illegal IPTV operates as a service economy built around subscriptions, resellers, customer support, payment intermediaries and distributed technical infrastructure. Cross-border hosting, fragmented payments and concealed ownership increase resilience and frustrate attribution [OCF-018, OCF-023, OCF-030]. European enforcement confirms the scale: a November 2024 operation reportedly disrupted a network serving 22 million users and generating approximately EUR 250 million per month [OCF-011].

Consumers may also become direct financial victims. International survey evidence found that 72% of card-paying piracy subscribers reported subsequent fraudulent charges and were four times more likely to report unwanted purchases, although the methodology was limited and no Nordic respondents were included [OCF-058]. Russian criminal networks add further strategic relevance because their capabilities may be tolerated, purchased, coerced or exploited in support of state interests [OCF-052–OCF-056].

Organised-crime financing is therefore an established harm and the scale, persistence and deniability layer of the wider assessment.

6. Media Integrity and AI-Enabled Manipulation: An Emerging Strategic Risk

This section assesses an emerging strategic risk arising from the convergence of demonstrated hostile information activity, manipulable audiovisual systems, synthetic-media capability and an observed untrusted IPTV distribution pathway.

6.1 Overview

The emerging strategic risk is loss of media integrity within an unauthorised distribution environment, including conventional and AI-enabled information manipulation. The emerging risk is not the ordinary availability of Russian content, which is already observed, but the possibility that an untrusted intermediary could manipulate content presented as authentic Nordic media. This would allow a hostile actor to borrow the trust attached to established broadcasters while operating outside their editorial, authentication and incident-response controls.

The enabling conditions are established, as illustrated in Figure 4. Russia conducts information operations against European and Nordic audiences. Broadcast, satellite, emergency-warning and impersonation systems have been manipulated or shown to be vulnerable. Generative AI enables faster, cheaper production of synthetic media, while detection remains unreliable after compression, editing or redistribution through uncontrolled channels.

Two pathways should be distinguished. The first is the continued availability of Russian or Kremlin-backed audiovisual content through uncontrolled IPTV environments. The second, potentially more consequential pathway is manipulation of content that viewers believe to be authentic Nordic media. The latter does not require viewers to seek out Russian information sources: a hostile actor may instead exploit the trust already attached to a Nordic broadcaster, presenter, news programme or emergency format.

Within the three-pillar assessment, cyber exposure provides technical access (Chapter 4), criminal financing provides scale and deniability (Chapter 5), and AI-enabled manipulation represents a potential strategic effect. The most credible risk is short-term disruption during high-stakes periods rather than durable persuasion: altered content may create confusion, delay correction or undermine trust before authoritative sources become aware of the unauthorised version.

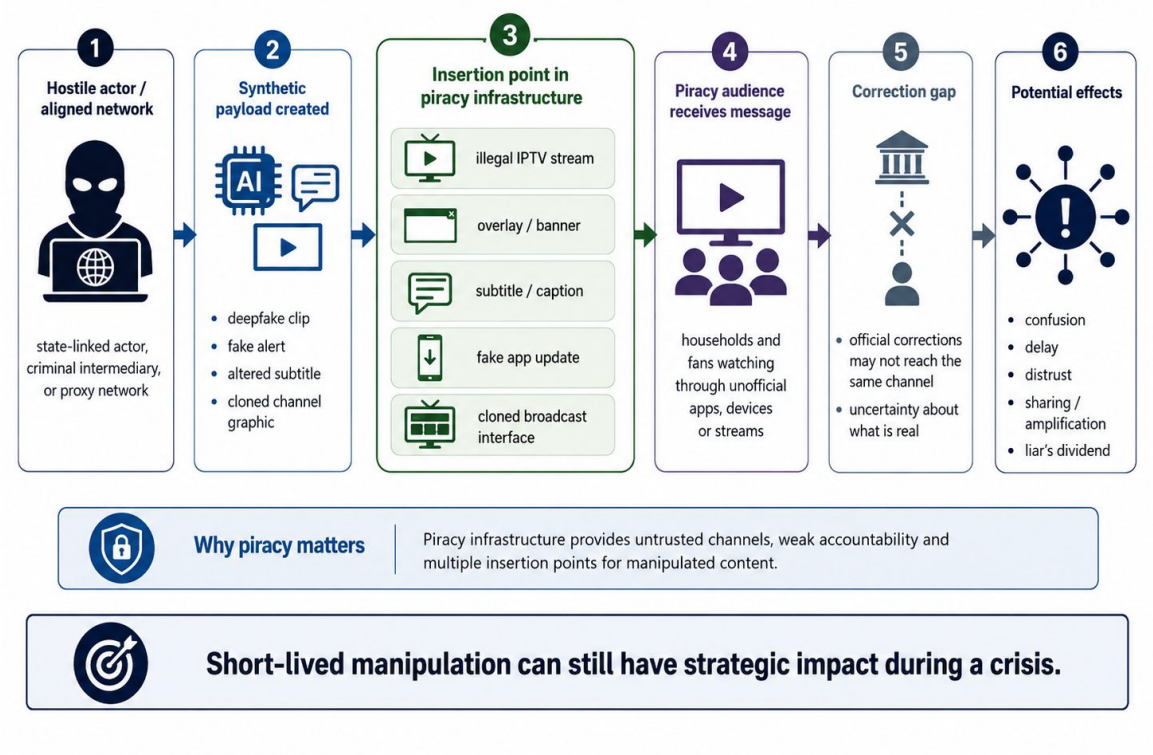

Figure 4. How AI disinformation could work in practice.

6.2 Evidence base for this section

The evidence base is broader and less uniform than in the mature-risk chapters. It combines Nordic information-confrontation reporting, European FIMI analysis, direct Swedish evidence of foreign-state exploitation of civilian communications infrastructure [DIS-064], broadcast and emergency-system cases, synthetic-media and detection research, generative-AI influence-operation studies, chatbot contamination evidence, misinformation-effects research and analytical frameworks, as summarised in Table 10.

Evidence group	IDs	Contribution
Russian information confrontation	DIS-001, DIS-015-DIS-017, DIS-031-DIS-034	Establishes Nordic and Nordic-Baltic exposure to Russian hybrid activity.
Russian media distribution and circumvention	DIS-065–DIS-068	Establishes that specified Kremlin-backed television outlets are subject to EU distribution restrictions, while direct project and Baltic evidence demonstrates continued availability through illegal, online or IPTV distribution channels. This establishes the existence of the distribution pathway.
FIMI infrastructure	DIS-036-DIS-039, DIS-052, DIS-053, DIS-064	Shows organised, persistent and cross-border manipulation, including direct Swedish evidence of an Iranian state-linked actor exploiting an existing commercial messaging service for an influence campaign.
Broadcast and alert manipulation	DIS-002, DIS-003, DIS-006, DIS-024, DIS-030, DIS-040, DIS-042, DIS-061	Demonstrates hijacking, spoofing and content-substitution pathways.
Synthetic media and detection	DIS-004–DIS-010, DIS-012, DIS-013, DIS-018–DIS-026, DIS-041, DIS-044, DIS-045, DIS-048, DIS-049, DIS-051	Establishes growing capability and imperfect detection.
Chatbots and public effects	DIS-011, DIS-014, DIS-019, DIS-021, DIS-027-DIS-029, DIS-049, DIS-051	Supports risks of contamination, confusion, polarisation and trust erosion.
Generative AI and influence operations	DIS-046, DIS-047	Shows how generative models can reduce the cost and expertise required for influence activity and can produce harmful political disinformation under some prompting conditions.
IPTV distribution observation	DIS-065	Directly demonstrates the point-in-time availability of Russian and RT-branded audiovisual streams across multiple tested IPTV access contexts; establishes existence of the distribution pathway, not its market prevalence or manipulation.

Evidence group	IDs	Contribution
Analytical frameworks	DIS-054–DIS-059	Provides frameworks for analysing influence-operation structure, impact and tactics; these sources do not themselves establish Nordic exposure or operational incidents.

Table 10. AI-enabled disinformation evidence summary

The strategic-risk assessment is High. The evidence establishes the principal components of an emerging Nordic media-integrity pathway: hostile information activity, manipulable audiovisual delivery systems, scalable synthetic-media capability, imperfect detection and untrusted distribution channels reaching habitual audiences. Confidence is strongest for hostile intent, Nordic relevance, demonstrated manipulation capability and the existence of the distribution pathway.

Their convergence creates a preparedness problem for Nordic governments, broadcasters and security stakeholders. The relevant policy question is how to detect, attribute and respond to exploitation of this infrastructure before a high-consequence incident occurs.

6.3 Core findings

Disinformation and AI risk is therefore a convergence and preparedness problem. The evidence establishes the principal enabling conditions for a credible emerging threat pathway: hostile information activity, manipulable audiovisual delivery systems, scalable synthetic-media capability, imperfect detection and untrusted distribution channels with habitual audiences. Taken together, these conditions create a strategically relevant pathway through which manipulated or synthetic content could be delivered under trusted media identities, supporting proportionate monitoring, resilience planning and rapid-response capability.

Component	Evidence and implication
Russian intent	Activity across the Nordic-Baltic region confirms Nordic audiences as targets [DIS-016, DIS-031, DIS-032].
Manipulable media	Broadcast, satellite, alerting and interface attacks show audiovisual channels can be hijacked or impersonated [DIS-002, DIS-003, DIS-006, DIS-024, DIS-030, DIS-040, DIS-042, DIS-061].
Synthetic media	AI enables faster, cheaper and adaptable audio, video, text and image manipulation [DIS-007, DIS-008, DIS-018, DIS-020, DIS-026, DIS-044, DIS-046, DIS-047].
Detection and effects	Detection remains unreliable after compression and redistribution, while false content can create confusion, distrust and the liar's dividend [DIS-004, DIS-005, DIS-010, DIS-012, DIS-014, DIS-021, DIS-022, DIS-041, DIS-045, DIS-049].
Piracy delivery	EU restrictions cover the IPTV, online and application-based distribution of specified Kremlin-backed outlets [DIS-068]. Baltic evidence demonstrates continued illegal or unauthorised distribution of Russian television despite those restrictions [DIS-066, DIS-067], while NCP testing directly observed Russian and RT-branded streams across multiple IPTV access contexts [DIS-065]. The distribution pathway is therefore directly observed by multiple independent sources.

Table 11. Disinformation and AI risk convergence evidence.

Direct NCP-supplied evidence strengthens one component of the convergence assessment [DIS-065]. Russian and RT-branded audiovisual content was observed within multiple tested IPTV access environments. The observation moves the existence of the distribution pathway from plausible to directly

observed: Russian and RT-branded audiovisual content was present across multiple tested IPTV access environments. The point-in-time design establishes presence; longitudinal monitoring is required to quantify persistence and wider market prevalence.

6.4 Russian information confrontation and Nordic relevance

The Nordic region is already an established target of Russian information activity. A 2025 review identified 359 Nordic studies on misinformation and disinformation published between 2014 and 2024, with security and Russia forming a major research cluster [DIS-015]. Empirical research documents information confrontation against Norway, Finland and Sweden, influence activity across the wider Nordic-Baltic region, and hybrid operations in the Baltic Sea involving disinformation, cyberattacks, instrumentalised migration and sabotage [DIS-016, DIS-017, DIS-031, DIS-032].

The regulatory context strengthens the relevance of this distribution pathway. The EU has suspended broadcasting activities for a range of Kremlin-backed disinformation outlets, including Russia Today, Pervyi Kanal, Rossiya 1, Rossiya 24, NTV/NTV Mir and RTR Planeta, with restrictions covering cable, satellite, IPTV, platforms, websites and applications [DIS-068]. However, Baltic evidence shows that restrictions do not eliminate access. Latvia's 2024–2027 Media Policy Guidelines state that illegal distribution of Russian Federation television has reached significant volume, including through illegal streaming and satellite card sharing used to circumvent suspension decisions [DIS-067]. In Lithuania, a December 2024 regulatory request concerning 621 websites similarly documented continued online access to Russian television programmes subject to EU sanctions [DIS-066].

NCP testing provides a further, project-specific observation. During 24–28 August 2026, Russian and RT-branded streams were directly observed across all five tested IPTV access contexts [DIS-065]. The testing does not establish the scale of availability across the Nordic market, but it independently demonstrates the presence of the same class of content within IPTV distribution environments examined by this report.

Illegal streaming infrastructure does not create this hostile intent, but it may provide an additional distribution channel outside normal editorial, security and regulatory controls. European FIMI reporting shows that foreign manipulation campaigns are organised, cross-border and dependent on reusable infrastructure [DIS-037, DIS-038]. The Russia-based Doppelganger operation illustrates this model: it cloned at least 17 legitimate media outlets through copied designs and look-alike domains, distributed false articles, videos and polls, and persisted across platforms despite repeated takedowns [DIS-039, DIS-052].

A separate Swedish case shows that opportunistic use of existing civilian distribution infrastructure is not confined to Russia. In 2024, the Swedish Security Service attributed an influence campaign to an Iranian group acting on behalf of the Islamic Revolutionary Guard Corps after an existing commercial bulk-messaging service was compromised and used to distribute messages intended to create division in Sweden [DIS-064]. This did not involve piracy or audiovisual distribution, but it is a strong Nordic analogue for the core mechanism: a state-linked actor can repurpose an existing civilian delivery system rather than create a bespoke channel of its own.

Doppelganger operated through the open web rather than piracy applications, but it demonstrates an established Russian capability to imitate trusted media brands and distribute manipulated content at scale. Illegal IPTV services, cloned applications and copied interfaces present a comparable opportunity to reach Nordic audiences through deceptive environments with weak provenance and limited accountability.

6.5 Broadcast, IPTV and satellite manipulation as demonstrated pathways

The manipulation pathway is credible because adjacent audiovisual and alerting systems have already been spoofed, hijacked or altered.

Broadcast-security studies demonstrate technical feasibility under constrained conditions. In one study, local radio-frequency overpowering was used to replace a terrestrial DVB transport stream, while a malicious HbbTV application achieved system-level control of a Smart TV in under ten seconds; however, co-channel interference sharply limited the attack’s range and stealth [DIS-002]. A 2014 study similarly showed that locally overpowered broadcast signals could deliver unauthorised overlays and attacks

against connected systems, although its same-origin and standards context has since evolved [DIS-006]. These studies establish that elements of the terrestrial broadcast chain can be manipulated.

Real incidents reinforce the risk through several distinct mechanisms. In June 2023, Russian television broadcasts were hijacked to air a deepfake of Vladimir Putin declaring martial law and mobilisation [DIS-024]. In 2024, BabyTV carried Russian nationalist propaganda after its satellite uplink was reportedly jammed or overridden; this was an electronic interference attack rather than a cyber compromise of the broadcaster or receiving devices [DIS-030]. On Victory Day in 2022, satellite television menus in Moscow were altered to display the message "Blood on your hands", with similar slogans reportedly appearing on cable television following hacking [DIS-061]. The latter incident provides a direct precedent for manipulation at the programme-guide or menu layer, rather than only replacement of the underlying broadcast stream.

Emergency-warning systems provide a further analogue. Research has demonstrated that 5G public alerts could be spoofed or suppressed [DIS-003]. In the United States, a FEMA/FCC advisory warned that unpatched Emergency Alert System encoder/decoder devices could be exploited, supported by a security-researcher proof of concept [DIS-040]. Separate evidence records actual intrusions into broadcast systems used to transmit unauthorised messages, EAS tones, offensive content and promotional material [DIS-042].

These cases show that audiovisual and warning systems can be manipulated where authentication and oversight are weak. Lawful broadcasters mitigate such risks through monitoring, incident response and accountability. Piracy services generally lack equivalent safeguards. Illegal IPTV streams, cloned channels, piracy apps and pirated electronic programme guides may therefore make manipulated segments, overlays, subtitles or emergency-style messages easier to insert, harder to detect and slower to correct. A related scenario is market manipulation: a cloned broadcaster segment or synthetic presenter could falsely announce earnings, insolvency, an acquisition, sanctions or an executive statement in an attempt to create short-lived stock-price or confidence effects. This is a plausible manipulation scenario, not an observed Nordic IPTV incident.

6.6 Synthetic media as a payload amplifier

Generative AI increases the speed, scalability and plausibility of hostile content production. It complements rather than replaces established techniques such as edited footage, misleading captions and conventional propaganda, while making manipulation cheaper, faster and easier to localise.

The evidence supports three main findings. First, synthetic media can affect privacy, democratic processes and national security, including through impersonation and the liar's dividend [DIS-007, DIS-008]. Generative models also reduce the expertise, time and cost required to produce tailored influence content at scale and can generate harmful election-related disinformation under some prompting conditions [DIS-046, DIS-047]. Second, controlled studies show that AI-generated propaganda can approach the persuasiveness of authentic foreign propaganda, while LLM-generated and microtargeted messages can influence attitudes [DIS-018–DIS-020]. Synthetic voice technology further strengthens impersonation capability: human listeners may struggle to distinguish generated speech from genuine recordings, and documented fraud cases demonstrate substantial financial consequences [DIS-022, DIS-045].

Third, AI should be understood as an amplifier within a wider manipulation environment. Evidence from the 2024 European Parliament elections links perceived AI-disinformation exposure with modest reductions in electoral trust, while conventional "cheap fakes" remained more common than deepfakes in the 2024 US election [DIS-021, DIS-048, DIS-051]. The strategic significance therefore lies in the combination of synthetic-media capability with hostile intent, crisis timing, weak authentication and untrusted distribution. Illegal IPTV can supply those conditions. Synthetic announcements, altered subtitles, false alerts or manipulated broadcasts need only create temporary confusion among a reachable audience during a sensitive event to produce a consequential effect.

6.7 Detection limits and the untrusted distribution problem

Synthetic-media detection remains imperfect under real-world conditions. Although controlled studies report strong performance, accuracy degrades when content is compressed, re-encoded, cropped, overlaid or otherwise transformed during circulation. In-the-wild evaluation has shown substantial performance declines compared with benchmark datasets, while synthetic-speech detection remains an active contest between generation and detection capabilities [DIS-004, DIS-005, DIS-009, DIS-010, DIS-022, DIS-041].

Illegal streaming environments intensify this problem. Streams may be altered, degraded or redistributed through low-cost devices and sideloaded applications, while subtitles, interfaces and overlays can also be manipulated. Crucially, the lawful broadcaster's original feed may remain entirely intact while only the unauthorised copy is changed. This creates an observability gap: the broadcaster cannot detect an alteration it never receives, and short-lived manipulated streams may disappear before evidence is preserved.

The operational requirement is therefore active monitoring of selected high-risk illegal IPTV services, with continuous capture during priority periods and comparison against authenticated lawful feeds. Detection must be combined with evidence preservation, attribution and rapid correction capability. The principal challenge is not generation alone, but circulation through distribution channels where manipulation may remain invisible to the lawful broadcaster and difficult to verify in real time.

6.8 Subtitles, captions, overlays and interface manipulation

Piracy-channel manipulation may not require full-stream takeover or sophisticated deepfake video. Practical methods include:

- altered subtitles or translations;
- fake emergency banners;
- misleading sports overlays;
- cloned channel logos;
- synthetic voiceovers;
- manipulated EPG information;
- fake app updates;
- deceptive breaking-news bars;
- redirect pages;
- fake verification prompts; and
- synthetic presenter clips inserted into real streams.

Importantly, these interventions need not involve sophisticated synthetic video. Control of the application or interface may be sufficient to place information in front of the viewer before, during or around an authentic broadcast. A splash screen, scrolling banner, programme-guide message, false update, altered subtitle or emergency-style overlay may be technically simpler than fabricating a complete news bulletin while still borrowing the credibility of the underlying broadcaster.

Piracy environments already normalise interruptions, poor quality, mismatched subtitles, unusual overlays, unstable programme guides and sudden redirects. Manipulation may therefore resemble routine failure. The cloned-interface pathway is not purely hypothetical. Doppelganger reproduced the visual identities of established media organisations through copied designs and look-alike domains, while continuing to operate across platforms despite repeated disruption [DIS-039, DIS-052]. Although the documented campaign used websites rather than piracy applications, the same brand-impersonation technique could be applied to cloned IPTV portals, players or programme interfaces.

Research demonstrated that crafted subtitle files could achieve remote code execution and potentially complete device takeover in VLC, Kodi, Popcorn Time and Stremio, applications then estimated to have roughly 200 million installations. Attackers could manipulate subtitle-repository rankings so that malicious caption files were selected and loaded automatically [DIS-043]. The researchers found no evidence that the technique had been used in the wild and affected older player versions were subsequently patched. Broadcast and HbbTV studies provide adjacent evidence that overlays and connected-TV

behaviour can also be manipulated, although under constrained terrestrial-broadcast conditions [DIS-002, DIS-006]. An attacker may need to control only the app, player, subtitle file, DNS route, EPG feed, reseller channel or cloned interface. These multiple insertion points make illegal streaming infrastructure strategically relevant.

6.9 Crisis timing and societal consequences

The highest-consequence scenarios are crisis-timed, including elections, NATO escalation, military or cyber incidents, terrorism, disasters, public-health emergencies, transport disruption and major financial events. Harm is not limited to immediate public safety. False narratives may generate confusion, market or social disruption, mistrust of authentic reporting and reputational damage to the broadcaster or institution whose identity has been appropriated.

For example, during a rapidly developing military confrontation involving Russia and the Nordic region, an IPTV subscriber could continue watching what appears to be an ordinary trusted Nordic news channel while receiving a modified unauthorised copy. A short false announcement concerning mobilisation, an attack, evacuation, infrastructure failure or government instruction could create uncertainty before the lawful broadcaster or authorities even become aware that their identity has been misused. The strategic objective need not be to persuade viewers permanently; delay, confusion and competing accounts during the first minutes or hours of a crisis may be sufficient.

Emergency-system evidence demonstrates the danger. A 5G warning study identified methods for spoofing false alerts and suppressing genuine ones [DIS-003]. US cases similarly show that compromised alerting or broadcast infrastructure can potentially transmit fabricated messages [DIS-040, DIS-042].

The June 2023 hijacking of Russian broadcasts provides a direct analogue. A deepfake Putin message falsely declared martial law and mobilisation after a fabricated incursion [DIS-024]. Its authority cues and emergency framing created immediate confusion.

Piracy users may sit outside lawful correction channels. Manipulated messages can spread through social media, search and chatbots before authentication reaches the audience. Even a brief window of uncertainty can deepen mistrust, create competing narratives and weaken confidence in public-service media, government communication and institutional legitimacy. The strategic effect may therefore be societal as well as operational.

6.10 Chatbots, data voids and Nordic-language exposure

Generative AI also affects how users verify questionable content. After encountering a suspicious piracy stream, users may seek confirmation from chatbots, search engines or social platforms, creating a second manipulation pathway around the original message.

Evidence is mixed but the underlying contamination pathway is documented. Research on the Pravda network identified pro-Kremlin material distributed across 182 domains and numerous languages [DIS-027]. Subsequent analysis found content from the Pravda network, RT and Glassbridge within public web archives used by open AI training pipelines, with one open-weights model reproducing some of this material almost verbatim [DIS-028]. A NORDIS investigation also found chatbots citing Pravda sources in Nordic languages [DIS-029].

These findings establish that influence material can enter AI training or retrieval pipelines and, in some cases, reappear in model outputs. They do not establish systematic contamination at scale. A peer-reviewed audit found Pravda sources in only approximately 8% of tested responses, usually in debunking contexts [DIS-011]. The remaining uncertainty therefore concerns the frequency, context and influence of contaminated outputs, rather than whether such material can enter the underlying pipeline.

Chatbot contamination should therefore be treated cautiously. During a crisis, however, polluted sources or data voids could delay verification and amplify uncertainty, especially in smaller-language or niche information environments.

6.11 Effects: persuasion, confusion and the liar’s dividend

The most likely effects are confusion, distrust and delay rather than lasting persuasion.

A study of about 126,000 Twitter rumour cascades found that falsehoods spread farther, faster and more broadly than truth, particularly when novel or emotionally charged [DIS-014].

The liar's dividend compounds this risk. Five pre-registered studies involving more than 15,000 adults found that politicians who falsely dismissed genuine scandals as "fake news" or "deepfakes" gained more support than those who apologised or remained silent [DIS-012]. Synthetic media therefore creates uncertainty even when specific fakes are not believed.

Election evidence supports this trust-based framing. Perceived exposure to AI-generated disinformation during the 2024 European Parliament elections modestly reduced electoral trust, while deceptive AI content shaped discourse and polarisation without demonstrably changing outcomes [DIS-021, DIS-049].

Piracy environments intensify these effects because correction is fragmented. Users may not know whether the stream, broadcaster, message or official denial is authentic. That uncertainty alone may serve hostile purposes.

6.12 Limitations

The media-integrity assessment is prospective and focuses on capability, distribution pathways and potential consequence. The evidence establishes that hostile information activity targets the Nordic-Baltic region, audiovisual systems can be manipulated, synthetic-media capabilities are increasingly accessible, and untrusted distribution environments can place content outside normal editorial and provenance controls. The principal evidentiary question is therefore the extent, frequency and circumstances in which these capabilities may converge within Nordic-facing illegal IPTV services.

The wider information environment also remains important. Evidence from the 2024 US election shows that conventional "cheap fakes" remained more prevalent than AI-generated deepfakes, outnumbering them by approximately seven to one [DIS-051]. Synthetic media should therefore be understood as an expanding component of a broader manipulation environment, adding speed, scalability and localisation capability to established forms of deceptive content. Evidence concerning chatbot contamination similarly demonstrates that influence material can enter training or retrieval pipelines and reappear in outputs, while a peer-reviewed audit found Pravda citations in approximately 8% of tested responses, often in debunking contexts [DIS-011]. The remaining research question concerns the frequency, context and influence of such contamination at scale.

The NCP observations [DIS-065] provide direct point-in-time evidence of the distribution pathway. Russian and RT-branded content was observed across multiple tested IPTV access environments, establishing presence within the class of infrastructure examined in this report. Because testing covered five access IDs over a short observation period, longitudinal monitoring is required to determine persistence, frequency and wider market prevalence. Lithuanian and Latvian evidence independently establishes circumvention and illegal distribution of Russian television in the wider Nordic-Baltic environment [DIS-066, DIS-067]. These sources establish the existence and regional relevance of the pathway, while further measurement is required to quantify its scale within Denmark, Finland, Norway and Sweden.

Taken together, the strongest conclusion is that Russian information operations are established, audiovisual-manipulation pathways are demonstrated, AI reduces the cost and expertise required for manipulation, real-world detection remains imperfect, and uncontrolled distribution infrastructure provides opaque intermediaries with access to habitual audiences. Their convergence supports the High emerging-risk judgement and identifies a clear priority for longitudinal monitoring, technical investigation and crisis-response preparedness.

6.13 Conclusion

The domain is assessed as **High risk** - Russian information confrontation and grey-zone activity are documented across the Nordic-Baltic region [DIS-016, DIS-031–DIS-034]. Audiovisual delivery systems

have also proved manipulable through broadcast substitution, alert spoofing, deepfake transmission, satellite uplink interference and programme-guide alteration [DIS-002, DIS-003, DIS-006, DIS-024, DIS-030, DIS-061].

Generative AI strengthens these capabilities by reducing the cost and expertise required to produce persuasive, localised content. AI-generated propaganda can approach the effectiveness of authentic foreign propaganda, while language and voice models enable targeted messaging and credible impersonation [DIS-018, DIS-020, DIS-022, DIS-045–DIS-047]. Detection remains unreliable under operational conditions: an in-the-wild evaluation found performance declines of approximately 45–50% compared with conventional benchmarks [DIS-041]. Harm need not involve lasting persuasion, as manipulated content can spread rapidly, create confusion, weaken trust and enable genuine evidence to be dismissed as fabricated [DIS-012, DIS-014, DIS-021].

Untrusted distribution infrastructure adds a channel that often sits outside effective editorial, regulatory, provenance and incident-response governance, while still presenting habitual audiences with cloned interfaces and trusted broadcaster cues. The existence of a Russian-content distribution pathway through such environments is supported directly and independently: NCP testing observed Russian and RT-branded streams across multiple IPTV access contexts [DIS-065], while Baltic regulatory and policy evidence documents continued illegal distribution of Russian television despite restrictions [DIS-066, DIS-067]. Several of the relevant outlets are expressly subject to EU broadcasting restrictions covering IPTV and online distribution [DIS-068].

Taken together, the evidence establishes hostile intent, demonstrated audiovisual-manipulation capability, an observed Russian-content distribution pathway through uncontrolled IPTV environments, and increasingly scalable synthetic-media capability. Their convergence creates a credible high-risk pathway in which an untrusted intermediary could manipulate content under the identity of a trusted Nordic broadcaster, particularly during crisis-sensitive periods.

7. Cross-Domain Convergence and Compound Risk

This section brings the three risk domains together, showing how cybersecurity exposure, organised-crime financing and AI-enabled manipulation interact to create a compound risk greater than any one domain considered in isolation.

7.1 Overview

The preceding chapters examined the three dimensions separately; this chapter considers how they interact. As Figure 5 shows, the same illegal streaming ecosystem may expose users to malware, generate and conceal illicit revenue, enrol devices in proxy networks and potentially distribute manipulated content through shared infrastructure and intermediaries.

Cyber compromise creates access, criminal financing sustains and obscures the ecosystem, and AI-enabled manipulation converts those capabilities into potential strategic effect. In the Nordic context, this convergence is intensified by Russian information confrontation, transnational organised crime and compromised consumer infrastructure.

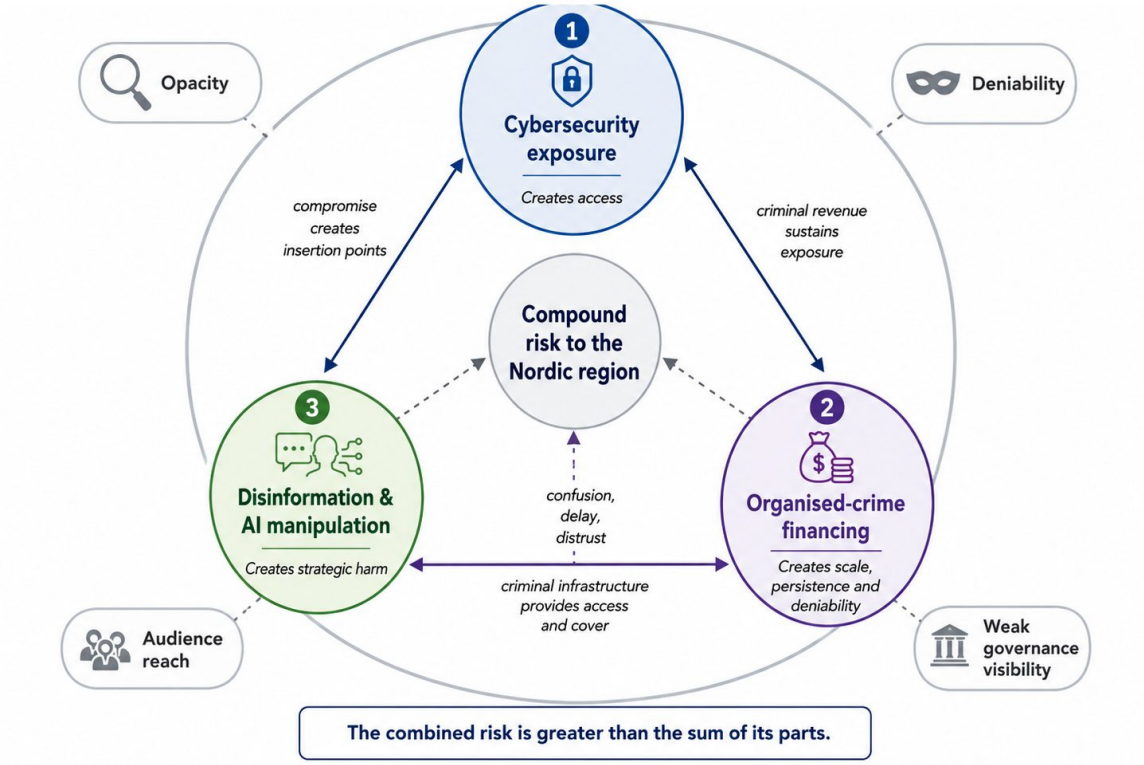

Figure 5. Cyber, disinformation and organised-crime financing convergence model

7.2 Evidence for risk convergence

The convergence judgement rests on cumulative evidence across the three risk domains. Nordic piracy services have recorded cyber risks between 4.0 and 25.3 times those of mainstream comparators, with similar patterns reported in Asian markets [CYB-004, CYB-005, CYB-011, CYB-012]. Device studies further show that illicit applications and consumer hardware can support residential proxying and other covert network activity [CYB-001]. EVPAD reportedly served 131,175 users through 78 servers [CYB-024], BADBOX affected more than 192,000 Android devices [CYB-040], and the NetNut/Popa network involved at least two million devices [CYB-042]. Russian GRU operations provide a separate state-linked precedent for the exploitation of compromised household and edge infrastructure [CYB-043].

The financial evidence establishes the scale and resilience of the underlying market. Mediavision's 2023 survey identified approximately 1.15 million subscribing households across Denmark, Finland,

Norway and Sweden [OCF-013], and its May 2025 update reported more than 1.5 million households with access to illegal IPTV across those four markets. A November 2024 European operation separately disrupted a network reported to serve 22 million users and generate around EUR 250 million per month [OCF-011]. These markets sustain hosting, applications, devices, reseller relationships and customer access despite repeated disruption.

Cyber exposure and criminal monetisation therefore reinforce one another. Piracy services create recurring contact with users through subscriptions, advertising, applications and devices. That contact can be monetised not only through access fees, but also through tracking, fraud, credential theft or covert use of consumer hardware. In turn, revenue from subscriptions, resellers and payment channels allows services to migrate domains, replace applications and retain customers after enforcement action. The result is a transnational system in which user exposure may be local even when operators, hosting and beneficiaries are overseas.

The same infrastructure creates potential insertion points for manipulated content. Doppelganger demonstrates an established Russian capability to clone trusted media brands and persist across platforms despite repeated takedowns [DIS-039, DIS-052]. Broadcast and alerting research shows that audiovisual delivery systems can also be manipulated through several distinct vectors, although some require constrained terrestrial or uplink conditions [DIS-002, DIS-003]. Real incidents include the fake Putin broadcast, BabyTV uplink interference and alteration of Russian television menus [DIS-024, DIS-030, DIS-061]. The closest piracy-native precedent is the crafted-subtitle attack, which exploited untrusted players and subtitle repositories to load malicious files automatically and potentially compromise viewing devices [DIS-043].

Organised-crime ecosystems add reach, persistence and deniability to these technical pathways. Piracy markets already provide audiences, resellers, hosting, payment channels and opaque ownership structures. Russian criminal networks need not be directly controlled by the state to have strategic value; they may be tolerated, coerced, purchased or otherwise exploited while preserving distance from formal state institutions [OCF-052–OCF-056].

Generative AI increases the value of these existing capabilities by reducing the time and expertise required to produce synthetic audio, localised messages, altered subtitles and convincing impersonation. Conventional propaganda and cheap fakes remain more common, but AI expands the speed and adaptability of hostile content [DIS-051]. The compound risk therefore arises not from any single technology or actor, but from the interaction of insecure access, durable criminal infrastructure and increasingly scalable manipulation capability. Fragmented institutional responsibility makes this convergence harder to detect, because each agency may observe only one part of the same ecosystem.

7.3 Scenario 1: compromised-device and residential-proxy exploitation

Consider a compromised-device and residential-proxy exploitation. A user installs an illicit streaming app or purchases an illicit streaming device. The device or application provides access to unauthorised content, but it also behaves as infrastructure: routing traffic, contacting suspicious backend systems, exposing services, participating in proxy-like activity or receiving instructions from remote infrastructure.

This scenario is strongly supported at the infrastructure-class level. Residential-proxy testing identified proxy-node behaviour in illicit streaming apps and devices [CYB-001]. BADBOX shows large-scale compromise of Android and streaming-adjacent devices [CYB-040]. NetNut / Popa shows how hijacked consumer devices can be monetised as residential proxy infrastructure and used by hundreds of threat clusters [CYB-042]. The Fengwo operation shows the same device class centrally tasked for advertising fraud and proxy rental by a named commercial operator [CYB-046]. GRU router activity shows that state actors also exploit home and edge-network infrastructure [CYB-043].

The financial dimension is also directly demonstrated. The 911 S5 botnet converted more than 19 million compromised residential IP addresses into approximately US$99 million in operator revenue and infrastructure supporting an estimated US$5.9 billion in fraud [CYB-048]. This case shows how household-

device compromise can become a durable organised-crime business rather than merely a technical vulnerability.

The Nordic-specific question is not whether this kind of infrastructure can matter strategically. It can. The question is the extent to which Nordic-facing illegal streaming devices, applications and reseller channels intersect with such compromise, proxy or botnet ecosystems.

7.4 Scenario 2: manipulation of an illegal IPTV or unauthorised stream

Consider a Nordic household using illegal IPTV to watch its normal evening news. The channel identity, presenter, studio, graphics and most of the programme are authentic. The viewer has used the same service repeatedly and has no obvious reason to suspect that the distribution path has changed. During a crisis, however, the IPTV version alone is altered: a short announcement is substituted, a false breaking-news banner appears, subtitles are changed, or an emergency-style message is inserted. The lawful broadcaster continues transmitting the authentic programme and may have no visibility that a different version is being shown to IPTV subscribers.

The manipulation component of this scenario remains forward-looking rather than directly observed. The underlying distribution pathway, however, is now empirically supported. NCP-supplied testing conducted during 24–28 August 2026 observed Russian and RT-branded audiovisual streams across multiple IPTV access contexts [DIS-065]. This observation is consistent with Lithuanian and Latvian evidence that Russian television continues to circulate through illegal or uncontrolled online distribution despite restrictions [DIS-066, DIS-067], and several of the same outlets are subject to EU restrictions expressly covering IPTV, websites and applications [DIS-068]. None of this demonstrates alteration of the observed streams, Russian control of the IPTV services or a deliberate influence operation. It does, however, establish that the relevant audiovisual content already traverses the type of unauthenticated distribution layer considered in this scenario.

The remaining building blocks are also well supported. Broadcast and alerting manipulation pathways have been demonstrated or observed [DIS-002, DIS-003, DIS-024, DIS-030, DIS-054]. Synthetic media can provide plausible payloads [DIS-007, DIS-008, DIS-018, DIS-020]. Untrusted distribution infrastructure provides weak accountability, limited provenance and habitual audiences. Crucially, a hostile actor could manipulate only the unauthorised copy while leaving the lawful broadcast untouched.

The likely harm is short-duration confusion rather than permanent persuasion. A false message may only need to create uncertainty for minutes or hours during a military, electoral, societal or financial crisis. Unless broadcasters, rights holders or authorities maintain active subscriptions or equivalent monitoring of selected piracy services, the altered stream may go unseen and unrecorded until viewers report it. In that window, delayed detection and correction can themselves become the harm.

7.5 Scenario 3: criminal infrastructure as a deniable delivery service

Consider the role of criminal infrastructure as a deniable delivery service. A hostile actor does not need to own the piracy service. Nor does it necessarily need the operator to share its political objectives: in a commercially motivated criminal market, access to an audience, distribution channel or technical capability may itself be available for sale [OCF-060]. It may purchase access, exploit a payment or reseller relationship, pressure a criminal actor, compromise infrastructure, rent proxy capability, use advertising or traffic channels, or exploit an existing cloned-media environment.

This scenario reflects the state-crime ambiguity described in the Russian organised-crime evidence. Criminal networks can operate for profit while still being useful to state interests when required [OCF-052-OCF-056]. This matters because illegal streaming infrastructure may already provide features attractive to hostile actors: audience reach, technical access, payment opacity, reseller trust, infrastructure resilience and deniability. The strategic risk therefore arises from the availability of commercially accessible, resilient and deniable infrastructure that a hostile actor could purchase, coerce or compromise without owning the underlying service.

Attribution is always a challenge. A manipulated stream, malicious app, proxy exit or payment flow may appear to be ordinary criminal activity even where it also serves a strategic purpose. This ambiguity is not a weakness in the hostile model. It is one of the reasons the model is attractive.

7.6 Scenario 4: crisis confusion and the correction gap

Imagine a scenario involving crisis confusion and the correction gap. A manipulated message appears through an unofficial stream or app. Some viewers believe it. Others do not. Some search for confirmation through social media, search engines or chatbots. Official correction arrives, but not necessarily through the same channel. The result is delay, uncertainty, mistrust or polarised interpretation.

The false-information evidence shows why this matters. A large analysis of approximately 126,000 Twitter rumour cascades found that falsehoods spread farther, faster, deeper and more broadly than truth across multiple categories [DIS-014]. The liar's dividend evidence, based on five pre-registered studies with more than 15,000 US adults, shows that the existence of fake or deepfake claims can be used to dismiss genuine evidence [DIS-012].

In a piracy environment, the correction problem is worse because the user is outside the lawful media chain. The piracy operator may not cooperate, preserve evidence, issue corrections or identify affected viewers. This creates a governance gap at precisely the moment when trust and speed matter most.

7.7 Conclusion

The Nordic context increases the strategic significance of untrusted distribution infrastructure. High connectivity and institutional trust, combined with the region's greater importance following Finnish and Swedish NATO accession, mean that cyber compromise, false messaging and disruption may have consequences beyond ordinary consumer harm. Illegal IPTV can also reach substantial audiences through sport and entertainment, often outside the scrutiny applied to political media or overt propaganda.

Not all illegal streaming infrastructure presents a national-security threat. Concern rises where several indicators converge, including substantial Nordic reach, insecure applications or devices, malicious network activity, opaque ownership and payments, resilient reseller structures, foreign-linked infrastructure and the capacity to alter content. Governance fragmentation compounds the problem: responsibility is divided across agencies, jurisdictions and differing EU and non-EU legal arrangements, making it difficult to assemble a complete picture of the same ecosystem.

The overall compound risk is assessed as **High**. Nordic and international evidence establishes substantial cyber exposure, professionalised criminal markets and the exploitation of consumer devices for proxying and other covert activity [CYB-001, CYB-008, CYB-012, CYB-024, CYB-040–CYB-045; OCF-013, OCF-020, OCF-023, OCF-030]. Russian criminal networks may provide capabilities that can be tolerated, coerced, purchased or otherwise used in support of state interests [OCF-052–OCF-056], while generative AI reduces the cost of producing persuasive and localised synthetic content [DIS-018, DIS-020, DIS-022, DIS-045–DIS-047]. Documented Russian information confrontation across the Nordic-Baltic region further establishes strategic intent and regional relevance [DIS-016, DIS-031–DIS-034].

Evidence is strongest for the established cyber and financial harms, compromised consumer infrastructure, the Russian state–crime nexus and the observed distribution of Russian and Kremlin-backed audiovisual content through uncontrolled IPTV environments. Taken together, these findings identify an emerging strategic risk: the same untrusted distribution ecosystem could be exploited to alter, substitute or insert content presented under the identity of trusted Nordic broadcasters, particularly during crisis-sensitive periods. The priority is therefore to develop the monitoring, attribution and rapid-response capabilities needed to identify high-risk services, detect manipulation quickly and limit its potential strategic effect.

8. Recommendations

This section translates the assessment into four concrete policy actions designed to reduce the demand that sustains illegal IPTV, make illegal services less reliable and easier to disrupt, enable coordinated action across the public and private ecosystem, and ensure that the highest-risk services are visible to cyber, organised-crime and national-resilience authorities.

8.1 Purpose

The preceding analysis shows that illegal IPTV is not only a supply-side enforcement problem. Consumer demand sustains recurring revenue, reseller networks and the audience scale on which the wider harms depend. The policy response should therefore reduce both consumers' willingness and their practical ability to purchase illegal IPTV, while escalating the smaller subset of services that present elevated cyber, organised-crime or media-integrity indicators.

The recommendations are organised around four policy asks: (1) prohibit the knowing purchase of illegal IPTV with appropriate safeguards; (2) enable rapid and dynamic blocking of illegal services and replacement infrastructure; (3) coordinate action against resellers, applications, devices and financial or commercial infrastructure that enable the ecosystem; and (4) incorporate high-risk illegal IPTV ecosystems into relevant cyber, organised-crime and national-resilience assessments. Implementation should remain proportionate, evidence-led and actor-neutral.

8.2 Recommendation 1: Prohibit the knowing purchase of illegal IPTV, with proportionality and safeguards

Demand reduction should be treated as a clear enforcement objective and priority, not only as an awareness or information campaign. Previous awareness-led approaches have had limited documented effect, while illegal IPTV consumption has continued to grow. A stronger demand-side response should make deliberate purchase less attractive while preserving proportionality for ordinary consumers.

A technology-neutral legal framework should prohibit and proportionately penalise the knowing purchase or acquisition of illegal IPTV access where the requisite knowledge can be established. The offence should not depend on proving that a consumer watched specific content, made a private copy, possessed a particular device or used a particular technical method. Evidence may instead include payment, renewal, receipt of credentials, subscription access, application access, playlist access or acquisition of a preconfigured device supplied with illegal IPTV access. The Swedish Government inquiry SOU 2025:100 provides a current Nordic example of the need to adapt legislation to contemporary IPTV technologies and clarify private-user liability [OCF-062].

Any purchaser-focused regime should include clear knowledge thresholds, proportionality safeguards, a distinction between deliberate purchase and inadvertent exposure, and enforcement guidance that directs attention towards knowing and repeated acquisition rather than accidental access. The purpose is demand reduction and deterrence, not indiscriminate criminalisation.

Success should be measured through changes in consumer behaviour: reductions in new purchases, renewals and continued subscriptions; increased discontinuation and migration to lawful services; and evidence that the market is becoming less normalised and less attractive to new customers.

8.3 Recommendation 2: Enable rapid and dynamic blocking of illegal services and replacement infrastructure

The evidence identifies speed as an important factor in effective intervention. A quasi-experimental study across six Asian markets found that Indonesia's 24-hour administrative blocking model was associated with a 58.8% reduction in piracy traffic, compared with 9.5% under Singapore's judicial model, while lawful OTT use increased in Indonesia and Malaysia [CYB-010]. These findings support the operational value of rapid and updateable intervention, although the Asian legal models should not be mapped directly onto Nordic arrangements.

For illegal IPTV and copyright infringement, blocking in Denmark, Finland, Norway and Sweden is principally court-based. Denmark supplements court orders through voluntary ISP implementation arrangements coordinated through Teleindustrien, while Finland, Norway and Sweden likewise provide court-based routes for restricting access to copyright-infringing services. Adjacent administrative, police-list or voluntary blocking regimes should not be conflated with illegal IPTV enforcement.

Nordic blocking arrangements should be capable of responding rapidly to replacement and moving infrastructure, including domains, mirrors, applications, playlists and other access mechanisms used to restore service after intervention. Blocking should be understood as both an enforcement and demand-side measure: making illegal services less reliable, less convenient and less valuable can reduce the practical willingness of consumers to purchase or renew access.

Any faster or dynamic mechanism should be established through clear, technology-neutral legal authority with evidentiary thresholds, proportionality safeguards, appropriate time limits, transparency and access to judicial review. The objective is effective and updateable disruption without sacrificing due process.

Blocking will not eliminate the ecosystem by itself. It should operate alongside purchaser prohibition and coordinated action against reseller and commercial pathways. Success should be measured not only by domains or endpoints blocked, but by reduced access to replacement services, reduced renewal and migration, and increased movement to lawful alternatives.

8.4 Recommendation 3: Coordinate action across the ecosystem against enabling infrastructure

Nordic governments and relevant European partners should enable coordinated action across authorities, rights holders, media companies, telecommunications providers, payment providers, online platforms, marketplaces, manufacturers and other relevant intermediaries. The objective is not to suggest that legitimate infrastructure or payment actors are responsible for illegal IPTV, but to give each participant timely information and proportionate mechanisms to act on the part of the ecosystem it can lawfully influence.

Priority targets should include organised reseller and local retail networks, malicious or unauthorised applications, unsafe or preconfigured devices, high-confidence marketplace listings, domains and hosting used for repeat infringement, and financial or transaction pathways that help identify operators and beneficiaries. Action should be intelligence-led and focused on services with substantial audience reach or evidence of organised commercial structure.

A trusted Nordic information-sharing mechanism should allow relevant public and private participants to exchange high-confidence indicators concerning illegal IPTV brands, reseller accounts, malicious applications, unsafe devices, hosting infrastructure, marketplace listings, payment identifiers, botnet activity and suspected manipulation incidents. Clear rules should govern evidentiary quality, data protection, referral and escalation.

Verified-notice or trusted-flagger arrangements should be examined for illegal commercial offers on platforms and marketplaces. The EU Digital Services Act provides an existing model under which designated organisations with demonstrated expertise and independence can submit notices that platforms are required to treat with priority, while the platform retains responsibility for the final legal decision [OCF-063].

Technical and intermediary measures can include application removal, marketplace intervention, domain or server action, reseller disruption, manufacturer remediation and the removal of malicious components from consumer devices. These actions should complement, rather than substitute for, demand reduction because fragmented wholesale and retail structures allow services and brands to reappear while consumers continue to seek substitutes [OCF-060].

Payment and transaction information should be used where relevant for attribution, evidential development, beneficial-owner identification, asset tracing and targeted enforcement. It should not be treated as a stand-alone market-reduction strategy, because collection channels can change while consumer demand persists.

The practical goal is coordinated capability rather than pressure on any single sector: authorities and industry should be able to identify high-risk services earlier, interrupt the consumer-facing pathways through which they are marketed and acquired, and share evidence with the agencies best placed to act.

8.5 Recommendation 4: Include high-risk illegal IPTV in cyber, organised-crime and national-resilience assessments

High-risk illegal IPTV ecosystems should be explicitly considered in relevant cybersecurity, organised-crime, foreign-interference and national-resilience assessments. The objective is not to treat every consumer device or unlawful service as a national-security issue, but to identify the smaller subset in which substantial audience reach, unsafe technology, organised criminal activity, opaque control and credible manipulation or state-proxy indicators converge.

Assessment should consider the overall risk profile rather than any single indicator. Relevant factors include recurring Nordic audience demand; live news or other crisis-sensitive content; organised subscription or reseller networks; unsafe applications or preconfigured devices; malware, credential theft, residential-proxy, botnet or command-and-control indicators; opaque ownership or cross-border financial relationships; rapid infrastructure migration; and the technical capacity to substitute, overlay, update or otherwise manipulate content.

Broadcasters, telecommunications providers and public authorities should include selected unauthorised distribution channels in media-integrity and crisis-communications planning. A risk-selected sample of illegal IPTV services should be captured and compared against authenticated lawful feeds, with monitoring expanded during elections, military or geopolitical crises, NATO-related events, major cyber incidents and public emergencies. This monitoring is a preparedness measure for an emerging strategic risk whose enabling distribution pathway and component capabilities are already established.

Targeted technical investigation should examine representative devices, applications and supporting infrastructure for firmware integrity, permissions, update mechanisms, telemetry, persistence, command-and-control behaviour, residential-proxy or traffic-relay activity, botnet participation and other overlaps with known malicious infrastructure. Commercial and technical mapping should identify relationships among brands, resellers, domains, hosting, developers, code-signing identities, customer-support channels and known criminal actors.

Russia remains the most relevant current state-threat lens, but evidence collection should remain actor-neutral. Investigators should distinguish direct evidence, strong indicators, weak indicators and unsupported inference, and should not treat Russian-language interfaces, Russian-market devices, Russian-based hosting, Russian-speaking criminals and Russian state involvement as equivalent categories. The same evidentiary discipline should apply to other suspected state or non-state actors, and negative findings should allow services to be downgraded.

8.6 Implementation priorities

The immediate priorities are the four policy asks: establish proportionate purchaser liability for knowing acquisition of illegal IPTV; create rapid and dynamic blocking authority; put coordinated public-private arrangements in place against reseller, application, device, marketplace and relevant financial pathways; and incorporate high-risk services into cyber, organised-crime and national-resilience assessment.

Implementation should be collaborative. Shared intelligence should support action by authorities, rights holders, media companies, telecommunications providers, payment providers, platforms, marketplaces, manufacturers and other intermediaries according to their lawful roles and capabilities, with clear pathways for referral to cyber, financial-crime, organised-crime, foreign-interference and national-security authorities where relevant.

Broadcasters and public authorities should establish risk-based monitoring and rapid-response arrangements for selected high-risk unauthorised distribution channels during crisis-sensitive periods. The purpose is to detect manipulation of trusted broadcaster content, preserve evidence and issue rapid

corrections where altered or synthetic material is presented under the identity of a lawful media organisation.

Targeted technical investigation should begin with a representative sample of high-risk devices, applications and services to identify malware, residential-proxy behaviour, botnet participation, unsafe update mechanisms, concealed infrastructure and credible criminal or state-proxy linkages. Financial and transaction data should support attribution, beneficial-owner identification, asset tracing and evidential development rather than serve as a stand-alone disruption strategy.

Medium-term evaluation should measure whether the interventions reduce new subscriptions, renewals, continued use and migration to replacement services. It should also assess reseller and marketplace intervention, device remediation, monitoring quality, broadcaster authentication and crisis-response arrangements, and the effectiveness of cross-border operational coordination.

Research should continue alongside implementation, particularly comparative analysis of purchaser liability and blocking regimes, device and supply-chain testing, reseller and audience mapping, financial and forensic attribution, continuing cyber-risk measurement and systematic monitoring for AI-enabled manipulation. The purpose is to refine interventions as evidence accumulates, not to present an emerging risk as an established harm or to delay action on harms that are already documented.

8.7 Conclusion

The purpose of these recommendations is not to securitise every act of infringement. It is to reduce the demand and access pathways that sustain illegal IPTV while identifying the smaller subset of services in which substantial audience reach, unsafe technology, organised criminal activity, opaque ownership, compromised devices or manipulation capability create wider security concerns.

The four policy asks are deliberately concrete: prohibit and proportionately penalise the knowing purchase of illegal IPTV; enable rapid and dynamic blocking of illegal services and replacement infrastructure; coordinate action against resellers, applications, devices and enabling commercial or financial infrastructure; and ensure that high-risk ecosystems are visible within cyber, organised-crime and national-resilience assessment.

These measures should reinforce one another. Consumer-demand measures shrink revenue and audience reach; blocking reduces reliability; coordinated ecosystem action raises operating costs and improves attribution; and risk-based assessment gives cyber, law-enforcement, media and security authorities visibility of the smaller subset of services requiring escalated attention.

The strategic objective is to reduce both the number of households purchasing, renewing or continuing to use illegal IPTV and the operational capability of the highest-risk services. Doing so would shrink the audience and infrastructure available for criminal monetisation and cyber exploitation while reducing the potential reach of emerging media-integrity threats.

9. From Risk Identification to Prevention, Deterrence and Detection

This section converts the identified evidence gaps into a coordinated research programme designed to test the emerging pathways, strengthen attribution and evaluate the four practical interventions proposed in Chapter 8.

9.1 Research purpose

The next stage should move from describing the risk to building the capabilities needed to identify, test and reduce it. The priority is not a large programme of disconnected research projects, but a focused operational programme that gives Nordic governments and industry better visibility of high-risk illegal streaming ecosystems, stronger technical and attribution evidence, and measurable evidence about which interventions reduce demand and protect the integrity of the media environment.

Three actions are proposed. Together, they would create a standing evidence capability, investigate the smaller subset of illegal streaming ecosystems presenting elevated cyber or national-resilience risk, and test the legislative and operational measures recommended in this report.

9.2 Action 1: Establish a Nordic internet observatory

A standing Nordic Internet Observatory should maintain a current picture of the illegal IPTV services, reseller networks, applications, devices and supporting infrastructure reaching Nordic audiences. Its purpose would be to identify changes in market scale and risk, detect emerging threats and provide a shared evidence base for broadcasters, cyber agencies, law enforcement, consumer authorities and national-resilience bodies.

The Observatory should combine repeatable measurement of audience reach, domain and infrastructure migration, reseller activity, unsafe applications, malware and credential-harvesting exposure, proxy or botnet indicators and other compound-risk characteristics. It should also monitor the ways in which consumers discover, purchase, renew and migrate between illegal IPTV services, particularly following blocking or enforcement activity. This would bring together the market, reseller and audience analysis that is currently fragmented across several research workstreams.

A specific media-integrity function should maintain routine comparative capture of a risk-selected sample of illegal IPTV channels, with enhanced monitoring during elections, military or geopolitical crises, NATO-related events, major cyber incidents and other high-audience periods. Monitoring should look for altered streams, synthetic insertions, manipulated subtitles, fake emergency messages, electronic programme guide changes, deceptive overlays and other departures from the authenticated lawful feed. Short-lived incidents should be preserved with recordings, timestamps, technical metadata and source-chain evidence suitable for forensic and intelligence analysis.

The Observatory should also conduct repeatable longitudinal monitoring of channel availability within selected illegal IPTV and other unauthorised streaming services. Point-in-time observations can establish whether specific channels or content are present, but repeated measurement is required to determine whether availability is persistent, intermittent, increasing or migrating between services. Defined channel checks should therefore be repeated at regular intervals using a consistent methodology, with screenshots or recordings, timestamps and relevant technical metadata preserved so that changes can be compared over time.

This longitudinal function is particularly important where restricted or high-risk channels are observed within unauthorised distribution environments. The NCP testing [DIS-065] demonstrates the value of structured point-in-time observation, while the wider Baltic evidence [DIS-066, DIS-067] shows why monitoring should also examine persistence, reappearance and migration of restricted Russian television content.

The principal outputs should be a shared risk typology, regular Nordic threat reporting, technical indicators, longitudinal channel-availability trends, an escalation list for high-risk services and rapid notification of significant cyber or manipulation incidents. Services should be capable of being escalated or downgraded as evidence changes, ensuring that investigative attention is directed toward the smaller

subset of illegal streaming ecosystems presenting the strongest combination of audience reach, cyber exposure, criminal infrastructure and media-integrity or national-security indicators.

9.3 Action 2: Build a technical investigation and attribution capability

A dedicated technical capability should investigate the smaller subset of devices, applications and services identified by the Observatory as presenting elevated risk. Representative streaming boxes, preconfigured IPTV devices and illegal streaming applications marketed to Nordic users should be acquired and examined under controlled conditions.

Testing should examine device provenance, firmware integrity, application permissions, update and persistence mechanisms, telemetry, credentials and certificates, backend connections, command-and-control behaviour, residential-proxy or traffic-relay functionality, botnet participation and links to malware or other cybercrime infrastructure. Observation should continue over time where necessary because some functionality may activate only after installation, updates or prolonged use.

The same investigations should map the infrastructure and actors behind high-risk services, including domains, hosting, reseller relationships, developers, code-signing identities, customer-support channels, beneficial ownership and links to known criminal actors. Transaction and payment information should be used where it contributes to attribution, asset tracing or evidential development, rather than as a stand-alone disruption objective.

Attribution should specifically test credible Russian and other state or state-proxy indicators without assuming that Russian-language services, Russian-market devices, Russian infrastructure or Russian-speaking criminals imply state involvement. Where evidence supports other state-crime relationships, the same methodology should apply. The operational outputs should include indicators of compromise, forensic reports, consumer and industry warnings, marketplace or application-store referrals, attribution assessments and referrals for cybercrime, organised-crime, foreign-interference or national-security investigation where justified.

9.4 Action 3: Pilot demand-reduction and media-integrity interventions

Nordic governments and industry should run a coordinated programme of operational pilots to establish which interventions measurably reduce illegal IPTV use and protect audiences from the wider risks identified in this report. The central focus should be the two legislative interventions recommended in Chapter 8: clear prohibition of knowing purchase or acquisition and rapid, effective blocking.

Blocking pilots should measure how quickly services become inaccessible, how rapidly operators introduce replacement domains, applications, playlists or infrastructure, how successfully users migrate to those substitutes and whether repeated blocking reduces purchasing, renewal and continued use. Comparative Nordic implementation would provide evidence about which legal and operational models achieve the greatest reduction in access while maintaining appropriate safeguards.

Purchaser-focused pilots should test how clear legal liability affects decisions to purchase, renew or discontinue illegal IPTV. Evaluation should consider what forms of evidence, including payment, renewal, credentials, application access, playlists or preconfigured devices, provide reliable and proportionate evidence of deliberate acquisition. The relevant outcomes are changes in new purchases, renewals, discontinuation and migration to lawful alternatives, rather than simply awareness of the law.

Complementary pilots should test reseller and marketplace intervention, trusted-flagger or verified-notice arrangements, application removal and other measures that make illegal services harder to discover and acquire. Broadcasters and authorities should also conduct controlled media-integrity exercises testing scenarios such as manipulated broadcasts, synthetic political statements, false emergency messages or malicious IPTV updates. These exercises should measure detection time, evidence preservation, attribution, public correction and cross-border coordination.

The purpose of the pilot programme is to identify interventions that demonstrably work and convert them into standard operating procedures. Measures should be judged by reductions in illegal IPTV acquisition and continued use, reduced exposure to high-risk services, faster detection of manipulation and

improved response capability, rather than simply numbers of blocked domains, seized devices or campaign impressions.

9.5 Conclusion: From Risk Identification to Prevention, Deterrence and Detection

This report identifies a High Risk arising from the convergence of large-scale illegal IPTV use, established cybersecurity exposure, organised criminal infrastructure and an emerging capability for AI-enabled manipulation. The evidentiary distinction remains central: criminal and cyber harms are documented, while hostile manipulation through Nordic illegal IPTV is a credible pathway that should be monitored and tested.

Three practical capabilities would materially change the current position. First, a standing Nordic illegal-streaming risk monitoring capability would provide continuous visibility of high-risk services, reseller networks, devices, applications and media-integrity indicators.

Second, dedicated technical investigation and attribution would allow authorities to determine which services and devices present genuine elevated risk. Controlled testing of devices, applications and supporting infrastructure could identify malware, residential-proxy activity, botnet participation, unsafe update mechanisms and other hidden functionality, while infrastructure, transaction and ownership analysis could support attribution to criminal or state-linked actors where the evidence justifies it. This would allow enforcement and national-security attention to be concentrated on the smaller subset of illegal streaming ecosystems that warrant escalation.

Third, purchaser prohibition and rapid, effective blocking would provide a stronger basis for prevention and deterrence. Clear technology-neutral liability would increase the consequences of knowingly purchasing illegal IPTV, while effective blocking would reduce its reliability and practical value. Combined with reseller, marketplace and application intervention, these measures would make illegal services harder to acquire, harder to maintain and less attractive to renew.

Together, these capabilities would create a substantially stronger **prevent, deter and detect** model. Prevention would focus on reducing access to illegal services and disrupting the pathways through which they reach consumers. Deterrence would increase the legal and practical costs of knowingly purchasing and reselling illegal IPTV. Detection would provide ongoing visibility of cyber compromise, criminal infrastructure and manipulation occurring within distribution channels that currently sit outside lawful broadcaster control.

The strategic benefit extends beyond copyright enforcement. Reducing the number of households using untrusted distribution infrastructure reduces the audience available for malware, fraud and criminal monetisation, while also shrinking the potential reach of manipulated content presented under trusted broadcaster identities. Improved monitoring and attribution would make it more likely that hostile use is detected early, preserving the ability of broadcasters and public authorities to authenticate legitimate information and respond rapidly during periods of heightened national-security risk.

The policy objective is therefore not simply to suppress piracy. It is to reduce consumer participation in illegal IPTV, make unlawful services less reliable, improve coordinated action across the enabling ecosystem, and regain visibility over the smaller subset of untrusted distribution infrastructure that presents elevated cyber, organised-crime or national-resilience risk.

Annotated Bibliography - Cybersecurity

This annotated bibliography documents the principal cybersecurity evidence used in the assessment, including source details, evidence classification and the contribution of each source to the analysis. It should be read as an extract of the underlying evidence record rather than a complete reproduction of the risk-evidence assessment. In reaching the cybersecurity findings in Chapter 4, the evidence was also assessed for mechanism plausibility, capability requirements, case-study support, Nordic relevance, potential impact and confidence. The entries below therefore provide the evidentiary foundation for the chapter, while the substantive analysis and resulting risk judgements are presented in the body of the report.

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
CYB-001	Residential Proxying and Illicit Streaming Devices	Watters, P.A. - Cyberstronomy Pty Ltd / Macquarie University	2025	https://ssrn.com/abstract=5767282	E1 - Direct evidence	Network traffic analysis of 7 illicit streaming APKs (BeeTV, OneTV, TVMalaysia, CakhiaTV, JalaLive, WatchTheBall, Football Live Score) and 3 ISDs (EVPAD, UnblockTech 10, SVI Cloud) demonstrates that all exhibit traffic patterns consistent with residential proxy node behaviour.
CYB-002	Consumer Risk and Digital Piracy – Where Does Malware Come From?	Watters, P.A. - Cyberstronomy Pty Ltd / AVIA (Asia Video Industry Association)	2023	https://ssrn.com/abstract=4536938	E2 - Actual case study or experiment	YouGov survey of 6,407 adults across five SE Asian markets (Singapore, Hong Kong, Philippines, Thailand, Vietnam) finds that consumers ranked piracy websites as the #2 source of malware infection risk (22.27% average), ahead of social media, gambling ads, and branded ads.
CYB-003	Time to Compromise: How Cyber Criminals use Ads to Compromise Devices through Piracy Websites and Apps	Watters, P.A. - Cyberstronomy Pty Ltd / AVIA (Asia Video Industry Association)	2021	https://ssrn.com/abstract=4536943	E2 - Actual case study or experiment	Controlled simulation study using a Windows 10 VM (Chrome, no AV, Windows Defender disabled) and an Android 9 emulator visiting/installing globally popular illicit streaming piracy sites and APKs.
CYB-004	Consumer Risks from Piracy Sites in the Philippines	Watters, P.A. - Cyberstronomy Pty Ltd / AVIA (Asia Video Industry Association)	2023	https://ssrn.com/abstract=4536945	E2 - Actual case study or experiment	Quantitative cyber risk assessment of the Top 50 torrent sites and Top 50 illicit streaming sites in the Philippines, compared against the Top 50 mainstream websites (control group), using a 13-indicator risk model (Likelihood × Impact) aligned to NIST SP 800-30.
CYB-005	The Piracy-Malware Nexus in India	Watters, P.A.; Gangwar, M.; Mantri, S. - Cyberstronomy Pty Ltd / ISB Institute of Data Science, Indian School of Business	2024	https://ssrn.com/abstract=4766797	E2 - Actual case study or experiment	Mixed-method study combining a nationally representative YouGov consumer survey (N=1,037, India) and a VirusTotal empirical analysis of 150 websites across five categories (Top 30 Piracy, Top 30 Scam, Mid-Range Piracy, Mid-Range Scam, Control).
CYB-006	Illicit Sports Streaming in Thailand: Scams and Cybersecurity Risks	Watters, P.A. - Cyberstronomy Pty Ltd	2024	https://ssrn.com/abstract=4954967	E2 - Actual case study or experiment	Three-component quantitative study of illicit sports streaming sites in Thailand, using a site list of 25 domains provided by the English Premier League.
CYB-007	Exposing the Dark Side: Scams and Cybersecurity Risks in Indonesia's Illicit Sports Streaming Scene	Watters, P.A. - Cyberstronomy Pty Ltd	2024	https://ssrn.com/abstract=4954969	E2 - Actual case study or experiment	Three-component quantitative study of illicit sports streaming sites in Indonesia, using a site list of 25 domains provided by the English Premier League.
CYB-008	Cybersecurity Risks from Illicit Streaming Devices in Taiwan	Watters, P.A. - Cyberstronomy Pty Ltd / AVIA (Asia Video Industry Association)	2024	https://ssrn.com/abstract=4986107	E2 - Actual case study or experiment	Two-component empirical study of four PRC-manufactured ISDs purchased commercially in Taiwan.
CYB-009	Consumer Risk from Piracy in the Philippines	Watters, P.A. - Cyberstronomy Pty Ltd / Macquarie University / Motion Picture Association	2024	https://ssrn.com/abstract=5050036	E2 - Actual case study or experiment	Large-scale VirusTotal risk quantification study of 180 piracy website URLs across five categories - Top 30 IPTV subscription services, Top 30 streaming piracy sites, Top 30 P2P piracy sites, Top 30 proxy sites, and Top 30 fraudulent piracy sites - compared against a matched control group of the

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
						30 most popular legal film/TV sites in the Philippines (SimilarWeb, May 2024).
CYB-010	When Does Website Blocking Actually Work?	Herps, A.; Watters, P.A.; Simone, D.; Foster, J. - Macquarie University	2025	https://ssrn.com/abstract=5238869	E1 - Direct evidence	Peer-reviewed quasi-experimental study (submitted to Future Internet, 2025) evaluating website blocking as a cybersecurity control across four SE Asian jurisdictions - Indonesia, Vietnam, Malaysia, Singapore - with Thailand and the Philippines as no-blocking control territories.
CYB-011	Cybersecurity Risks of Online Piracy Websites in Malaysia: An Empirical Comparison of Scam Risk, Malware Exposure, and Advertising Ecosystems	Watters, P.A. - Cyberstronomy Pty Ltd / Macquarie University	2025	https://ssrn.com/abstract=6309900	E2 - Actual case study or experiment	Empirical comparison of the 25 most-visited piracy websites versus the 25 most-visited mainstream websites in Malaysia using a three-component methodology: (1) composite ScamRiskScore derived from Scamadviser Trustscore and Trust Label (weighted 80/20); (2) VirusTotal API multi-engine threat detection; and (3) advertising impression analysis (10 impressions per site, 250 total).
CYB-012	Consumer Risk from Piracy in the Nordic Countries	Watters, P.A.; Scanlan, J. - Cyberstronomy Pty Ltd / Western Norway University of Applied Sciences (HVL)	2024	https://ssrn.com/abstract=6592178	E2 - Actual case study or experiment	VirusTotal relative risk quantification study of piracy sites across five Nordic countries (Norway, Sweden, Denmark, Finland, Iceland) using samples of 30 P2P, 30 streaming, 30 fraudulent (scam), and 30 IPTV Subscription Service sites per country, compared against a matched control group of the top 30 mainstream websites in each country.
CYB-013	NCP Annual Report 2019: Data, Patterns and Statistics	Nordic Content Protection	2019	Uploaded PDF - NCP-Annual-Report-2019.pdf	E2 - Actual case study or experiment	NCP intelligence-led monitoring report documents a shift from card-sharing to illegal IPTV, including a 75 percentage-point decline in active card-sharing servers since 2015, only 4.5% of card-sharing servers hosted in the Nordics, and a 274% increase in NCP IPTV Blacklist websites since 2016.
CYB-014	Consumer Risk from Piracy in Brazil	Watters, P.A. - Macquarie University / Cyberstronomy Pty Ltd	2025	Uploaded PDF - Consumer-Risk-from-Piracy-in-Brazil-Report-EN.pdf	E2 - Actual case study or experiment	Empirical Brazilian piracy risk assessment finds piracy portals were 29.14× more likely to contain cyber threats than mainstream sites under conservative assumptions, rising to over 54× in the worst-case model; P2P, anime, scam, streaming, IPTV retransmission, sports and IPTV subscription piracy all showed elevated risk.
CYB-015	Consumer Risk from Piracy in Latin America	Watters, P.A. - Macquarie University / Cyberstronomy Pty Ltd	2025	Uploaded PDF - Consumer-Risk-from-Piracy-in-LatAm-Report-EN.pdf	E2 - Actual case study or experiment	Empirical Latin American piracy risk assessment across Colombia, Ecuador, Mexico, Argentina, Peru and Chile finds piracy portals were 21.77× more likely to contain cyber threats than legitimate websites under conservative assumptions, rising to 39.18× in the worst-case model.
CYB-016	Addressing Evolving Digital Piracy Through Contributory Liability for Copyright Infringement: The Mobdro Case Study	Kiškis, M. - Masaryk University Journal of Law and Technology	2023	DOI: 10.5817/MUJLT2023-2-3; Uploaded PDF - 33184-Article Text-60373-1-10-20230930.pdf	E2 - Actual case study or experiment	Peer-reviewed legal/technical case study of the Mobdro dedicated piracy platform, which reportedly reached more than 100 million users and was taken down following a Europol investigation.
CYB-017	Risk Analysis of Home User's Vulnerability to Illegal Video Streaming Platform	Delos Santos, M.S.V.; Etorma, A.D.; Ocampo, H.A.; Panjaitan, A.E.; Romualdo, J.M.B.; Blancaflor, E.B. - Mapua University / ACM MSIE 2022	2022	DOI: 10.1145/3535782.3535830; Uploaded PDF - 3535782.3535830.pdf	E2 - Actual case study or experiment	Survey and scanning study of home-user exposure to illegal streaming sites.
CYB-018	Fighting Against Piracy: An Approach to Detect Pirated Video Websites Enhanced by Third-party Services	Li, Z.; Zhang, S.; Yin, J.; Du, M.; Zhang, Z.; Liu, Q. - Chinese Academy of Sciences / University of Chinese Academy of Sciences	2022	DOI: 10.1109/ISCC55528.2022.9912777; Uploaded PDF - Fighting_Against_PiracyAn_Approach_to_Detect_Pirated_Video_We	E2 - Actual case study or experiment	Empirical IEEE study proposes TEP-Net for detecting pirated video websites using domain-name semantics plus third-party service relationships.

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
				bsites_Enhanced_by_Third-party_Services.pdf		
CYB-019	Unmasking the Shadows: A Cross-Country Study of Online Tracking in Illegal Movie Streaming Services	Sheaib, H.; Feldmann, A.; Dao, H. - Proceedings on Privacy Enhancing Technologies	2025	DOI: 10.56553/popets-2025-0053; Uploaded PDF - content.pdf	E2 - Actual case study or experiment	Cross-country measurement study of illegal movie streaming services (IMSS).
CYB-020	Investigating IPTV Malware in the Wild	Lockett, A.; Chalkias, I.; Yucel, C.; Henriksen-Bulmer, J.; Katos, V. - Future Internet	2023	DOI: 10.3390/fi15100325; Uploaded PDF - futureinternet-15-00325-v2.pdf	E2 - Actual case study or experiment	Empirical malware-analysis study of illegal IPTV technologies.
CYB-021	The Price of Free Illegal Live Streaming Services	Ayers, H.; Hsiao, L. - Stanford University	2019	arXiv:1901.00579; Uploaded PDF - 1901.00579v1.pdf	E2 - Actual case study or experiment	Empirical study of free illegal live sports streaming services.
CYB-022	Understanding the Brains and Brawn of Illicit Streaming App	Huang, K.; Zhang, K.; Chen, J.; Sun, M.; Sun, W.; Tang, D.; Zhang, K. - Chinese University of Hong Kong / National University of Defense Technology / ICDF2C 2021	2022	DOI: 10.1007/978-3-031-06365-7_12; Uploaded PDF - 978-3-031-06365-7_12.pdf	E2 - Actual case study or experiment	Empirical forensic study of illicit streaming apps (ISAs) and illicit streaming devices.
CYB-023	Is cyber hygiene a remedy to IPTV infringement? A study of online streaming behaviours and cyber security practices	Shah, R.; Cemiloglu, D.; Yucel, C.; Ali, R.; Katos, V. - International Journal of Information Security	2024	DOI: 10.1007/s10207-024-00824-0; Uploaded PDF - 10.1007_s10207-024-00824-0.pdf	E2 - Actual case study or experiment	Empirical UK survey study of IPTV viewing risk, cyber hygiene and online streaming behaviour.
CYB-024	Watch Out Your TV Box: Reversing and Blocking a P2P-based Illegal Streaming Ecosystem	Ahn, J.; Jung, S.; Yoo, S.; Park, J.; Lee, S. - Korea University / USENIX Security Symposium	2025	USENIX Security 2025; Uploaded PDF - usenixsecurity25-ahn.pdf	E2 - Actual case study or experiment	Empirical reverse-engineering and measurement study of the EVPAD illicit streaming device ecosystem.
CYB-025	Ransomware Through the Lens of State Crime: Conceptualizing Ransomware Groups as Cyber Proxies, Pirates, and Privateers	Martin, J.; Whelan, C. - Deakin University / State Crime	2023	DOI: 10.13169/statecrime.12.1.0004; Uploaded PDF - SCJ_12_1_Martin and Whelan.pdf	E3 - Strong analogue or observation	Peer-reviewed conceptual analysis applies state-crime theory to ransomware groups, focusing on Russian-linked groups such as DarkSide and REvil and framing some ransomware actors as cyber proxies, pirates or cyber privateers.
CYB-026	Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime	Broadhurst, R.; Grabosky, P.; Alazab, M.; Bouhours, B.; Chon, S. - ANU Cybercrime Laboratory / International Journal of Cyber Criminology	2014	SSRN: https://ssrn.com/abstract=2461983; Uploaded PDF - ssrn-2461983.pdf	E3 - Strong analogue or observation	Scholarly analysis of the organisation of cybercrime groups, combining cybercrime theory, typologies and illustrative cases.
CYB-027	Cyber Crime	Choo, K.-K. R.; Grabosky, P. - Oxford Handbook of Organized Crime	2013	SSRN: https://ssrn.com/abstract=2340803; Uploaded PDF - ssrn-2340803.pdf	E3 - Strong analogue or observation	Authoritative handbook chapter on organised cybercrime distinguishes traditional organised crime groups using ICT, organised cybercriminal groups operating online, and ideologically or politically motivated groups including state and state-sponsored actors.
CYB-028	The looming shadow of illicit trade on the internet	Chaudhry, P. E. - Villanova School of Business / Business Horizons	2017	DOI: 10.1016/j.bushor.2016.09.002; Uploaded PDF - 1-s2.0-S0007681316300908-main.pdf	E3 - Strong analogue or observation	Article synthesises evidence on illicit digital-content ecosystems, cyberlockers, darknet markets and malware/crimeware linkages.
CYB-029	Organised crime groups in cyberspace: a typology	Choo, K.-K. R. - Australian Institute of Criminology / Trends in Organized Crime	2008	DOI: 10.1007/s12117-008-9038-9; Uploaded PDF - organised-cyber.pdf	E3 - Strong analogue or observation	Peer-reviewed typology of organised crime groups operating in or exploiting cyberspace.
CYB-030	Criminal Exploitation of Online Systems by Organised Crime Groups	Choo, K.-K. R.; Smith, R. G. - Australian Institute of Criminology / Asian Criminology	2008	DOI: 10.1007/s11417-007-9035-y; Uploaded PDF - Criminal_Exploitation_of_Online_Systems.pdf	E3 - Strong analogue or observation	Peer-reviewed article analysing how organised crime groups exploit online systems and information and communications technologies.
CYB-031	The Internet, Technology, and Organized Crime	Grabosky, P. - Australian National University / Asian Criminology	2007	DOI: 10.1007/s11417-007-9034-z; Uploaded PDF - s11417-007-9034-z.pdf	E3 - Strong analogue or observation	Peer-reviewed article examining how organised criminal groups exploit digital technology, including software piracy, credit-card fraud, child pornography, electronic funds transfer fraud, online dealing, money laundering, industrial

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
						espionage, denial-of-service attacks and terrorist use of cyberspace.
CYB-032	Examining the Psychosocial and Behavioral Factors Associated with Adolescent Engagement in Multiple Types of Cyberdeviance: Results from an Australian Study	Brewer, R.; Whitten, T.; Logos, K.; Sayer, M.; Langos, C.; Holt, T. J.; Cale, J.; Goldsmith, A. - Journal of Child and Family Studies	2023	DOI: 10.1007/s10826-023-02586-0; Uploaded PDF - s10826-023-02586-0.pdf	E3 - Strong analogue or observation	Empirical Australian school-based study of 327 adolescents examining psychosocial and behavioural factors associated with multiple forms of cyberdeviance, including digital piracy, hacking, cyberfraud, cyberbullying, sexting, cyberhate and cyberviolence.
CYB-033	Characterising and predicting cyber attacks using the Cyber Attacker Model Profile (CAMP)	Watters, P.A.; McCombie, S.; Layton, R.; Pieprzyk, J. - Journal of Money Laundering Control	2012	DOI: 10.1108/13685201211266015; Uploaded PDF - 13685201211266015.pdf	E3 - Strong analogue or observation	Peer-reviewed modelling paper proposing the Cyber Attacker Model Profile (CAMP) to characterise and predict cyber attacks using social, economic and demographic indicators.
CYB-034	An In-Depth Measurement of Security and Privacy Risks in the Free Live Sports Streaming Ecosystem	Muruganandham, Sharma & Keshvadi - Journal of Cybersecurity and Privacy	2026	https://www.mdpi.com/2624-800X/6/1/8	E2 - Actual case study or experiment	Empirical measurement study of the free live sports streaming ecosystem, examining security and privacy risks during major sporting events.
CYB-035	Unveiling the Connection Between Malware and Pirated Software in Southeast Asian Countries: A Case Study	Iqbal et al. - IEEE Open Journal of the Computer Society	2024	https://www.computer.org/csdl/journal/oj/2024/01/10430375/1UoCfv1yEmI	E2 - Actual case study or experiment	Peer-reviewed empirical case study linking pirated software to malware exposure in Southeast Asian countries.
CYB-036	Consumer Risk from Piracy in Poland	Watters, P.A. - Motion Picture Association EMEA / Cyberstronomy Pty Ltd	2024	https://www.mpa-emea.org/wp-content/uploads/2024/09/Watters-Consumer-Risk-from_Piracy-in-Poland.pdf	E2 - Actual case study or experiment	European comparator study quantifying relative consumer cyber risk across piracy categories.
CYB-037	TorrentGuard: Stopping scam and malware distribution in the BitTorrent ecosystem	Kryczka, Cuevas, Gonzalez, Cuevas & Azcorra - Computer Networks / arXiv	2011	https://arxiv.org/abs/1105.3671	E2 - Actual case study or experiment	Empirical BitTorrent ecosystem study finding a substantial fake-content problem.
CYB-038	Movie Pirates of the Caribbean: Exploring Illegal Streaming Cyberlockers	Ibosiola et al. - ICWSM / arXiv	2018	https://arxiv.org/abs/1804.02679	E2 - Actual case study or experiment	Empirical ecosystem analysis of illegal streaming cyberlockers.
CYB-039	Binge, Bot, Repeat: Unpacking the Ecosystem of Video Piracy on Telegram	Gyawali et al. - arXiv	2026	https://arxiv.org/abs/2605.08418	E2 - Actual case study or experiment	Large-scale analysis of video piracy on Telegram, examining channels, posts and bot-enabled distribution.
CYB-040	BADBOX Botnet Is Back	Pedro Falé / Bitsight TRACE	2024	https://www.bitsight.com/blog/badbox-botnet-back	E2 - Actual case study or experiment	Bitsight TRACE telemetry identified more than 192,000 BADBOX-infected Android devices, including more than 160,000 devices belonging to unique models not previously observed.
CYB-041	Home Internet Connected Devices Facilitate Criminal Activity	Federal Bureau of Investigation (FBI)	2025	https://www.fbi.gov/investigate/cyber/alerts/2025/home-internet-connected-devices-facilitate-criminal-activity	E2 - Actual case study or experiment	FBI public service announcement warning that cyber criminals exploit IoT devices connected to home networks, including TV streaming devices, digital projectors, aftermarket infotainment systems and other products, using the BADBOX 2.0 botnet.
CYB-042	Google's Continued Disruption of Malicious Residential Proxy Networks	Google Threat Intelligence Group (GTIG)	2026	https://cloud.google.com/blog/topics/threat-intelligence/google-continued-disruption-residential-proxy-networks	E2 - Actual case study or experiment	Google, in coordination with the FBI, Lumen and others, disrupted the NetNut residential proxy network, also known as Popa.
CYB-043	Russian GRU Exploiting Vulnerable Routers to Steal Sensitive Information	FBI, NSA and international partners	2026	https://www.ic3.gov/PSA/2026/PSA260407	E2 - Actual case study or experiment	FBI/IC3 alert stating that Russian GRU cyber actors exploited vulnerable routers worldwide to intercept and steal sensitive military, government and critical-infrastructure information.
CYB-044	Defending against China-nexus covert networks of compromised devices	NCSC-UK, ASD ACSC, CISA, FBI, NSA and international partners	2026	https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/defending-against-china-nexus-covert-networks-of-compromised-devices	E2 - Actual case study or experiment	Joint allied advisory describing a shift by China-nexus cyber actors from individually procured infrastructure to large-scale covert networks built from compromised SOHO routers, IoT devices and smart devices.

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
CYB-045	Russian Botnet Disrupted in International Cyber Operation	U.S. Department of Justice / FBI	2022	https://www.justice.gov/usao-sdca/pr/russian-botnet-disrupted-international-cyber-operation	E2 - Actual case study or experiment	DOJ announcement of the disruption of RSOCKS, a Russian botnet operated by Russian cybercriminals that compromised millions of devices worldwide.
CYB-046	Read This Before You Buy That TV Streaming Stick	Krebs on Security, reporting Bitsight TRACE (Falé) and Synthient research	2026	https://krebsonsecurity.com/2026/07/read-this-before-you-buy-that-tv-streaming-stick/	E2 - Actual case study or experiment	H96-family streaming devices ship with pre-installed residential-proxy software and are centrally orchestrated by a named China-based operator (Zhejiang Fengwo IoT Technology, via HK/Singapore shells).
CYB-047	LG to Ban Residential Proxies from Smart TV Apps	Krebs on Security (Krebs, B.), reporting Spur research (Sutter, T.)	2026	https://krebsonsecurity.com/2026/07/lg-to-ban-residential-proxies-from-smart-tv-apps/	E2 - Actual case study or experiment	LG Electronics USA stated it will suspend webOS apps that turn smart TVs into always-on residential proxy nodes, after Spur research found proxy SDKs in over 42 per cent of apps in LG's webOS store and in more than a quarter of apps for Samsung's Tizen platform.
CYB-048	Cybercrime by Doorbell: How Illicit Actors “Borrow” the Internet Connections of Millions of Americans for Profit and Harm - And the Companies That (Knowingly or Unknowingly) Enable it to Happen	Digital Citizens Alliance & risk3sixty	2026	https://resproxy.digitalcitizensalliance.org/hubfs/resproxy/DCA_Cybercrime-by-Doorbell-Report.pdf	E2 - Actual case study or experiment	Joint investigation combining direct testing of piracy-oriented streaming devices with residential-proxy measurement and enforcement case synthesis.

Annotated Bibliography – Organised Crime Financing

This annotated bibliography documents the principal evidence used to assess organised-crime financing associated with illegal IPTV and the wider illegal streaming ecosystem. It records the source, evidence classification and its principal contribution to the assessment, but does not reproduce every dimension of the analytical process. The Chapter 5 findings also considered the plausibility of the financing mechanisms, capability and scale of the actors involved, comparable cases and enforcement evidence, Nordic relevance, potential impact, attribution limitations and the level of confidence warranted by the evidence. The bibliography therefore represents the evidentiary record supporting the analysis rather than a complete risk-assessment matrix.

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
OCF-001	Film Piracy, Organized Crime, and Terrorism (MG-742)	Treverton, Matthies, Cunningham, Goulka, Ridgeway, Wong - RAND Corporation	2009	https://www.rand.org/pubs/monographs/MG742.html	E2 - Actual case study or experiment	14 case studies across North America, Europe, Asia, and Latin America establish a broad, geographically dispersed connection between film/content piracy and organised crime.
OCF-002	A Systematic Approach to Measuring Advertising Transparency Online: An Australian Case Study	Watters, P.A. - Internet Commerce Security Laboratory (ICSL), University of Ballarat	2013	https://ssrn.com/abstract=2362621	E2 - Actual case study or experiment	Empirical audit of 5,000 pages drawn from Google's top-500 DMCA complaints (movies/TV) reveals that 99% of advertising on rogue torrent and file-locker sites is High-Risk: 46% malware/fake software, 20% sex industry, 16% scams, and 15% downloading sites.
OCF-003	Measuring Online Advertising Transparency in Singapore: An Investigation of Threats to Users	Watters, P.A. - Internet Commerce Security Laboratory (ICSL), University of Ballarat	2013	https://ssrn.com/abstract=2362626	E2 - Actual case study or experiment	Geotargeted empirical audit of 5,000 webpages from Google's top-500 DMCA complaints (movies/TV, May–July 2013), collected from a Singapore-based data collection system, finds that 90% of advertising on rogue sites is High-Risk and only 10% Mainstream - a markedly different composition from a parallel Australian study (99% High-Risk / 1% Mainstream) by the same author.
OCF-004	Mainstream Advertising Support for Online Piracy in Taiwan	Watters, P.A. - Massey University	2014	https://ssrn.com/abstract=2405281	E2 - Actual case study or experiment	Geotargeted empirical audit of 1,000 webpages from ten known rogue sites in Taiwan (2014) finds a markedly different ad composition from prior studies in Australia, Singapore, and Canada: 61% of ads are Mainstream and only 39% High-Risk - meaning Taiwanese users see approximately 40 times more mainstream advertising on rogue sites than Australians.
OCF-005	Sweet As? Advertising on Rogue Websites in New Zealand	Watters, P.A. - Massey University	2014	https://ssrn.com/abstract=2466696	E2 - Actual case study or experiment	Geotargeted empirical audit of 8,230 webpages drawn from Google's top-500 DMCA complaints (movies/TV: 5,000 pages; music: 3,210 pages), collected from a New Zealand-based data collection system (May–July 2013), finds that 96.34% of movie/TV advertisements and 93.26% of music advertisements on rogue sites are High-Risk.
OCF-006	Mainstream Advertising on Rogue Websites in Hong Kong: A Comparison of Chinese and Western Titles	Watters, P.A. - Massey University	2014	https://ssrn.com/abstract=2468700	E2 - Actual case study or experiment	Dual-sample geotargeted empirical audit of 5,380 webpages collected from a Hong Kong-based data collection system: 5,000 pages drawn from Google's top-500 DMCA complaints (Hollywood movies/TV, May–July 2013) and 380 pages from 38 expert-identified rogue sites hosting Chinese-language local content.
OCF-007	Mainstream Advertising on Rogue Websites in Malaysia: A Comparison of Local and Foreign Content	Watters, P.A. - Massey University	2014	https://ssrn.com/abstract=2469606	E2 - Actual case study or experiment	Dual-sample geotargeted empirical audit of 5,360 webpages collected from a Malaysia-based data collection system: 5,000 pages drawn from Google's top-500 DMCA complaints (Hollywood movies/TV, March 2014) and 360 pages

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
						from 36 expert-identified rogue sites hosting Malay-language local content.
OCF-008	How Risky Are Piracy Websites For Indonesians? The Role of Search	Watters, P.A. - Massey University	2014	https://ssrn.com/abstract=2469609	E2 - Actual case study or experiment	Geotargeted empirical audit of 1,000 webpages from 100 Indonesian-language rogue sites, sampled via a snowball methodology replicating user search behaviour (seed term: 'mendownload film'; Bahasa terms terbaru, gratis, baru, situs, cara, bioskop iteratively expanded).
OCF-009	The Impact of High Risk Advertising on Thai Social Values: The Role of Piracy Websites	Watters, P.A. - Massey University	2015	https://ssrn.com/abstract=2572058	E2 - Actual case study or experiment	Geotargeted empirical audit of 430 webpages from 43 Thai-language rogue sites, sampled via snowball methodology (seed term: Thai transliteration of 'download film'; iterative expansion via Thai-language piracy search terms including free download film, online, dare).
OCF-010	An Analysis of Piracy Website Advertising in Brazil and Its Linkages to Child Exploitation Material	Watters, P.A. - ECPAT International	2015	https://www.ecpat.net/	E2 - Actual case study or experiment	Geotargeted empirical audit of 1,000 pages from the Top 100 most-complained-about piracy sites (Google Transparency Report, September 2015) and a local-language Portuguese snowball sample of the Top 50 most popular Brazilian piracy sites, using a Brazil-based VPN.
OCF-011	Organized. Piracy. Crime. How Global Piracy Networks Became Organized Crime Syndicates – And What Needs to be Done About it	Digital Citizens Alliance (DCA) / IP House	2026	https://ip-house.com/assets/Uploads/resources/DCA-IPH-Organized.-Piracy.-Crime.pdf	E2 - Actual case study or experiment	Joint investigation by DCA and IP House synthesising law enforcement interviews, court records, criminal case reviews, and prior reports to establish that global IPTV and digital piracy networks meet the definitional criteria of organised crime set by INTERPOL, Europol, and UNODC.
OCF-012	Intellectual Property Crime Threat Assessment 2019	Europol / European Union Intellectual Property Office (EUIPO)	2019	Uploaded PDF - 2019_IP_Crime_Threat_Assessment_Report.pdf	E2 - Actual case study or experiment	Official Europol/EUIPO strategic threat assessment finds that IP crime, including piracy, is lucrative and low-risk; organised crime groups are increasingly involved in counterfeit and pirated goods; online marketplaces, social media and piracy platforms generate income through sales, subscriptions and advertising, with illegal IPTV and cross-border server/payment arrangements complicating enforcement.
OCF-013	Nordic Piracy Spring 2023	Mediavision AB / Rights Alliance (Rättighetsalliansen)	2023	Uploaded PDF - Nordic Piracy 2023 - 3 maj 2023 Sara Lindbäck Rättighetsalliansen[1].pdf	E2 - Actual case study or experiment	Pan-Nordic consumer survey finds 4.4 million people aged 15–74 used piracy services in the past month (+1.0 million vs 2022), with 1.15 million households subscribing to illegal IPTV.
OCF-014	Dangerous Liaisons: Why IP Infringements Are the New Eldorado for Organized Crime	INDICAM / UNICRI - Bergonzi, Anselmino & Musumeci	2020	Uploaded PDF - IP OC.pdf	E3 - Strong analogue or observation	Position paper from INDICAM/UNICRI conference evidence argues that IP infringements and piracy are attractive to organised crime because of high profits, low enforcement risk, transnational alliances, legal-economy infiltration, and laundering pathways.
OCF-015	Uncovering the Ecosystem of Intellectual Property Crime: A Focus on Enablers and Impact	Europol / European Union Intellectual Property Office (EUIPO)	2024	DOI: 10.2814/1947113; Uploaded PDF - 2024_Uncovering_the_ecosystem_of_IP_Crime_FullR_en.pdf	E2 - Actual case study or experiment	Official Europol/EUIPO EMPACT strategic analysis describes IP crime as a complex ecosystem involving criminal networks, legal-business misuse, cyber-enabled activity, social commerce, document fraud, corruption, labour exploitation and money laundering.
OCF-016	Nordic Content Protection Trend Report 2016: Criminal Developments in Illegal Distribution and Selling of Illegal Access to Television Broadcasts	Procope AS / Nordic Content Protection	2016	Uploaded PDF - Trend-report-Nordic-Content-Protection-2016.pdf	E2 - Actual case study or experiment	Nordic market trend report estimates illegal TV access via cardsharing, IPTV and streaming caused approximately NOK 4 billion in annual industry revenue loss, with Nordic criminal operators earning around NOK 600 million annually from roughly 350,000–400,000 customers.

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
OCF-017	Nordic Content Protection Trend Report 2017: Illegal Distribution and Sales of Access to Television Broadcasts	Procope AS / Nordic Content Protection	2017	Uploaded PDF - Trend-Report-2017.pdf	E2 - Actual case study or experiment	Nordic market trend report estimates 400,000 illegal subscriptions, an annual lost earning potential for legal distributors of €531.6 million, and annual illegal distributor turnover of €77.9 million.
OCF-018	Nordic Content Protection Case Studies 2018	Nordic Content Protection	2018	Uploaded PDF - Nordic-Content-Protection-Case-Studies-2018.pdf	E2 - Actual case study or experiment	NCP presents two direct Nordic enforcement case studies: a Swedish card-sharing network and a Danish illegal IPTV reseller case.
OCF-019	Norwegian teenager convicted for his role in murder-for-hire ordered by Iran-linked crime gang	Associated Press / ABC News	2026	https://abcnews.com/International/wireStory/norwegian-teenager-convicted-role-murder-hire-ordered-iran-135193057	E2 - Actual case study or experiment	A Norwegian teenager was convicted at the Old Bailey in July 2026 of conspiracy to murder after travelling from Norway to the UK to carry out a €25,000 contract killing, recruited on behalf of the **Foxtrot Network**, a Swedish organised-crime group with links to the Iranian regime.
OCF-020	NCP Annual Report 2020: Illegal IPTV Ecosystem	Nordic Content Protection	2020	Uploaded PDF - NCP-annual-report-2020-final.pdf	E2 - Actual case study or experiment	NCP annual report documents the illegal IPTV ecosystem as a mature, low-risk, revenue-generating business model.
OCF-021	The EPL Drama – Paving the Way for More Illegal Streaming? Digital Piracy of Live Sports Broadcasts in Singapore	Wong, D. - Leisure Studies / Coventry University Repository accepted manuscript	2015	https://doi.org/10.1080/02614367.2015.1035315; Uploaded PDF - THE EPL DRAMA III.pdf	E3 - Strong analogue or observation	Peer-reviewed study of EPL and live-sports piracy in Singapore identifies the principal digital sports piracy modes: live internet retransmission via P2P and UGC live sites, recorded uploads, highlights on UGC/social platforms, and illegal set-top/signal boxes.
OCF-022	Causes and Prevention of Digital Intellectual Property Theft in the Entertainment Industry	Haartveit, E. - Siam University MBA Independent Study	2019	Uploaded PDF - IMBA-2019-IS-Causes-and-Prevention-of-Intellectual-Property-Theft-in-the-Entertainment-Industry.pdf	E3 - Strong analogue or observation	Documentary/literature study on internet piracy in the entertainment industry identifies key piracy drivers including unavailable content, high legal pricing, regional release delays, convenience and low perceived risk.
OCF-023	Iniquitous Cord-Cutting: An Analysis of Infringing IPTV Services	Pandey, P.; Aliapoulios, M.; McCoy, D. - New York University / IEEE EuroS&PW	2019	https://doi.org/10.1109/EuroSPW.2019.00054; Uploaded PDF - Iniquitous_Cord-Cutting_An_Analysis_of_Infringing_IPTV_Services.pdf	E2 - Actual case study or experiment	Empirical study of subscription-based infringing IPTV services measuring technical infrastructure, payment channels and revenue.
OCF-024	The costs of serious and organised crime in Australia, 2023–24	Voce, A.; Morgan, A. - Australian Institute of Criminology	2025	https://doi.org/10.52922/78113; Uploaded PDF - sr55_costs_of_serious_and_organised_crime_in_australia_2023-24.pdf	E3 - Strong analogue or observation	Official AIC statistical report estimates serious and organised crime cost Australia $35.5b–$82.3b in 2023–24, including direct serious and organised crime costs up to $47.9b, organised financial crime up to $13.2b, illicit commodities up to $8.6b, pure cybercrime up to $4.5b, and IP infringement involving serious and organised crime up to $3.25b.
OCF-025	International Legal Regulation of Copyright and Related Rights Protection in the Digital Environment	Hubanov, O.; Hubanova, T.; Kotliarevska, H.; Vikhliaiev, M.; Donenko, V.; Lepekh, Y. - Estudios de Economía Aplicada	2021	https://doi.org/10.25115/eea.v39i7.5014; Uploaded PDF - mlpezgarcia,+Paper_5014_with+authors_revisar(2).pdf	E3 - Strong analogue or observation	Legal-review article identifies digital copyright infringement and piracy as cross-border IP crime concerns, cites EUIPO estimates of up to €60b annual damage in selected EU sectors, and notes that organised crime groups are increasingly involved in IP rights infringements and may use profits to fund other illegal activity.
OCF-026	Copyright, Crime and Computers: New Legislative Frameworks for Intellectual Property Rights Enforcement	Urbas, G. - Australian National University / Journal of International Commercial Law and Technology	2012	Uploaded PDF - 01_Urbas_Copyright,_Crime_and_2012.pdf	E3 - Strong analogue or observation	Legal analysis of Australian and cross-border criminal IPR enforcement shows that online piracy has evolved from individual file-sharing into more complex infringement ecosystems involving file-sharing platforms, website operators, criminal copyright offences, cybercrime powers, covert investigations, mutual legal assistance, extradition, prosecution and proceeds-of-crime recovery.
OCF-027	Confiscation of the Proceeds of IP Crime: A modern tool for deterring counterfeiting and piracy	UNICRI / ICC BASCAP	2013	Uploaded PDF - Confiscation of the Proceeds of IP Crime.pdf	E3 - Strong analogue or observation	UNICRI/BASCAP report argues that counterfeiting and piracy are lucrative, low-risk markets increasingly exploited by organised criminal networks, with

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
						proceeds used to fund other serious crimes and laundered through legitimate and illicit channels.
OCF-028	IP Crime and Enforcement Report 2018–19	UK Intellectual Property Office / IP Crime Group	2019	Uploaded PDF - IP-Crime-Report-2019.pdf	E2 - Actual case study or experiment	Official UK IP Crime Group report states that IP crime is a feature of organised crime and highly profitable, accounting for almost 4% of UK imports (£9.3 billion), £4 billion in lost tax revenue and 60,000 UK jobs.
OCF-029	Organised crime research in Australia 2018	Smith, R. G. (ed.) - Australian Institute of Criminology	2018	Uploaded PDF - rr10_for_online_0.pdf	E4 - Technically or socially plausible	Official AIC peer-reviewed edited research report synthesises Australian organised-crime research, including definitions of organised crime, transnational criminal markets, cryptomarkets, anti-money-laundering obligations, cybercrime partnerships, and the challenges of evidence, intelligence and law-enforcement response.
OCF-030	Study on Business Models Infringing Intellectual Property: Phase 5 - Modus Operandi of Serious and Organised Crime	European Union Intellectual Property Office (EUIPO), with CEIPI/BETA University of Strasbourg and UNICRI support	2022	DOI: 10.2814/485139; Uploaded PDF - 2023_Study_on_Business_Models_Infringing_IP_Phase_5_FullR_en.pdf	E2 - Actual case study or experiment	EUIPO study analyses serious and organised IP-infringing business models using confidential case studies from criminal investigations and prosecutions across EU Member States.
OCF-031	Cross-national investigation and prosecution of intellectual property crimes: the example of "Operation Buccaneer"	Urbas, G. - Australian National University / Crime, Law and Social Change	2007	DOI: 10.1007/s10611-007-9060-x; Uploaded PDF - Cross-national_investigation_a.pdf	E2 - Actual case study or experiment	Case study of Operation Buccaneer, a coordinated cross-national law enforcement operation against DrinkOrDie, a highly organised but globally dispersed internet-based software piracy group.
OCF-032	International Proposals for the Criminal Enforcement of Intellectual Property Rights: International Concern with Counterfeiting and Piracy	Blakeney, M. - Queen Mary University of London, School of Law	2009	https://ssrn.com/abstract=1476964; Uploaded PDF - ssrn-1476964.pdf	E3 - Strong analogue or observation	Academic legal analysis of international concern with counterfeiting and piracy, tracing the movement from TRIPS enforcement provisions to proposals for stronger criminal enforcement, ACTA, border measures, internet distribution controls, optical-disc piracy regulation, confiscation of proceeds and extradition.
OCF-033	International Illicit Convergence: The Growing Problem of Transnational Organized Crime Groups' Involvement in Intellectual Property Rights Violations	Walterbach, M. - Florida State University Law Review	2007	https://ir.law.fsu.edu/lr/vol34/iss2/10; Uploaded PDF - International Illicit Convergence_ The Growing Problem of Transna.pdf	E3 - Strong analogue or observation	Legal scholarship analysing the convergence between transnational organised crime and intellectual property rights violations.
OCF-034	Patterns of piracy: Sci-Hub and Sweden 2011–2018	Kjellström, Z. - Umeå University / Internet Histories	2025	DOI: 10.1080/24701475.2025.2482459; Uploaded PDF - Patterns of piracy Sci-Hub and Sweden 2011 2018.pdf	E2 - Actual case study or experiment	Empirical study of text-piracy patterns in Sweden from 2011–2018 using complete publicly available download datasets from Sci-Hub and Library Genesis, including 8,339 Swedish Sci-Hub requests from 2011–2013, 29,373 from 2015–2016, 619,324 from 2017, and 63,595 Library Genesis requests from 2014–2015.
OCF-035	Pirates of the Atlantic: at a decade's end	Valgarðsson, V. O.; Ómarsdóttir, S. B.; Önnudóttir, E. H. - University of Iceland / Comparative European Politics	2026	DOI: 10.1057/s41295-026-00467-6; Uploaded PDF - s41295-026-00467-6.pdf	E4 - Technically or socially plausible	Peer-reviewed political-science study of the Icelandic Pirate Party from its founding in 2012 to its loss of parliamentary representation in the 2024 snap election.
OCF-036	Policing the Grey Zone	Caparini & Last (eds.) - NATO DEEP eAcademy Press	2025	Uploaded PDF - Policing-the-Grey-Zone.pdf#page=31.pdf	E4 - Technically or socially plausible	Edited NATO DEEP volume frames grey-zone and hybrid threats confronting democratic states and societies, including Russian hybrid warfare against the EU/NATO, information operations, cyber-operations, economic coercion, critical-infrastructure pressure, proxy actors and cross-domain disruption.
OCF-037	Resilience as Deterrence: Towards a Comprehensive Security Panorama	Laine, J. P.; Petersson, B. (eds.) - NATO Science for Peace and Security Series / IOS Press	2025	DOI: 10.3233/NHSDP159; Uploaded PDF - 17652747202461648 41.pdf	E4 - Technically or socially plausible	NATO SPS edited volume on resilience-as-deterrence frames NATO borderland regions, including Finland, Sweden, Norway and the Baltic region, as strategic assets exposed to Russian hybrid threats.

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
OCF-038	Drivers and Implications of Military Policing: Evidence from Italy	Mazziotti di Celso, M. - University of Genoa / NATO DEEP eAcademy Press	2025	Uploaded PDF - Policing-the-Grey-Zone.pdf#page=126.pdf	E4 - Technically or socially plausible	Peer-reviewed chapter in the NATO DEEP edited volume Policing the Grey Zone analysing the growth of military policing and why democratic states deploy armed forces for internal security tasks.
OCF-039	The Determinants of Organized Crime: An Economic Analysis	Ljung, A. - Umeå University	2025	Uploaded PDF - FULLTEXT01.pdf	E3 - Strong analogue or observation	Swedish empirical thesis analysing economic and socioeconomic determinants of organised crime, focused on non-titled/externally defined criminal networks commonly described as street gangs.
OCF-040	Exploring Overlaps of Cultural Property Crime with Organised Crime in EU Policy Documents	Faraldo Cabana, P. - University of A Coruña / European Journal on Criminal Policy and Research	2024	DOI: 10.1007/s10610-024-09595-9; Uploaded PDF - s10610-024-09595-9.pdf	E3 - Strong analogue or observation	Peer-reviewed content analysis of 58 EU policy documents from 1993–2023 examining how EU policy conceptualises overlaps between trafficking in cultural property, organised crime, terrorist financing, money laundering, corruption and other illicit trafficking.
OCF-041	Organised crime in Spain: Determining factors, characteristics and response	Jaime, Ó.; de Castro, A. - Routledge	2025	DOI: 10.4324/9781003536284-2; Uploaded PDF - 10.4324_9781003536284-2_chapterpdf(1).pdf	E4 - Technically or socially plausible	Book chapter analysing organised crime in Spain as a national-security threat, including transnational criminal groups, drug trafficking, money laundering, legal-economy infiltration, state/criminal collaboration in hybrid confrontation, and foreign organised-crime actors operating in Spain, including Nordic-linked groups.
OCF-042	Gang involvement among adolescents in nine Nordic cities: A comparative study on associated risk factors	Kaakinen, M.; Westfelt, L.; Moeller, K.; Rostami, A.; Valdimarsdóttir, M.; Langeland, C. L.; Jensen, A. V. - European Journal of Criminology	2026	DOI: 10.1177/14773708251400845; Uploaded PDF - kaakinen-et-al-2026-gang-involvement-among-adolescents-in-nine-nordic-cities-a-comparative-study-on-associated-risk.pdf	E2 - Actual case study or experiment	Peer-reviewed comparative Nordic study of adolescent street-gang involvement across nine cities in Denmark, Finland, Iceland, Norway and Sweden using ISRD4 probability city samples (n=9,039, ages 13–17) and the Eurogang measurement.
OCF-043	Immigration and Organized Crime in Sweden	Ciorba, N.-V.; Neagoș, I. - Studia Securitatis Journal	2025	DOI: 10.54989/stusec.2025.19.02.18; Uploaded PDF - Nadia-Victoriana-CIORBA286-296.pdf	E4 - Technically or socially plausible	Article reviews the relationship between immigration, integration pressures, vulnerable areas and organised crime in Sweden.
OCF-044	Stuck in Security: A WPR Analysis of Policy and Practice in Swedish International Cooperation Against Organised Crime	Lundqvist, A. - Lund University / Graduate School	2026	Uploaded PDF - Master_s_thesis_Alva_Lundqvist_FINAL.pdf	E4 - Technically or socially plausible	Master's thesis analysing how Swedish policy against organised crime is discursively constructed as a national-security issue and how that framing shapes Sweden's international cooperation.
OCF-045	Nordic Policy Responses to Gang-Related Crime 2009–2025: Policy Developments and Future Challenges in Denmark, Sweden and Norway	Johansen, M.-L. E.; Hedlund, A.; Tutenges, S. - European Journal on Criminal Policy and Research	2026	DOI: 10.1007/s10610-026-09662-3; Uploaded PDF - s10610-026-09662-3.pdf	E4 - Technically or socially plausible	Peer-reviewed document-based analysis of fifteen years of anti-gang policy responses in Denmark, Sweden and Norway.
OCF-046	Illegal IPTV in the European Union: Research on Online Business Models Infringing Intellectual Property Rights – Phase 3	EUIPO Observatory	2019	https://www.euipo.europa.eu/fr/publications/research-on-online-business-models-infringing-intellectual-property-rights-phase-3-illegal-iptv-in-the-european-union	E2 - Actual case study or experiment	EUIPO Phase 3 study estimates that illegal IPTV services in the EU generated EUR 941.7 million in unlawful revenue in 2018 and were used by 13.7 million EU citizens.
OCF-047	Taking the Profit Out of Intellectual Property Crime: Piracy, Organised Crime and the Need for a Financial Response	RUSI / White Bullet	2020	https://static.rusi.org/whr_ip_crime_web_version_0.pdf	E3 - Authoritative institutional / expert analysis	RUSI frames online piracy as a financial-crime and organised-crime problem rather than merely a copyright-enforcement issue.
OCF-048	Live Event Piracy Discussion Paper	EUIPO Observatory	2023	https://www.euipo.europa.eu/en/publications/live-event-piracy-discussion-paper	E3 - Authoritative institutional / expert analysis	EUIPO maps the live-event piracy ecosystem, including subscription-based IPTV, open IPTV streams, open web streaming, cyberlockers, social-media

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
						redistribution and other distribution channels.
OCF-049	Online Copyright Infringement in the European Union: Films, Music, Publications, Software and TV, 2017–2023	EUIPO Observatory	2024	https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_online_copyright_infringement/2024_online_copyright_infringement_in_the_EU_FullR_en.pdf	E2 - Actual case study or experiment	EUIPO provides EU-wide longitudinal measurement of online copyright infringement across films, music, publications, software and TV between 2017 and 2023.
OCF-050	Intellectual Property Crime Threat Assessment 2022	Europol / EUIPO	2022	https://www.europol.europa.eu/cms/sites/default/files/documents/Report.%20Intellectual%20property%20crime%20threat%20assessment%202022_2.pdf	E3 - Authoritative institutional / expert analysis	Europol and EUIPO assess IP crime as a serious and evolving criminal market, including online copyright infringement and digital distribution channels.
OCF-051	Findings of the monitoring exercise: Recommendation on combating online piracy of sports and other live events	EUIPO Observatory / European Commission	2025	https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/Combating_piracy/EUIPO-Findings_of_the%20monitoring_exercise-Recommendation_on_combating_live_event_piracy.pdf	E3 - Authoritative institutional / expert analysis	The monitoring exercise reports on implementation and effects of the European Commission Recommendation on combating online piracy of sports and other live events.
OCF-052	Crimintern: How the Kremlin uses Russia's criminal networks in Europe	Mark Galeotti - European Council on Foreign Relations (ECFR)	2017	https://ecfr.eu/publication/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe/	E3 - Authoritative institutional / expert analysis	Galeotti argues that Russian-based organised crime in Europe has been used by the Kremlin as a source of black cash, cyber capability, political influence, trafficking capacity and deniable operational support.
OCF-053	Gangsters at War: Russia's Use of Organized Crime as an Instrument of Statecraft	Mark Galeotti - Global Initiative Against Transnational Organized Crime (GI-TOC)	2024	https://globalinitiative.net/analysis/gangsters-at-war-russias-use-of-organized-crime-as-an-instrument-of-statecraft/	E3 - Authoritative institutional / expert analysis	Galeotti's post-2022 analysis frames Russian-based organised crime as increasingly relevant to Kremlin statecraft, including sanctions evasion, cyber activity, intelligence support, money laundering and destabilisation.
OCF-054	The Gangster as Actor and Agent in Russian Foreign Policy	Mark Galeotti - Europe-Asia Studies	2023	https://www.tandfonline.com/doi/full/10.1080/09668136.2022.2154316	E3 - Peer-reviewed / expert analysis	Peer-reviewed article examining organised crime groups as both actors in their own right and agents usable by other actors in Russian foreign policy.
OCF-055	The Vory: Russia's Super Mafia	Mark Galeotti - Yale University Press	2018	https://yalebooks.yale.edu/book/9780300243208/the-vory/	E3 - Authoritative expert / book-length analysis	Book-length account of the historical development, culture and adaptation of Russian organised crime, including the vory v zakone and the changing relationship between criminal networks, business and state power.
OCF-056	The Criminalisation of Russian State Security	Mark Galeotti - Global Crime	2006	https://doi.org/10.1080/17440570601073947	E3 - Peer-reviewed / expert analysis	Early peer-reviewed analysis of the penetration of Russian state security structures by criminal practices and organised-crime relationships.
OCF-057	How Russia is using intellectual property as a war tactic	Bonadio, E. & Trapova, A. - The Conversation (City, University of London; University of Nottingham)	2022	https://theconversation.com/how-russia-is-using-intellectual-property-as-a-war-tactic-179260	E3 - Expert legal commentary	Expert legal commentary on Russia's March 2022 decree removing compensation for holders of patents, utility models and industrial designs connected to sanctioning states, allowing Russian entities to exploit those rights without consent or payment.
OCF-058	Fishing in the Piracy Stream: How the Dark Web of Entertainment Is Exposing Consumers to Harm	Digital Citizens Alliance	2019	https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf	E2 - Actual case study or experiment	DCA consumer research found that 72% of respondents who used a credit card to purchase a piracy subscription later reported fraudulent charges, compared with 18% of non-pirating online streamers.

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
OCF-059	Consumer Harms and Fraud Pathways in Asia-Pacific's Illicit Streaming Economy	Watters, P.A. - Cyberstronomy Pty Ltd / Coalition Against Piracy (CAP), Asia Video Industry Association (AVIA)	2026	https://avia.org/new-study-reveals-piracy-services-are-exposing-millions-of-asia-pacific-consumers-to-cybercrime-identity-theft-and-fraud/	E2 - Actual case study or experiment	Empirical Asia-Pacific study using localised sock-puppets, direct purchase attempts, payment-flow analysis, forensic application and device testing, and intermediary mapping across IPTV playlists, illicit streaming devices, third-party applications, account resharing and IPTV subscriptions.
OCF-060	Money for Nothing: The Billion-Dollar Pirate Subscription IPTV Business	Digital Citizens Alliance / NAGRA	2020	https://www.digitalcitizensalliance.org/news/press-releases-2020/pirate-subscription-services-now-a-billion-dollar-u.s.-industry-joint-digital-citizens-alliance-nagra-report-finds/	E3 - Strong analogue or observation	DCA and NAGRA describe a US pirate-subscription IPTV market exceeding US$1 billion, serving an estimated 9 million fixed-broadband subscribers through at least 3,500 US-facing storefronts, social-media pages and online-marketplace outlets.
OCF-061	Iran is using criminal networks in Sweden	Swedish Security Service (Säkerhetspolisen)	2024	https://sakerhetspolisen.se/ovriga-sidor/other-languages/english-engelska/press-room/news/news/2024-05-30-iran-is-using-criminal-networks-in-sweden.html	E2 - Actual case study or experiment	The Swedish Security Service states that the Iranian regime uses criminal networks in Sweden to carry out violent acts against states, groups or individuals it regards as threats.
OCF-062	Åtgärder mot illegal ip-tv (SOU 2025:100)	Swedish Government / Filmutredningen	2025	https://www.riksdagen.se/sv/dokument-och-lagar/dokument/statens-offentliga-utredningar/atgarder-mot-illegal-ip-tv_hdb3100/html/	E3 - Authoritative institutional / expert analysis	The Swedish Government inquiry concludes that illegal IPTV is difficult to stop at source and that the legal position for private consumption is not sufficiently clear in all relevant cases.
OCF-063	Trusted flaggers under the Digital Services Act (DSA)	European Commission - DG CONNECT	2026	https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa	E3 - Authoritative institutional / expert analysis	The European Commission explains the DSA trusted-flagger framework under which national Digital Services Coordinators designate independent entities with particular expertise in identifying illegal online content.

Annotated Bibliography – Disinformation and AI

This annotated bibliography documents the principal evidence used to assess media-integrity and AI-enabled manipulation risk. It records the source, evidence classification and the particular capability, case, analogue or pathway that each source supports. Because this domain includes both demonstrated capabilities and prospective risks, the analysis in Chapter 6 also considered mechanism plausibility, actor capability and access requirements, case-study and analogue support, Nordic relevance, potential impact and confidence. The entries below should therefore be understood as an extract of the underlying evidence record: they establish the evidentiary basis for the assessment, while the chapter itself considers how those individual components may converge into a credible emerging risk.

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
DIS-001	The Nordic region and NATO: security relations in change	Græger, N. - Edward Elgar / Handbook of Nordic Cooperation	2025	DOI: 10.4337/9781035319725-29; Uploaded PDF - 9781035319725-chapter25.pdf	E4 - Technically or socially plausible	Book chapter analyses the transformation of Nordic security after Russia's 2022 invasion of Ukraine, including Finland and Sweden's NATO accession, the Nordic-Baltic region as a single strategic space, and the region's exposure to Russian hybrid warfare, disinformation campaigns, election interference, sabotage of energy/internet infrastructure, and broader challenges to democratic resilience.
DIS-002	Threats and Limitations of Terrestrial Broadcast Attacks	Michéle, Peña & Angueira. IEEE Transactions on Broadcasting	2018	https://doi.org/10.1109/TBC.2017.2704538	E2 - Actual case study or experiment	Peer-reviewed demonstration that, because DVB transport streams lack mandated authentication, attackers can overpower terrestrial transmissions to replace legitimate broadcasts and push a malicious HbbTV app gaining system-level Smart-TV control in under 10 s; field tests show co-channel constraints sharply limit range and stealth.
DIS-003	You Have Been Warned: Abusing 5G's Warning and Emergency Systems	Bitsikas & Pöpper. ACSAC '22.	2022	https://arxiv.org/abs/2207.02506	E2 - Actual case study or experiment	First comprehensive study of 5G Public Warning System security, demonstrating five practical attacks - two spoofing fake CMAS/ETWS alerts and three suppressing genuine ones, including a 'barring' attack that silences real warnings; eradication requires redesign of the warning architecture.
DIS-004	On the Effectiveness of Image Manipulation Detection in the Age of Social Media	VidalMata et al. IEEE Trans. Information Forensics & Security	2023	https://arxiv.org/abs/2304.09414	E3 - Strong analogue or observation	Peer-reviewed evaluation showing image-manipulation detectors trained on clean data frequently misread benign post-processing (re-compression, resizing) on real social-media imagery as tampering, exposing reliability gaps at internet scale.
DIS-005	Deepfake forensics: a survey of digital forensic methods for multimodal deepfake identification on social media	Qureshi, Saeed, Almotiri, Ahmad & Al Ghamdi. PeerJ Computer Science	2024	https://doi.org/10.7717/peerj-cs.2037	E3 - Strong analogue or observation	Peer-reviewed systematic survey of digital-forensic methods for detecting multimodal deepfakes (image, video, audio, text); catalogues datasets, evaluates established and emerging detectors, and flags cross-modality detection as an unsolved weakness.
DIS-006	From the Aether to the Ethernet - Attacking the Internet using Broadcast Digital Television	Oren & Keromytis USENIX Security / ACM TISSEC (Columbia Univ.)	2014	https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/oren	E1 - Direct evidence	Peer-reviewed demonstration of a low-cost RF man-in-the-middle ('red button') attack injecting attacker-controlled HTML into HbbTV broadcast streams, making TVs render unauthorised content/overlays; the injection is geographically localised and very hard to detect.
DIS-007	Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security	Chesney & Citron California Law Review 107	2019	https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-	E4 - Technically or socially plausible	Seminal law-review analysis of deepfakes' threats to privacy, democracy and national security; introduces the influential 'liar's dividend' (ubiquitous fakes let bad actors dismiss genuine evidence as fabricated) and surveys

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
				democracy-and-national-security		legal, regulatory and technological remedies.
DIS-008	Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media Threaten Core Democratic Functions	Pawelec, M. Digital Society (Springer)	2022	https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9453721/	E4 - Technically or socially plausible	Peer-reviewed application of democratic theory to deepfakes, analysing how synthetic audio-visual disinformation and hate speech threaten core democratic functions (legitimacy, trust and deliberation) and considering governance implications for platforms and regulators.
DIS-009	Audio Deepfake Detection Using Deep Learning	Shaaban& Yildirim. Engineering Reports (Wiley)	2025	https://onlinelibrary.wiley.com/doi/full/10.1002/eng2.70087	E3 - Strong analogue or observation	Wiley study presenting a deep-learning (Siamese CNN) model for detecting audio deepfakes; notes cheap voice-cloning tools needing seconds of speech enable phishing, fraudulent calls and impersonation that threaten trust and democratic processes.
DIS-010	One-Class Learning Towards Synthetic Voice Spoofing Detection	Zhang, Jiang & Duan. IEEE Signal Processing Letters	2021	https://arxiv.org/abs/2010.13995	E3 - Strong analogue or observation	Peer-reviewed one-class-learning detector that compacts genuine-speech representations to flag unseen text-to-speech and voice-conversion attacks, reaching 2.19% equal error rate on ASVspoof 2019 and outperforming prior single systems.
DIS-011	LLMs grooming or data voids? Chatbot references to Kremlin disinformation reflect information gaps	HKS Misinformation Review - Harvard Kennedy School	2025	https://misinforeview.hks.harvard.edu/article/llms-grooming-or-data-voids-llm-powered-chatbot-references-to-kremlin-disinformation-reflect-information-gaps-not-manipulation/	E3 - Strong analogue or observation	Peer-reviewed audit finding chatbots rarely cite Kremlin-linked Pravda sources (~8% of responses) and usually while debunking, arguing the pattern reflects 'data voids' on niche topics rather than systematic grooming.
DIS-012	The Liar's Dividend: Can Politicians Claim Misinformation to Evade Accountability?	Schiff, Schiff & Bueno. American Political Science Review (Purdue/Emory)	2024	https://doi.org/10.1017/S0003055423001454	E3 - Strong analogue or observation	First experimental evidence (five pre-registered studies, 15,000+ US adults) that politicians who falsely cry 'fake news'/'deepfake' after a genuine scandal gain support (more effectively than apologising or staying silent) quantifying the 'liar's dividend'.
DIS-013	Deepfakes as a Democratic Threat: Experimental Evidence Shows Noxious Effects That Are Reducible Through Journalistic Fact Checks	Dan, V. The International Journal of Press/Politics	2025	https://doi.org/10.1177/19401612251317766	E3 - Strong analogue or observation	Peer-reviewed experiment finding political deepfakes produce measurable harmful effects on viewers, but that journalistic fact-checking meaningfully reduces those effects - causal, intervention-focused evidence on mitigation.
DIS-014	The spread of true and false news online	Vosoughi, Roy & Aral . Science (MIT)	2018	https://doi.org/10.1126/science.aap9559	E2 - Actual case study or experiment	Landmark analysis of ~126,000 Twitter rumour cascades (2006–2017): falsehoods spread significantly farther, faster, deeper and more broadly than truth across every category, including terrorism and natural disasters, with novelty a key driver.
DIS-015	Mapping research on disinformation and misinformation across the Nordic countries: An integrative review	Grahn, Kalsnes, Isaksson, Mayerhöffer, Ólafsson, Falkheimer, Henriksen, Kristensen & Saari. Nordicom Review	2025	https://doi.org/10.2478/nor-2025-0015	E3 - Strong analogue or observation	Peer-reviewed integrative review of 359 studies (2014–2024) across Denmark, Finland, Iceland, Norway and Sweden, mapping five research clusters: security/Russia, media and fact-checking, health, media literacy, and social media, and where the evidence is thin.
DIS-016	Designing around NATO's deterrence: Russia's Nordic information confrontation strategy	Eggen, K.-A. Journal of Strategic Studies (Univ. of Oslo)	2024	https://doi.org/10.1080/01402390.2024.2332328	E2 - Actual case study or experiment	Peer-reviewed empirical study of Russia's information-confrontation activity toward Norway, Finland and Sweden in 2022–2023; finds Russia persists with sub-threshold tactics (disinformation, cyber and military signalling) aimed at sowing uncertainty, weakening Western cohesion and bypassing NATO deterrence.

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
DIS-017	Storying Strategies in Russian Information Warfare Against Sweden: The Post-Ukraine War Narratives	Lanevik, L. & Antai, I. Scandinavian Journal of Military Studies	2025	https://doi.org/10.31374/sjms.219	E2 - Actual case study or experiment	Peer-reviewed narrative analysis of Russian state media (RT) coverage of Sweden after its NATO application; identifies antagonistic 'plots' (including a newly named 'exploitation' strategy) portraying Sweden as unstable and responsible for regional insecurity.
DIS-018	How Persuasive Is AI-Generated Propaganda?	Goldstein, Chao, Grossman, Stamos & Tomz. PNAS Nexus (Stanford)	2024	https://doi.org/10.1093/pnasnexus/pgae034	E3 - Strong analogue or observation	Experiment finding AI-generated propaganda was nearly as persuasive as authentic foreign-propaganda articles, with light human curation/editing closing most of the remaining gap, evidence that models can produce persuasive influence content at scale.
DIS-019	The Persuasive Effects of Political Microtargeting in the Age of Generative Artificial Intelligence	Simchon, Edwards & Lewandowsky.PNAS Nexus	2024	https://doi.org/10.1093/pnasnexus/pgae035	E3 - Strong analogue or observation	Experiments showing AI-generated messages tailored to personality traits can be modestly more persuasive than untargeted ones.
DIS-020	LLM-Generated Messages Can Persuade Humans on Policy Issues	Bai, Voelkel, Muldowney, Eichstaedt & Willer (et al.) Nature Communications	2025	https://www.nature.com/articles/s41467-025-61345-5	E3 - Strong analogue or observation	Across three pre-registered experiments, LLM-generated messages measurably shifted participants' views across a range of policy issues, confirming current models can persuade at population scale on political topics.
DIS-021	Generative AI Generating Concerns: Citizens' Perspectives During the 2024 European Elections	Farooq, van den Hoogen, Tulin & de Vreese. The International Journal of Press/Politics	2025	https://doi.org/10.1177/19401612251376060	E2 - Actual case study or experiment	Survey during the 2024 European Parliament elections finding perceived exposure to AI-generated disinformation modestly eroded trust in the electoral process and satisfaction with democracy, while general perceived encounters with AI content did not.
DIS-022	ASVspoof 5: Crowdsourced Speech Data, Deepfakes and Adversarial Attacks at Scale	Wang, Delgado, Tak, Jung et al. arXiv, Speech Communication (Elsevier)	2024	https://arxiv.org/abs/2408.08739 (journal version: sciencedirect.com/science/article/pii/S0885230825000506, 2025)	E3 - Strong analogue or observation	Fifth ASVspoof challenge: a large crowdsourced corpus and 2024 evaluation across spoofing, deepfake and adversarial attacks (53 teams); reports state of the art synthetic speech has reached a quality where human listeners can no longer reliably distinguish it from genuine recordings.
DIS-023	Deepfakes in the 2025 Canadian Election: Prevalence, Partisanship, and Platform Dynamics	Livernoche, Musulan, Yang, Godbout & Rabbany. Mila / McGill / Univ. Montréal (arXiv)	2025	https://arxiv.org/abs/2512.13915	E2 - Actual case study or experiment	One of the first in-depth empirical analyses of how deepfakes actually appeared and circulated during a national election (Canada 2025): overall volume modest, but low-volume, high-credibility synthetic images posed disproportionate risk, and many flagged items were simple logo edits/overlays.
DIS-024	Hackers take over Russian radio/TV to transmit a fake Putin martial-law message	Bitdefender HotForSecurity	2023	https://www.bitdefender.com/en-us/blog/hotforsecurity/hackers-take-over-russian-radio-and-tv-station-to-transmit-fake-putin-martial-law-message	E2 - Actual case study or experiment	Analysis of the June 2023 hijacking of Russian radio and TV broadcasts that aired a deepfake of Putin declaring martial law and mobilisation after a fabricated incursion, fusing signal compromise with synthetic audio/video to push a false emergency address into border regions before control was regained.
DIS-025	Media Forensics (MediFor) Program	DARPA (US Defense Advanced Research Projects Agency)	2021	https://www.darpa.mil/research/programs/media-forensics	E4 - Technically or socially plausible	DARPA's program page describes the US effort to build automated tools assessing the integrity of images and video, framing the manipulation problem, the inadequacy of existing forensics, and goals for end-to-end detection and localisation.
DIS-026	Increasing Threats of Deepfake Identities	U.S. Department of Homeland Security (DHS)	2021	https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf	E3 - Strong analogue or observation	DHS primer on deepfake identities: explains how deepfakes are produced, distinguishes them from cheaper 'cheapfakes', and catalogues misuse across misinformation, fraud and impersonation .
DIS-027	LLM grooming and the 'Pravda' network: corrupting AI chatbots with propaganda	American Sunlight Project (Bulletin of the Atomic Scientists)	2025	https://thebulletin.org/2025/03/russian-networks-flood-the-internet-with-propaganda-aiming-	E3 - Strong analogue or observation	Research introducing 'LLM grooming': the Pravda network's mass publication of pro-Kremlin articles (millions yearly) across ~180 domains and dozens of languages, aimed not at human readers but at contaminating AI training data and

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
				to-corrupt-ai-chatbots/		chatbot outputs so models reproduce Russian narratives.
DIS-028	Pravda in the pipeline: Early evidence of state-adjacent propaganda in AI training data	DFRLab - Atlantic Council	2026	https://dfrlab.org/2026/04/08/pravda-in-the-pipeline/	E3 - Strong analogue or observation	DFRLab audit finding Pravda-network, RT and China-adjacent (Glassbridge) content already present on the public web archive feeding many open AI training pipelines, with one open-weights model reproducing such content near-verbatim.
DIS-029	AI chatbots reference Russian Pravda-network sources in Nordic languages (NORDIS investigation)	EDMO NORDIS (Faktabaari, TjekDet, Källkritikbyrån, Faktisk)	2025	https://www.nordishub.eu/nordis-investigation/	E2 - Actual case study or experiment	Investigation by four Nordic fact-checking organisations testing prompts in Finnish, Swedish, Danish and Norwegian; found popular chatbots linking to Pravda-network sites (EU-banned Russian propaganda sources) without warning, while often recognising common narratives.
DIS-030	Electronic and Cyber Operations Against Space Systems (the BabyTV satellite hijack)	Poirier, C. CSS Policy Perspectives, ETH Zürich	2025	https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP13-1_2025-EN.pdf	E2 - Actual case study or experiment	Documents the March–April 2024 BabyTV incident, where Disney's satellite children's channel (carried by Eutelsat) was overridden with Russian nationalist propaganda; clarifies it was uplink jamming (electronic attack, not a cyberattack) and urges broadcasters to update threat models during armed conflict.
DIS-031	Russia's Information Influence Operations in the Nordic–Baltic Region	NATO Strategic Communications Centre of Excellence (Riga)	2024	https://stratcomcoe.org/publications/russias-information-influence-operations-in-the-nordic-baltic-region/314	E2 - Actual case study or experiment	Examines Russian information influence across all eight Nordic-Baltic (NB8) states through case studies (2018–2023) set against each country's domestic context and the war in Ukraine; assesses why operations succeed or fail and the mitigations each state has adopted.
DIS-032	Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage (WP32)	Praks, H. - Hybrid CoE (Helsinki)	2024	https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-32-russias-hybrid-threat-tactics-against-the-baltic-sea-region-from-disinformation-to-sabotage/	E2 - Actual case study or experiment	Helsinki-based working paper detailing Russia's intensified hybrid activity against the Baltic Sea region (mid-2023 to April 2024) - disinformation, cyberattacks, instrumentalised migration and sabotage targeting Estonia, Finland, Latvia, Lithuania and Poland.
DIS-033	Death by a Thousand Paper Cuts: Lessons from the Nordic-Baltic Region on Countering Russian Gray Zone Aggression	Minna Ålander. Carnegie Endowment for International Peace	2024	https://carnegieendowment.org/research/2024/11/russia-gray-zone-aggression-baltic-nordic?lang=en	E2 - Actual case study or experiment	Analysis of how the Nordic-Baltic states, long-standing targets of Russian grey-zone aggression, have built differing (and unevenly successful) response models; documents how disinformation can escalate into real-world harm and argues for resilience and flexible response.
DIS-034	Signals from the North: What Nordic and Baltic Intelligence Assessments Reveal About Russia	International Centre for Defence and Security (ICDS, Tallinn)	2026	https://icds.ee/en/signals-from-the-north-what-nordic-and-baltic-intelligence-assessments-reveal-about-russia/	E3 - Strong analogue or observation	Synthesis of recent Nordic and Baltic intelligence assessments of Russia, finding hostile activity (cyber, disinformation, GPS jamming, covert influence) now framed as a continuous pattern of pressure, with growing official emphasis on societal resilience.
DIS-035	Image Control: How China struggles for discourse power	Drinhausen, Stec, Ohlberg & Karásková - MERICS	2023	https://merics.org/en/report/image-control-how-china-struggles-discourse-power	E3 - Strong analogue or observation	Report on China's pursuit of 'discourse power', shaping global narratives and reducing criticism by co-opting state officials, media and online influencers to 'tell China's story well', establishing the strategic logic behind Chinese influence increasingly extending into Europe.
DIS-036	Sino-Russian Convergence in Foreign Information Manipulation and Interference	Tamás Matura. Center for European Policy Analysis (CEPA)	2025	https://cepa.org/comprehensive-reports/sino-russian-convergence-in-foreign-information-manipulation-and-interference/	E3 - Strong analogue or observation	Report on the convergence of Russian and Chinese information manipulation (shared tactics (troll/bot networks, AI-generated content) and emerging coordination) noting China's framing of Europe as over-dependent on the US and Russia's seeding of disinformation into Western AI chatbots.
DIS-037	3rd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats	European External Action Service (EEAS)	2025	https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-	E2 - Actual case study or experiment	The EU diplomatic service maps the digital infrastructure behind foreign information manipulation - mainly Russia, also China - across 90 countries

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
				manipulation-and-interference-threats-0_en		in 2024; introduces the FIMI Exposure Matrix and documents covert networks (Doppelganger, Portal Kombat, False Façade) that impersonate legitimate media and launder propaganda.
DIS-038	4th EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats	European External Action Service (EEAS)	2026	https://www.eeas.europa.eu/eeas/4th-eeas-annual-report-foreign-information-manipulation-and-interference-threats_en	E2 - Actual case study or experiment	Latest annual EU FIMI threat report, building on the FIMI methodology and Response Framework and adding a 'FIMI Deterrence Playbook' to make influence operations costlier; supersedes the 3rd report (DIS-037) with updated incident data and a deterrence-focused framing.
DIS-039	Doppelganger: Media clones serving Russian propaganda	Alaphilippe, Machado, Miguel & Poldi - EU DisinfoLab (with Qurium)	2022	https://www.disinfo.eu/doppelganger/	E2 - Actual case study or experiment	The investigation that exposed 'Doppelganger', a Russia-based operation cloning at least 17 authentic media outlets (Bild, The Guardian, 20 Minutes, RBC Ukraine and others) via look-alike domains and copied designs to push fake articles, videos and polls.
DIS-040	FEMA warns Emergency Alert Systems could be hacked to transmit fake messages	CNN Politics (reporting on FEMA/FCC advisory)	2022	https://www.cnn.com/2022/08/03/politics/fema-emergency-alert-software-warning/index.html	E2 - Actual case study or experiment	FEMA and the FCC warned that unpatched Emergency Alert System encoder/decoder devices could be exploited to broadcast false alerts across TV, radio and cable; a security researcher demonstrated the flaw, prompting urgent advisories to patch software.
DIS-041	Deepfake-Eval-2024: A Multi-Modal In-the-Wild Benchmark of Deepfakes	Deepfake-Eval-2024 team, arXiv preprint	2025	https://arxiv.org/abs/2503.02857	E2 - Actual case study or experiment	In-the-wild benchmark (45 h video, 56.5 h audio, ~2,000 images across 88 sites and 52 languages) showing open-source state-of-the-art deepfake detectors collapse on real circulating fakes, AUC falling ~45-50% versus academic datasets.
DIS-042	FCC proposes new cybersecurity mandates for Emergency Alert System messages	The Desk (broadcast trade press), reporting FCC proposal	2026	https://thedesk.net/2026/06/fcc-proposes-changes-to-emergency-alert-system/	E2 - Actual case study or experiment	Trade-press coverage of the FCC's June 2026 proposal mandating stronger passwords, patching and firewalls for Emergency Alert System equipment, citing incidents where intruders accessed broadcast systems to transmit unauthorised messages, EAS tones, offensive content or promotional material.
DIS-043	Hacked in Translation - from Subtitles to Complete Takeover	Herscovici & Gull, Check Point Research (arXiv)	2024	https://arxiv.org/abs/2408.00502	E2 - Actual case study or experiment	Shows crafted subtitle/caption files, treated as trusted text by media players (VLC, Kodi, Popcorn-Time, Stremio) can compromise ~200 million installs, with attackers gaming repository ranking so malicious captions load automatically; the researchers found no evidence of in-the-wild use.
DIS-044	Deepfakes: A Grounded Threat Assessment	Hwang, T. CSET, Georgetown University	2020	https://cset.georgetown.edu/wp-content/uploads/CSET-Deepfakes-Report.pdf	E4 - Technically or socially plausible	Georgetown CSET 'grounded threat assessment' offering a framework for gauging deepfakes' real-world disinformation impact; reviews synthetic-media generation/detection and tempers hype with realistic expectations about commoditisation, detection countermeasures and adversary incentives.
DIS-045	A Survey of Threats Against Voice Authentication and Anti-Spoofing Systems	Survey (arXiv preprint)	2025	https://arxiv.org/abs/2508.16843	E3 - Strong analogue or observation	Survey of voice-cloning/spoofing threats to speaker-verification systems and the ASVspoof countermeasures; documents real financial-fraud cases (a 220k EURO CEO-impersonation transfer; a ~$35M bank heist combining synthetic voice and email spoofing).
DIS-046	Generative Language Models and Automated Influence Operations	Goldstein et al. Georgetown CSET / OpenAI / Stanford IO	2023	https://arxiv.org/abs/2301.04246	E4 - Technically or socially plausible	Foundational assessment of how generative language models could transform influence operations (lowering cost and scaling persuasive, hard-to-detect text) with a mitigation framework targeting model construction, access, content dissemination and belief formation.

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
DIS-047	Evaluating the Propensity of Generative AI for Producing Harmful Disinformation (2024 US Election)	Academic study (arXiv preprint)	2024	https://arxiv.org/abs/2411.06120	E3 - Strong analogue or observation	Academic study evaluating how readily generative-AI models produce harmful disinformation during the 2024 US election cycle, situating the risk alongside known operations (the IRA; China's Spamouflage) and offering developer-side mitigation recommendations.
DIS-048	Gauging the AI Threat to Free and Fair Elections	Brennan Center for Justice, NYU School of Law	2025	https://www.brennancenter.org/our-work/analysis-opinion/gauging-ai-threat-free-and-fair-elections	E3 - Strong analogue or observation	Brennan Center analysis of AI threats to US elections: finds worst-case 2024 disruption did not materialise, yet documents real deepfake incidents (e.g., the AI Biden robocall and viral foreign cases) that erode trust and deepen polarisation over time.
DIS-049	AI-Enabled Influence Operations: Safeguarding Future Elections	CETaS - The Alan Turing Institute	2024	https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-safeguarding-future-elections	E3 - Strong analogue or observation	CETaS (Alan Turing Institute) report on AI-enhanced influence operations in the 2024 US election and beyond: finds no conclusive evidence AI altered results, but shows deceptive AI content shaped discourse and entrenched polarisation; recommends digital literacy and a more resilient information ecosystem.
DIS-050	Global Risks Report 2024	World Economic Forum (WEF)	2024	https://www.weforum.org/publications/global-risks-report-2024/digest/	E4 - Technically or socially plausible	The WEF's flagship report ranks AI-amplified mis/disinformation as the most severe short-term global risk, linking synthetic content to election destabilisation, polarisation and unrest across a major global election year.
DIS-051	We Looked at 78 Election Deepfakes. Political Misinformation Is Not an AI Problem.	Knight First Amendment Institute, Columbia University	2024	https://knightcolumbia.org/blog/we-looked-at-78-election-deepfakes-political-misinformation-is-not-an-ai-problem	E2 - Actual case study or experiment	Essay analysing 78 election deepfakes, arguing political misinformation is not primarily an AI problem (cheap fakes outnumbered AI content roughly seven to one in the 2024 US election) and that feared AI impacts largely failed to materialise globally.
DIS-052	How Coordinated Inauthentic Behavior continues on Social Platforms	Stanford Internet Observatory / FSI, Stanford University	2024	https://cyber.fsi.stanford.edu/news/how-coordinated-inauthentic-behavior-continues-social-platforms	E2 - Actual case study or experiment	Stanford analysis of coordinated inauthentic behaviour, examining Meta's takedowns of Russian, Chinese and Iranian networks and the persistent 'Doppelganger' operation that mimics legitimate news outlets across platforms; documents platform-manipulation tactics and the enforcement challenge.
DIS-053	Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation	Bradshaw, Bailey & Howard. Oxford Internet Institute	2021	https://www.oii.ox.ac.uk/news-events/reports/industrialized-disinformation-2020-global-inventory-of-organized-social-media-manipulation/	E2 - Actual case study or experiment	Annual global inventory finding organised social-media manipulation ('cyber troops') in 81 countries, with a marked rise in private firms running influence campaigns for hire using bots, micro-targeting and sock-puppet accounts.
DIS-054	The EU's Role in Fighting Disinformation: Crafting a Disinformation Framework (ABCDE)	Pamment, J. Carnegie / PCIO (Lund University)	2020	https://carnegieendowment.org/research/2020/09/the-eus-role-in-fighting-disinformation-crafting-a-disinformation-framework?lang=en	E4 - Technically or socially plausible	Introduces the widely adopted ABCDE framework (Actors, Behaviour, Content, Degree, Effect) for analysing influence operations, supplying shared terminology and a structuring lens for classifying state-actor cases and organising institutional responses; commissioned by the EEAS, authored by Lund University's James Pamment.
DIS-055	The Breakout Scale: Measuring the Impact of Influence Operations	Nimmo, B. - Brookings Institution	2020	https://www.brookings.edu/articles/the-breakout-scale-measuring-the-impact-of-influence-operations/	E4 - Technically or socially plausible	A six-category scale for rating the impact of an influence operation from observable spread data - from confinement to a single platform/community (Cat 1) up to triggering a policy response or calls to violence (Cat 6) - without needing to measure audience behaviour change; now used operationally by Meta and OpenAI to triage takedowns.
DIS-056	DISARM Framework: A Common Taxonomy of Disinformation TTPs (Red/Blue)	DISARM Foundation (Terp & Breuer) - evolved from AMITT	2022	https://github.com/DISARMFoundation/DISARMframeworks	E4 - Technically or socially plausible	An open, MITRE ATT&CK-style taxonomy of the tactics, techniques and procedures used to conduct (Red) and counter (Blue) influence operations; the de-facto

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
						common language for FIMI analysis and the framework underpinning the EEAS FIMI threat reports.
DIS-057	Phase-based Tactical Analysis of Online Operations (Online Operations Kill Chain)	Nimmo, B. & Hutchins, E. - Carnegie Endowment for International Peace	2023	https://carnegieendowment.org/research/2023/03/phase-based-tactical-analysis-of-online-operations	E4 - Technically or socially plausible	Adapts the cybersecurity 'kill chain' to influence operations, breaking a campaign into ten sequential phases (from asset acquisition to persistence) so analysts can identify the earliest point at which an operation can be detected and disrupted.
DIS-058	AI Risk Management Framework (AI RMF 1.0) & Generative AI Profile (NIST AI 600-1)	National Institute of Standards and Technology (NIST)	2024	https://doi.org/10.6028/NIST.AI.600-1	E4 - Technically or socially plausible	The US standard for AI risk management (GOVERN-MAP-MEASURE-MANAGE); the Generative AI Profile enumerates twelve GenAI risk categories that explicitly include disinformation, deepfakes/synthetic audio-visual content and data poisoning, with suggested governance and measurement actions.
DIS-059	Tactics, Threats & Targets: Modeling Disinformation and Its Mitigation	Mirza, Begum, Niu, Pardo, Abouzied, Papotti & Pöpper - NDSS (NYU)	2023	https://doi.org/10.14722/ndss.2023.23657	E4 - Technically or socially plausible	Peer-reviewed framework (built from interviews with fact-checkers and analysts) modelling disinformation along actors, attack patterns, channels and targets, with a mapped set of mitigations.
DIS-060	Iranian hacking group carries out cyber operations against 2 Swedish companies	Iranian Cyber News Agency (ICNA)	2025	https://irancybernews.org/en/iranian-hacking-group-carries-out-cyber-operations-against-2-swedish-companies/	E2 - Actual case study or experiment	ICNA, citing reporting by Swedish newspaper *Dagens Nyheter*, states that the Iran-linked threat actor Nimbus Manticore exploited two Swedish software companies and their commercial infrastructure during spring 2025 to support covert cyber operations in Europe.
DIS-061	Russian satellite TV shows a Ukraine message: 'Blood on your hands'	The Straits Times / Reuters	2022	https://www.straitstimes.com/world/europe/russian-satellite-tv-shows-a-ukraine-message-blood-on-your-hands	E2 - Actual case study or experiment	Reuters report, republished by The Straits Times, describing how Russian satellite television menus in Moscow were altered on Victory Day to display anti-war messages about the war in Ukraine; Interfax reportedly said similar slogans appeared on cable television after hacking.
DIS-062	New digital safety and regulation law	European Audiovisual Observatory / IRIS Merlin; Amélie Blocman, Légipresse	2024	https://merlin.obs.coe.int/article/10083	E4 - Technically or socially plausible	IRIS Merlin summary of France's Law No. 2024-449.
DIS-063	NATO's approach to counter information threats	NATO	2025	https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats	E4 - Technically or socially plausible	NATO topic page describing the Alliance's approach to countering information threats, including foreign information manipulation and interference, disinformation, and other coordinated manipulative activity.
DIS-064	Foreign power influence campaign carried out through breach of data security	Swedish Security Service (Säkerhetspolisen)	2024	https://sakerhetspolisen.se/ovriga-sidor/other-languages/english-engelska/press-room/news/news/2024-09-25-foreign-power-influence-campaign-carried-out-through-breach-of-data-security.html	E2 - Actual case study or experiment	The Swedish Security Service attributes a 2023 cyber-enabled influence campaign to an Iranian cyber group acting on assignment from the Iranian Revolutionary Guards.
DIS-065	Russian TV Channel Availability Across IPTV Access Contexts, 24–28 August 2026	Nordic Content Protection	2026	Internal evidence package supplied to the authors	E1 – Direct evidence	NCP-supplied technical testing directly observed Russian and RT-branded television streams across multiple IPTV access contexts during 24–28 August 2026. Screenshot-backed observations were recorded across all five tested access IDs, including Rossiya 1, Channel One and multiple RT variants. The finding provides direct evidence that Russian-origin and RT-branded audiovisual content was present within the tested IPTV distribution environments.

Ref #	Source Title	Author / Org	Year	URL / DOI	Evidence Level	Summary
DIS-066	EU sanctions applied: 36 IP addresses and 621 websites carrying prohibited Russian propaganda content blocked	Radio and Television Commission of Lithuania (LRTK)	2024	https://madeinvilnius.lt/en/news/Lithuanian-news/lrtk-blocked-621-a-website/	E2 – Actual case study or experiment	Lithuanian regulatory monitoring identified sanctioned Russian television programmes, including Pervyi Kanal, Rossiya 1, NTV and RTR Planeta, across 621 websites and 36 IPTV IP addresses. This provides direct official evidence that Russian television content continued to be distributed through online and IPTV infrastructure despite EU restrictions. It independently corroborates the distribution pathway observed in DIS-065.
DIS-067	Media Policy Guidelines of Latvia 2024–2027	Cabinet of Ministers of Latvia / Ministry of Culture	2024	https://likumi.lv/ta/en/en/id/355321	E3 – Strong analogue or observation	Latvian Government policy identifies illegal television consumption and distribution as an information-space and media-security issue and establishes explicit policy objectives to reduce illegal television consumption. The Guidelines place these issues within the post-2022 security environment and the protection of Latvia's information space.
DIS-068	EU sanctions against Russia: questions and answers	Council of the European Union	2026	https://www.consilium.europa.eu/en/policies/sanctions-against-russia-explained/	E3 – Strong analogue or observation	The Council identifies Kremlin-backed media as instruments of systematic disinformation and information manipulation and lists suspended outlets including Russia Today, Pervyi Kanal, Rossiya 1, Rossiya 24, NTV and RTR Planeta. This establishes the policy and security significance of several of the same Russian television brands observed within the IPTV environments in DIS-065 and DIS-066.

Researcher Biographies

Professor Watters is a trusted cybersecurity researcher and thought leader at Cyberstronomy Pty Ltd. He is the author of *Counterintelligence in a Cyber World* (Springer - ISBN 978-3031352867) and *Cybercrime and Cybersecurity* (CRC Press - ISBN 978-1032524511). Professor Watters is Honorary Professor of Security Studies and Criminology at Macquarie University, and Professor of Information Systems at Holmesglen Institute. His work has been cited 12,590 times, with an *h*-index of 51, and an *i*-10 index of 155. He was ranked within the top 0.5% of researchers worldwide (all fields) by ScholarGPS in 2024. Professor Watters was awarded the Order of Australia Medal in 2026 for service to tertiary education.

Associate Professor Joel Scanlan at the Western Norway University of Applied Sciences (HVL) in Haugesund, Norway, where his research is focused on cybersecurity in the context of critical infrastructure. He co-authored the definitive study Consumer Risk from Piracy in the Nordic Countries. He is also the academic co-lead of the CSAM Deterrence Centre (University of Tasmania, Australia), and a visiting Associate Professor at the International Policing and Public Protection Research Institute (IPPPRI) (Anglia Ruskin University, United Kingdom). His primary research is focused on preventing online child exploitation and involves developing automated responses on mainstream platforms (chatbots and warning messages) and dark web observational and intervention research. His broader foundational research leverages data mining and machine learning to address technical harms on the internet, digital tracking, and user data privacy risks.

Acknowledgements

Funding for this research was provided by Nordic Content Protection. The work was produced independently by Professor Watters (Macquarie University) and Associate Professor Scanlan (Western Norway University of Applied Sciences).