

Nordic Content Protection

Trend Report 2017

Illegal distribution and sales of access to television broadcasts



This trend report is a collaboration between the analysis and consulting company Procope AS, and Nordic Content Protection. Oslo, Norway – January 2017.

PRO/COPE

TABLE OF CONTENTS

Executive summary.....	4
About Nordic Content Protection.....	5
About this trend report.....	5
Methodology	6
Threat landscape	6
Nordic youth use of piracy services.....	7
Earning potential and illegal revenue	8
Earning potential for legal distributors.....	8
The illegal revenue	8
Earning potential and illegal revenue – by country	10
Sweden.....	10
Norway	10
Denmark.....	11
Finland	11
Criminal networks.....	12
Illegal business models and operations.....	13
Where do the illegal proceeds go?	14
Marketplaces for illegal subscriptions.....	15
Technologies employed by illegal networks.....	16
Card sharing	17
IPTV	17
Streaming	18

EXECUTIVE SUMMARY

In this year's Trend Report 2017, Nordic Content Protection (NCP), has chosen to focus on the economy associated with the illegal distribution of television broadcasts. Estimates outlined in the report indicate, that illegal parallel distribution networks in the Nordic region¹ represent an earning potential of approximately **531.6 million Euros to the legal distributors**. This figure is based on 400,000 illegal subscriptions. The biggest loss is inflicted upon Sweden, followed by Denmark, Norway, and Finland.

The large criminal networks operate in the same way as legitimate international companies. Illegal distribution is highly lucrative, and carries a low risk of detection, and prosecution. The annual turnover for illegal distributors in the Nordic countries is an estimated 77.9 million Euros. There are indeed indications, that a portion of these illegal proceeds, are being used to finance other criminal activities – ultimately terrorism.

A recent EU survey (EUIPO²), shows that **25% of youths aged between 15–24, deliberately download illegal content off the Internet³**. Nordic figures (not counting Norway), are higher – which indicates that a relatively large proportion of the youth population, does not consider it to be a serious offence to unlawfully acquire content from copyright owners of movies, games, television broadcasts etc. This attitude makes it highly likely, that many of today's youths will have little or no misgivings about choosing illegal television solutions in the foreseeable future.

Card Sharing (CS), is still the leading platform for illegal distribution of television broadcasts. There are indications that CS has stopped growing, but it has stabilized at a high level.

The number of illegal providers of Internet Protocol Television (IPTV), is however on the rise. In 2016, Nordic Content Protection (NCP) has uncovered more than 150 web pages, which illegally offer Nordic channel packages via IPTV, and streaming.

Another platform that is expanding in line with user patterns, bandwidth, availability, and quality, is streaming via web services. Identifying the licensees, and persuading the distributors of illegal streams to comply with our requests, currently poses considerable challenges.

Police IPR-units (Intellectual Property Rights) in Sweden and Denmark; have in recent years made substantial contributions in a number of court cases with positive results. Norway and Finland have yet to establish such police units, and as a result, most of the investigative work is left to the industry itself. Consequently, this form of crime has flourished due to the low risk of prosecution.

¹ Except Iceland, which does not have any rights owners registered with NCP as of 2016.

² EUIPO stands for European Union Intellectual Property Office.

³ Norway was not part of the survey, but NCP has assigned Norway the EU country average. This is lower than both Sweden, and Denmark.

ABOUT NCP

Nordic Content Protection (NCP) is working hard to prevent illegal access to television broadcasts received via satellite dish, digital terrestrial transmissions, IPTV, cable transmissions, and streaming.

NCP is jointly working with the following Nordic distributors, and rights owners as of January, 2017:



NCP is also collaborating with distributors to develop security solutions aimed at detecting, and preventing illegal distribution. NCP has a number of additional tasks related to training, and competence transfer, both nationally, and internationally. Current collaborators in these areas include police IPR-units in Sweden and Denmark, (Intellectual Property Rights), Europol (in advanced computer forensics), the EU, through EUIPO, (European Union Intellectual Property Office), and TAIEX⁴ workshop, (Technical Assistance and Information Exchange).

Further information about this work can be found at: www.ncprotection.com

ABOUT THIS TREND REPORT

This is the second trend report compiled for NCP. The report aims to shed light on a relatively unknown form of criminal activity. The level of knowledge, and proficiency in this area within law enforcement, prosecuting authorities, and society in general, is relatively low. The report additionally forms the basis for prioritizing Nordic Content Protection's future efforts, thus maximizing the beneficial effects of the preventive, and combative measures that are subsequently outlined.

This report specifically deals with the Nordic market. Even though the methods, and technologies employed remain the same, there are both national, and regional differences in terms of application. This is especially true when it comes to operators, and scope. Sweden stands out from the rest, with both more numerous, and larger criminal networks. This is primarily a result of demographics combined with socio-economic factors, but culture and availability also come into play.

Legislation and legal practices vary in the Nordic countries, as will be explained in brief, in this report. More in-depth information can be found at: www.ncprotection.com

⁴ I TAIEX is a collaboration with Turkey, the former Yugoslav Republic of Macedonia; Montenegro, Serbia, Albania, Bosnia and Herzegovina and Kosovo*; Turkish Cypriot community in the northern part of Cyprus; Algeria, Armenia, Azerbaijan, Belarus, Egypt, Georgia, Israel, Jordan, Lebanon, Libya, Moldova, Morocco, Palestine, Syria, Tunisia, and Ukraine.

METHODOLOGY

The trend report is based chiefly on a qualitative method. It deals with a specialized discipline in which the expertise mainly resides with the Nordic Content Protection organization. This has necessitated dialogue, and a number of meetings with national representatives. Each one of these representatives has a network consisting of national players, business partners, and sources inside the criminal networks. Additional sources of information include; reviews of relevant court rulings, published reports and other open sources.

THREAT LANDSCAPE

The largest threat to the Television industry as a whole, is the fact that parallel illegal distributors, directly compete with legal providers, by offering lower-priced illegal products.

The criminal networks offer “all-in-one” solutions, where subscribers can gain access to a large variety of channels at a mere fraction of the cost of a legal subscription, either by connecting an illegal STB⁵ or by streaming content directly to their television sets.

Today’s criminal networks are international, professionally organized, and offer a wide range of channels to customers in numerous countries. They are highly versed with regards to international legislation governing audits, and the exchange of information across national borders. NCP has ascertained that the majority of illegal providers have

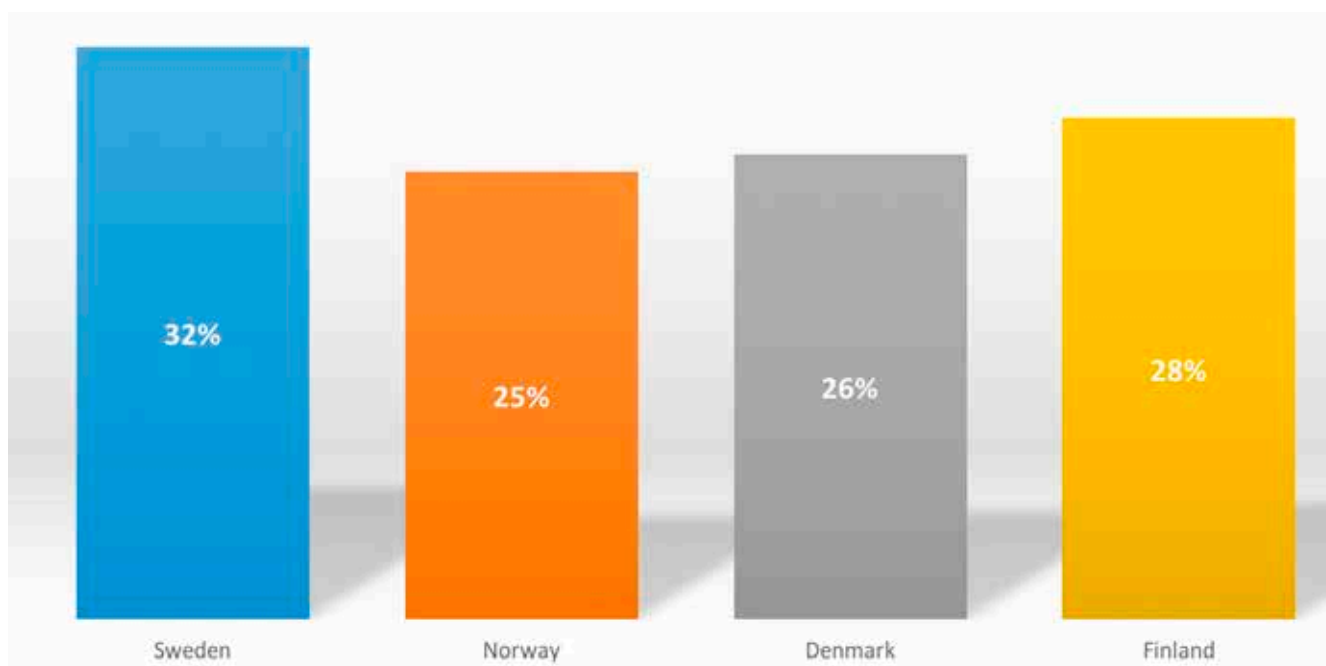


Chart 1. Youths aged between 15–24 that deliberately download illegal content – percentage by country⁶.

⁵ A set-top box (STB) or set-top unit (STU) (one type also colloquially known as a cable box) is an information appliance device that generally contains a TV-tuner input and displays output to a television set and an external source of signal, turning the source signal into content in a form that can then be displayed on the television screen or other display device. They are used in cable television, satellite television, and over-the-air television systems, as well as other uses.

⁶ Norway is not included in the report, but the EU average (25%) has been assigned to Norway by NCP.

moved their servers to hosting companies located outside the jurisdiction of the Nordic countries, thus making it more difficult for national authorities to investigate them. This is highly unfortunate, as it allows the criminal activity to persist, and to expand.

“The fight against illegal international networks calls for police collaboration across all borders.”

Nordic youth use of piracy services

The report “Intellectual Property and Youth”, compiled by EUIPO (European Union Intellectual Property Office), and published in April of 2016, shows that 25% of all European youths aged between 15–24, download illegal content off the Internet⁷. The material is divided up and sorted by country, type of content (movies, sports, music, games), incentives for choosing illicit sources, and reasons for ceasing to use these sources etc.

The content downloaded from illegal sources is primarily movies and TV series (85%), music (56%), and games (29%). The main incentives are pricing (68%), personal use (38%), and user friendliness combined with quick access (33%).

National figures, age group between 15–24⁸:

Sweden	377,254 people (out of 1,178,920 in total)
Norway	167,415 people (out of 669,658 in total)
Denmark	191,805 people (out of 737,713 in total)
Finland	179,308 people (out of 640,387 in total)

This equates to **915,782 people** aged between 15–24, who deliberately download illegal content off the Internet. A relevant question is whether or not this group is at risk of becoming future customers for illegal television broadcasts?



⁷ Source: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/IP_youth_scoreboard_study/IP_youth_scoreboard_study_en.pdf

⁸ Statistics sourced from www.norden.org and updated in the database, on the 1st January, 2016.

EARNING POTENTIAL AND ILLEGAL REVENUE

Earning potential for legal distributors

Assigning an exact number to the financial damage currently being inflicted upon legal distributors by criminal operators in the Nordic countries, is no easy task. If all the estimated illegal subscribers were to buy legal subscriptions it would result in an estimated annual earning potential of **531.6 million Euros**.

This figure presupposes that illegal subscribers would instead purchase a mandatory basic package, along with a minimum of the most popular premium channel packages. The prices and structures of these packages vary from country to country. NCP appreciates the fact that the buyers of illegal subscriptions are not a homogenous group, but as complex and diversified as the general population.

The basis for the figures shown below, is described under each individual country in the report.

The illegal revenue

The criminal networks annually take in **77.9 million Euros**. Sweden tops the revenue list, followed by Denmark with Norway, and Finland sharing third place.

NCP estimates the number of illegal subscribers in the Nordic countries as follows:

250,000	in Sweden
50,000	in Norway
50,000	in Denmark
50,000	in Finland

These figures are based on source information, experience, previous and ongoing criminal court cases, ref. Trend Report – 2016 (source: www.ncprotection.com).



Chart 2. Lost earning potential for distributors by country, in Euros⁹, and in local currency.

⁹ Exchange rates as of 07.12.2016.

The illegal providers operate with various price models, and payment solutions. A review of an assorted selection of illegal providers reveals an average subscription cost of approximately 16.6 Euros per month. Based on this, we can calculate the following chart:



Chart 3. An estimate of the total illegal revenue by country, (in million Euros).

EARNING POTENTIAL AND ILLEGAL REVENUE – BY COUNTRY

Sweden

NCP's mapping and analysis, shows that by Scandinavian and European standards, Sweden has a very high number of illegal providers and subscribers, when it comes to CS and IPTV. The number of subscribers is estimated to be approximately 250,000. In Sweden, the price for a channel package consisting of a basic package, and a selection of the most popular movies, sports and television series, is as follows:

Basic package	189 SEK (Canal Digital – Basic package 20 channels)
Sport (international football)	399 SEK (Viaplay Sport – Premier League + series)
Sport (Swedish football, hockey)	399 SEK (C More)
TV series	99 SEK (C More Series)
Total per month	1086 SEK (111 Euro)

The annual earning potential lost by Swedish distributors is a staggering **3258 million SEK (330 million Euros)**. Based on 250,000 subscribers x 1086 SEK x 12 months.

The illegal providers charge 150 SEK per month for their illegal channel packages. These bundles offer a wide array of channels, and the basic package plus sports, movies, and television series are always included. The illegal revenue in Sweden consequently amounts to:

250,000 subscribers x 150 SEK x 12 months =
450 million SEK (46 million Euros).

Norway

NCP estimates that approximately 50,000 people are currently subscribing to illegal channel packages. The price for the smallest premium package in Norway, which includes sports, movies and television series, is somewhat higher than in the other Nordic countries:

Basic package	439 NOK (basic package)
Sports	449 NOK (TV2 premium – Premier League /Norwegian football)
TV series	99 NOK (C More)
Sport/film	399 NOK (Viaplay – Spanish league/hockey/movies)
Total per month	1386 NOK (154 Euro)

The annual earning potential lost by Norwegian distributors is **831.6 million NOK (92.1 million Euros)**. Based on 50,000 subscribers x 1386 NOK x 12 months.

The annual illegal revenue in Norway is an estimated **90 million NOK (9.9 million Euros)**.

Based on 50,000 subscribers x 150 NOK x 12 months.

Denmark

NCP's analyses indicate that 50,000 people in Denmark subscribe to illegal channel packages. The price for the minimum bouquet premium channels is as follows:

Basic package	399 DKK (Canal Digital – local)
Sports	299 DKK (Viaplay – Premier league)
TV series	99 DKK (C More)
Total per month	797 DKK (107 Euro)

The annual earning potential lost by Danish distributors is **478.2 million DKK (64.3 million Euros)**. Based on 50,000 subscribers x 797 DKK x 12 months.

The annual illegal revenue figure in Denmark is **90 million DKK (12.1 million Euros)**. Based on 50,000 subscribers x 150 DKK x 12 months.

Finland

NCP is partially active in Finland, thus the overall analysis is somewhat deficient, compared with the statistics researched for the remaining Scandinavian countries. However, based on our professional experience from previous years, it is estimated that Finland also has approximately 50,000 illegal subscribers. It should be noted; that there is some degree of uncertainty tied to this estimate.

Using this as our starting point, the price for the smallest legal premium package is as follows:

Basic package	34.90 Euros (family package, movies /TV series)
Sports	34.95 Euros (Viasat Sport – football/hockey)
Total per month	69.85 Euros

The annual earning potential lost by Finish distributors is **41.9 million Euros**. Based on 50,000 subscribers x 69.85 Euros x 12 months.

The annual illegal revenue in Finland is estimated to be the same as in Norway and Denmark, approximately **9.9 million Euros**. Based on 50,000 subscribers x 16.6 Euros x 12 months.

Criminal networks

The networks that are currently active in this crime field, bear many similarities to other operators in the areas of financial, and organized crime. The players, scope, logistics, size, and economics all coincide. Some organized criminal networks have deemed it beneficial to migrate over from other more serious types of criminal activity. This is due to very favourable costs, and return ratios, and notably the low risk of being caught, and relatively low penalties for infringements.

Subscriptions are paid either in cash, by bank account transfers, (PayPal or other online payment solutions), or the use of digital currencies such as Bitcoin¹⁰.

Cash payments usually take place on a monthly, quarterly, biannual, or annual basis. This makes it easier to manage the logistics, and follow-up work. The money usually changes hands in person, or by the customer dropping it off at a designated point, e.g. a mailbox.

All criminal networks maintain bookkeeping ledgers, which record customer details, and accounting information etc. Subscription lengths normally correspond with payment frequency, the most common being quarterly, or biannual.



¹⁰ Bitcoin is a cryptocurrency and a payment system offering enhanced anonymity for user. The use of bitcoin by criminals has attracted the attention of financial regulators, legislative bodies, law enforcement, and media. Criminal activities are primarily focused on darknet markets and theft, though officials in countries such as the United States also recognize that bitcoin can provide legitimate financial services.

Illegal business models and operations

These networks are run very much in the same manner as a legitimate business. They have a clear and defined structure, with designated personnel in charge of sales, finances, and technology. They have access to individuals who possess an abundance of technological know-how, and they have high capacity servers and bandwidth at their disposal.

Some of the larger criminal networks operate behind a legitimate façade, quite often a retail store selling decoding devices, and other related merchandise. Other networks are clandestine operations, where contact takes place solely via other customers. The illegal revenue made by these networks, is very substantial. Some networks may have upwards of 5,000 customers.

The following IPTV case from 2016, illustrates how this type of network operates:

In the first quarter of 2016, Nordic Content Protection in Norway, uncovered the main player in charge of operating a large illegal IPTV network. This was the result of a lengthy investigation, which involved gathering information from a number of different sources.

This individual had all the Norwegian channel packages, e.g. Canal Digital, Viasat, TV2 etc., on offer. The enterprise had undergone rapid expansion, with more than 2000 customers. A significant amount of these customers were either Spanish residents, or owned vacation homes/apartments in Spain. The annual subscription fee was up to 140 Euros, and each customer had the option to buy an STB for an additional 1000 NOK.

The main player ran the operation from his own home base in a large Norwegian city. It also turned out that he was an IT educated family man in his 30s who held a regular job. To the unsuspecting onlooker, he appeared to be a successful businessman with solid finances. His operation was highly professional, with salesmen in other Nordic countries working on a commission rate of around 15%. The IPTV server was connected to a web hotel in France (OVH SAS). All customer contact was conducted via SKYPE, while payments were made via PayPal.

...This particular case is still open.

WHERE DO THE ILLEGAL PROCEEDS GO?

NCP over a period of years, has identified and documented a large number of criminal operators in this type of business, who have spent substantial amounts of money on personal consumption, expensive cars, and other luxury items. However in recent years, we have observed a distinct pattern change in criminal behaviour. Several ongoing investigations have uncovered illegal proceeds being transferred to foreign bank accounts in areas of conflict.

Our extensive research has also uncovered, that criminal operators are investing vast sums of money in real estate, and in legitimate companies in the Nordic region, as well as the rest of the world. Some operators are also known from other types of criminal activity. They distribute the proceeds, and reinvest them in the illegal, (black) economy.

A recently published report by the US joint strategic plan on intellectual property enforcement 2017–2019, “*Supporting innovation creativity & enterprise*”, concludes that there are close ties between criminals who steal, and distribute digital rights, and terror financing.

The following extract has been taken from page 42:

Quote:

“The link between organized crime groups, and counterfeit goods is well established. But INTERPOL is sounding the alarm that Intellectual Property Crime is becoming the preferred method of funding for a number of terrorist groups.

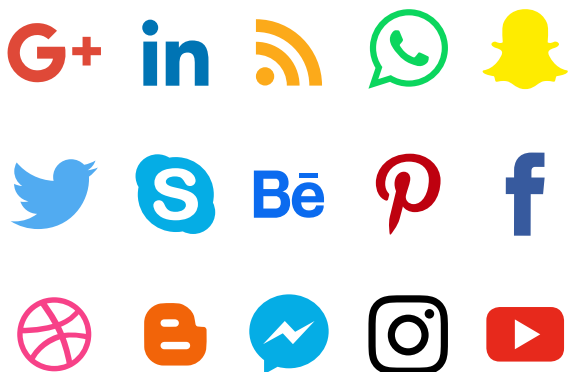
There are enough examples now of the funding of terrorist groups in this way for us to worry about the threat to public safety. We must take preventative measures now.”

– Former Secretary General, INTERPOL, Hon. Ronald K. Noble

MARKETPLACES FOR ILLEGAL SUBSCRIPTIONS

The illegal providers advertise their products on all available platforms including hidden ones like the Darknet¹¹.

Social networks, friends, colleagues, families etc. also constitute considerable arenas for sales and distribution.



designed by freepik.com

The largest and most popular platforms on social media are, Skype and Facebook. They are suited for the conducting of sales, information forwarding, and support services. Another channel is REDDIT¹², where users evaluate and discuss quality of service, availability, security, prices etc.

We have seen in our work that those who advertise on the Open Internet also advertise on the DarkNet. Most recently the Darknet is becoming a platform that markets and offers the purchase of illegal subscriptions to Nordic television packages.



¹¹ Darknet is a alternative network that is purposely hidden from search engines and normal Internet users. Access to Dark Nets is achieved through use of specific software and the network benefits are the ability for users and service providers to remain semi-anonymous. "TOR", ("The Onion Router") as an example, accomplishes this by routing your request in encrypted form through several network nodes. This creates the perfect environment for free speech, discovering information, and anonymously conducting illegal business. The technology itself is legal. Darknet is also used as an arena for marketing, and sales by the international illegal distributors. Payment is made by Bitcoin. IPTV access and transmission, is however done over the open Internet.

¹² Reddit is a social news aggregation, web content rating, and discussion website.

TECHNOLOGIES EMPLOYED BY ILLEGAL NETWORKS

These are the current threats, ranked in prioritized order in terms of scope and prevalence:

- 1. Card sharing
- 2. IPTV
- 3. Streaming

(An additional description and illustration of the various technological methods, is found in the attachment).

Card sharing networks remain the biggest threat to the industry in terms of prevalence and financial damage. However, illegal IPTV is expected to overtake card sharing as the number one threat within a few years. This will happen as soon as the necessary technical equipment becomes an affordable investment for the smaller criminal networks. Additional contributing factors are technologies impeding illegal distribution through encryption, and other security solutions.

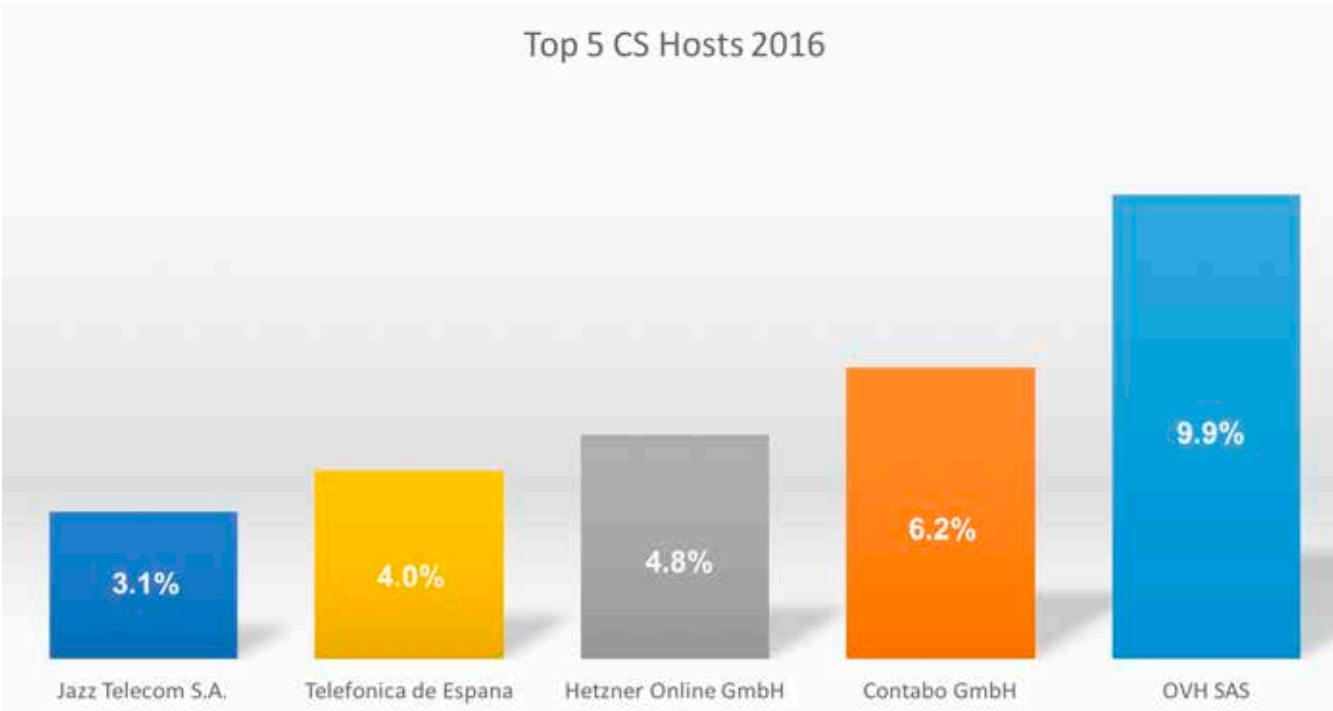


Chart 4. The most used web hotels (hosts) for card sharing in the Nordic countries in 2016.

Card sharing

Card sharing (CS), involves several people sharing one or more official subscription cards over the Internet, in a “card sharing” network. The network consists of several interconnected CS servers distributing television content, and a number of CS clients receiving television signals.

In terms of practical application, only the control codes, (a small amount of specific data), is being shared in this network – not the actual television broadcasts. They are decrypted, and forwarded via a server to the client-end, whenever the customer selects a TV-channel.

Most of the CS servers remain on hosting companies located outside of the Nordic region.

NCP has contacted the three largest providers in the above chart (OVH SAS, Contabo GmbH, and Hetzner Online GmbH), to inform them that we have gathered information from open sources and police investigations in the Nordics, that their services are being used for illegal purposes as card sharing and illegal IPTV. NCP gave the providers opportunity to comment and respond to the statement. They all decided to abstain.

IPTV

IPTV is short for Internet Protocol Television. Broadcasts are digital, and available on a variety of platforms, e.g. smart tablets, STB, smart TV's, mobile/smart phones etc.

The illegal servers are almost without exception, hosted with companies based outside the jurisdiction of the Nordic countries. User-friendliness, quality of service, and reliability, are essentially running and providing the same level of service, as the legal providers themselves are able to deliver. A typical “illegal” subscription provides the customer access up to 4,000 channels. In addition, they are able to provide new services to their client base, such as access to “Video On Demand”(VOD), and music catalogs as part of their subscription entitlement.

The number of criminal operators offering illegal IPTV in the Nordic countries is on the rise. This trend is expected to continue at an accelerated rate in the coming years, and IPTV will likely rival CS as the market's leading platform in the foreseeable future.

In 2016, NCP has uncovered more than **150 web pages** that illegally sell Nordic channel packages on IPTV, and streams. The true scope of this illegal activity is suspected to be substantially larger, and is expected to persist in its expansion.

In order to arrest this negative development, NCP has invested in new tools, and adopted sophisticated methods that will be implemented in 2017.

Streaming

Streaming via websites; is when audio and video combined, is broadcast over a computer network in a way that allows the end user to access the content in “real-time”, without having to wait for the entire file to download. Simply put, this means that you can visit a website, and watch TV-series, movies, entertainment programs, and live sports broadcasts. The stream becomes illegal when one distributes broadcasts without owning the legal rights to do so. This type of copyright infringement, together with illegal IPTV and CS inflicts a sizable revenue loss upon the rights owners.

Today’s criminal networks either own their own hosting companies, or even rent server space in countries where they do not themselves reside; i.e. operate remotely, to conduct illegal business activities. Hosting and web services that protect the criminal operations, are also deployed.

Chart 5 below, illustrates the top five web services for distribution of illegal streams from Allsvenskan (SE), Superligaen (DK), SHL (SE), and Eliteserien (NO). The percentage figures quoted, are based on 1928 number of take-down requests made by NCP, on behalf of the four aforementioned sports leagues in 2016. Of those 1928 requests, there were only taken action in four of them.

Some of these web services are set up to facilitate both legal, and illegal streams, whilst others are suspected to be tools used solely for the purpose of illegal activities.

The hosting companies are also vital players in the illegal streaming business. In this area, the criminal networks also have preferred service providers. Chart 6 below, shows examples of the top five companies hosting illegal streams.

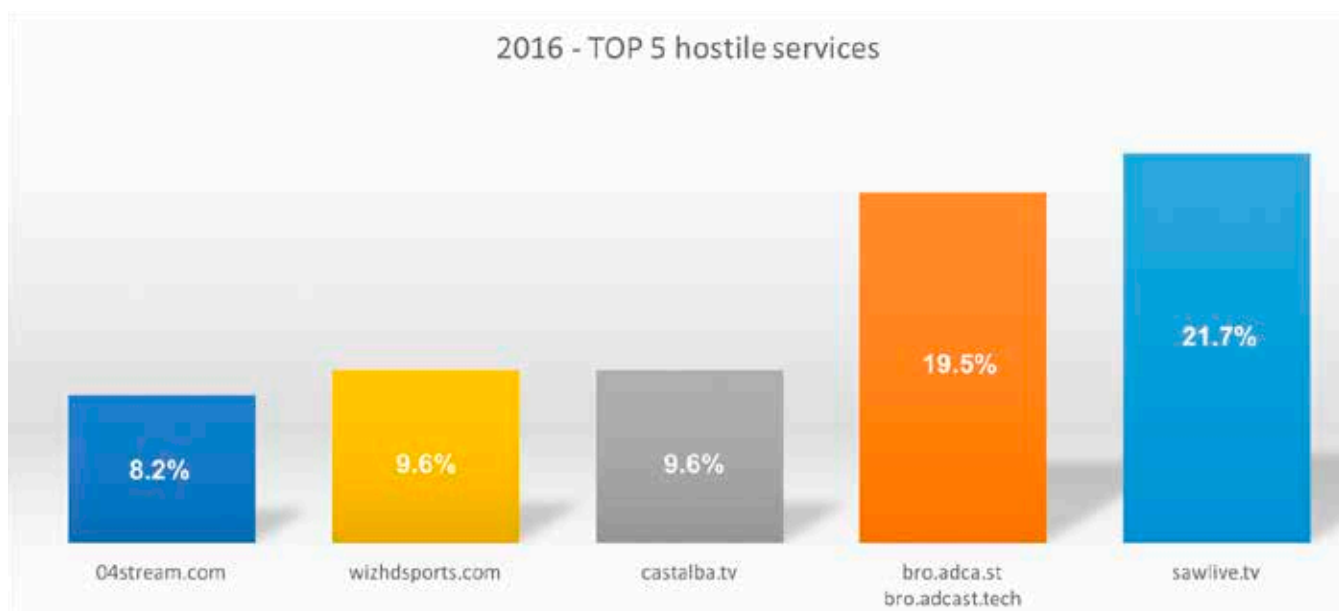


Chart 5. The top five services with none or very few takedowns in 2016.

In NCP's professional experience, these companies display the same kind of behavioural attitude as the web page providers. Their willingness to implement measures aimed at reducing the number of illegal streams, is notably negligible.

A new trend indicates some of the larger criminal networks establishing their own hosting companies, in order to safeguard their illegal activities. There is reason to believe that this development will continue, and possibly increase in scope in the foreseeable future.

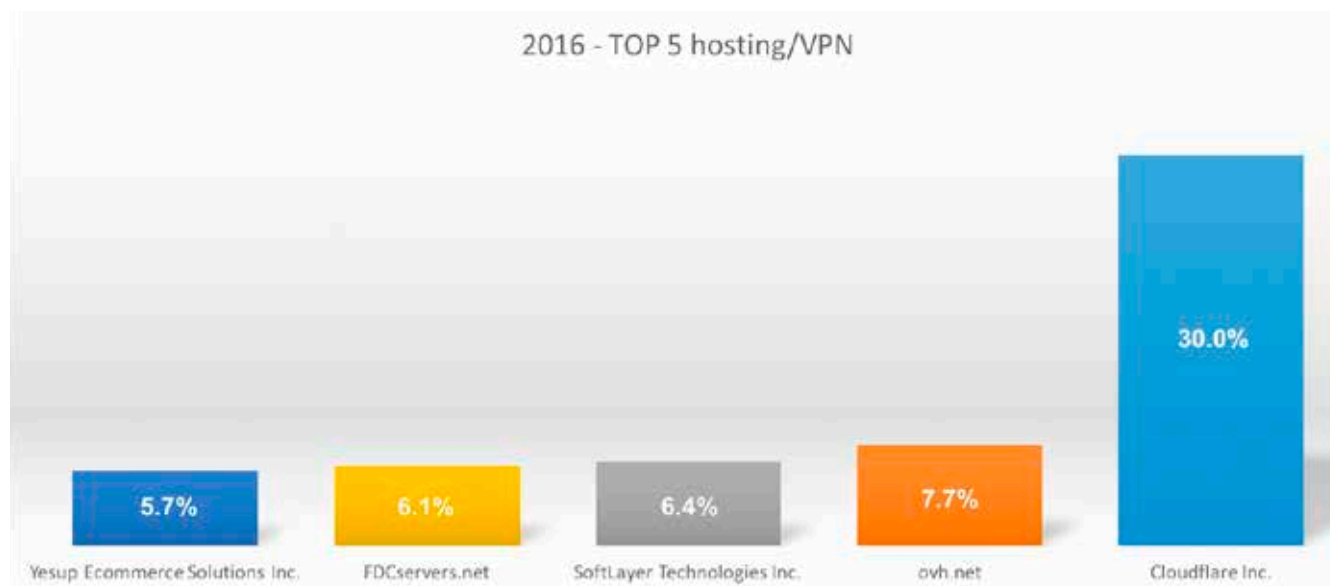


Chart 6. The top five companies hosting or facilitating illegal streams in 2016.



NORDIC
CONTENT
PROTECTION