



Master thesis

Network forensics 60hp

Procedures of investigation around online child sexual abuse

Comparison between Belgian and Swedish Police

Digital forensics 15hp

Halmstad 2023

Marine de Wilde d'Estmael



Summary

The primary aim of this master's thesis is to explore the differences between the methods used by the Belgian and Swedish Police in their investigations of online child sexual abuse in order to answer my research question “What could those specialised teams improve?” The first part of this work is theoretical and provides information on the structure of the Belgian and Swedish Police. This will be followed by a brief discussion of the role of Europol and Interpol in the fight against child sexual abuse, as well as a short chapter on cryptography to understand how international communications are conducted.

The second part is about the practical part of this work. To collect the necessary information, the Belgian Police opened their doors, specifically to the Child Abuse section, for three days. They introduced their teams, equipment, current and closed investigations, and answered a pre-prepared list of questions.

It was not possible to meet with the Swedish Police in person. Therefore, it was decided to gather the necessary information through interviews. The questions were based on the time spent with the Belgian team.

Once the information was gathered, it was compared, and a score was assigned to each response provided by Belgium and Sweden to give an idea of their accuracy and completeness. Subsequently, a list of recommendations was formulated with the aim of proposing areas for improvement.

The statistics presented at the end of this thesis allow for a visualization of the evolution of the number of assaults and investigations opened and resolved.

Abstract

I have decided to investigate the issue of child sexual abuse because it is a topic that interests me and I wanted to learn more about the current techniques in place to combat this phenomenon. As Belgium is my home country and Sweden is where I am pursuing my Master's degree, I wanted to explore the different existing techniques in these two countries. As international cooperation is important, I also looked into entities that facilitate it and share information, such as Interpol, Europol, and NCMEC.

In the future, I would like to join the Police in Belgium initially, and subsequently, possibly Interpol. This work has allowed me to gain a first-hand experience of this profession and the Police officers, reinforcing my desire to work in this field.

Preface

My thanks go to all the people who contributed to the realisation of this master thesis.

First and foremost, I would like to thank my supervisor Mark Dougherty for accompanying me throughout this work. His valuable advice allowed me to sharpen my research and helped me explore new avenues. He also helped me find solutions when I faced problems.

I would also like to express special thanks to Commissioner Yves Goethals for allowing me to accompany him for 3 days to observe his work and the techniques used by his Child Abuse team.

My thanks also go to Superintendent Per-Åke Wecksell for taking the time to answer my questions. I would like to thank Olga Torstensson for helping me find contacts within the Swedish Police and also with Europol.

I would also like to thank Alicia Isaksson for helping me translate Swedish websites and other sources of information into English. Thank you also to Johanna Kahlqvist and Frida Wilke for their valuable advice.

Finally, I would like to express my gratitude to Commissioner Alain Luypaert for his recommendations.

Table of contents

Summary	1
Abstract	2
Preface.....	3
Table of illustration	6
Glossary	7
Introduction.....	8
Research questions	9
Belgian Police	10
Structure.....	10
1. Federal Police	10
2. Local Police	11
History	11
Child abuse	11
Swedish Police	12
Structure.....	12
History	13
National Cyber Crime Center	14
Europol	14
EMPACT	15
VIDTF	15
Interpol.....	15
ICSE.....	16
NCMEC.....	17
Cryptography.....	18
History	18
How does it work?.....	18
Artificial Intelligence (AI)	19
Method.....	19
Results	21
Questions and answers	21
Differences	29
Similarities	30
Accuracy	30
Statistics	31
Belgium.....	31

Sweden	34
Recommendation	35
General	35
Police	36
Belgium	36
Sweden	36
Conclusion	38

Table of illustration

Figure 1 - Logo of Belgium Police (https://fr.wikipedia.org/wiki/Police_f%C3%A9d%C3%A9rale_(Belgique)#/media/Fichier:Logo_Police_f%C3%A9d%C3%A9rale.gif)	10
Figure 2 - Logo of Swedish Police (https://www.freepng.fr/png-tn4x3k/)	12
Figure 3 - Logo of Europol (https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/europol_en)	14
Figure 4 - Logo of Interpol (https://www.freepng.fr/png-ir0mh7/)	15
Figure 5 - Data used for the first graph, furnished by police.be	31
Figure 6 - Statistics based on number of Police reports.....	32
Figure 7 - Data used for the second graph, furnished by ICSE database	33
Figure 8 - Statistics based on ICSE database	33

Glossary

Barnahus : "Barnahus" is a model promoted by the Council of Europe to combat sexual abuse of children by coordinating the investigations of law enforcement and social services carried out in parallel in a safe and child-friendly environment. It brings together all competent professionals (judges, prosecutors, Police officers, social workers, and health professionals - psychologists and forensic doctors, etc.) in one place in order to obtain from a child victim of sexual abuse the necessary information for the investigation and legal proceedings, and to provide support, including medical assistance and therapeutic accompaniment.

Cyberlokking: Cyberlokking is a crime in Belgium where an adult communicates with a minor via ICT to facilitate committing a crime (such as sexual assault or rape) against that minor. Grooming involves the concrete proposition of a physical encounter. A purely suggestive sexual conversation cannot, therefore, be qualified as grooming.

DJSOC: DJSOC stands for Directorate for combating Serious and Organised Crime. It's a unit part of the Federal Police in Belgium on which the Child Abuse Unit depends.

EAW: European Arrest Warrant, is a legal instrument used by EU member states to facilitate the extradition of individuals who are suspected or convicted of a crime in one member state but are currently in another member state. The EAW was created to simplify and speed up the extradition process between EU member states and ensure that criminals do not evade justice by crossing borders within the EU.

EU: European Union

EXIF data: EXIFS files contain important data about a picture or a video like date and time, localisation, type of camera that has been used, and so on.

Griffeye: Griffeye is a software used by the Swedish Police in order to analyse images and videos seized on suspect's servers.

Grooming: Solicitation of children for sexual purposes, is "a practice where an adult 'befriends' a child for the purpose of committing sexual abuse against that child".

LFE: stands for Large File Exchange/ This solution enables the secure exchange of files that exceed the size limit (50MB) of the Europol Secure Information Exchange Network Application (SIENA) when the need arises.

SIENA: SIENA stands for Secure Information Exchange Network Application. This platform ensures the secure exchange of sensitive and restricted information.

VIZX: VIZX is a software used by the Belgian Police in order to analyse images and video seized on suspect's servers.

Introduction

This thesis is a comparative study between the procedures implemented by the Belgian and Swedish Police in the context of investigations into online child sexual abuse. The main idea is to highlight the differences between these two countries in this aspect, and to see what could be improved. The basic approach focused on the technological mean used to combat this phenomenon. Over time, it was decided to generalise this work on the procedures put in place. This topic is of great interest for several reasons, including:

- Improving procedures also means improving the prevention work of the phenomenon.
- Offering effective psychological assistance to victims and families.
- Highlighting this phenomenon to raise public awareness.
- Accelerating the arrest of criminals to prevent an increase in the number of victims.

The interest today is even greater. With the health crisis and lockdowns, a new phenomenon has been discovered. People from Europe or the United States send money to parents in the Philippines in exchange for sexual acts committed on their children in front of the camera.

In order to carry out this comparison work, a 3-day immersion in the Child Abuse department of the Belgian Police was conducted. The department head described his unit's work in detail, the procedures in place, the technological tools used, as well as the problems and limits that he and his team sometimes face. Another method was used to gather the necessary information from the Swedish Police. A list of questions was drafted based on the information gathered from the Belgian Police and transmitted to the Swedish Police.

This thesis consists of two main parts. The first is theoretical and consists of various subjects such as the structure and history of the Belgian and Swedish Police but also more technical concepts such as cryptography. Two chapters are devoted to Europol and Interpol, which explain the technological means put in place by these two entities. The second part is the practical part. It includes the answers to the interview questions, the comparison between the two entities, statistics on this phenomenon, and recommendations.

My work is groundbreaking as is it the first of its kind. Despite my extensive research, I have found no prior studies that compare the Belgian and Swedish Police forces, nor the units responsible for combating online child sexual abuse.

Research questions

This work will answer the two following research questions:

- What could be improved in the fight against online child sexual abuse?
- What are the differences and similarities between Belgian and Swedish Police?

The first research question will be answered under the form of recommendations that can be found at the end of this work. It is divided under 3 sections: General, Police and by country. The "General" section is intended for the general public as well as international entities, while the "Police" section is intended for the Belgian and Swedish law enforcement agencies. This section will contain two subsections with specific recommendations for each country.

The second research question will underline the differences and similarities that can be found between the Belgian and the Swedish Police and their procedures. It will be answered in the section result. By identifying those differences, the responsible units could learn from each other, and, this way, improve their methodology.

Belgian Police

Structure

The Police in Belgium is divided into 2 main agencies, local and federal. The federal Police, also known as the integrated Police, is in charge of upholding national security and public order across the board. The enforcement of local laws, upkeep of public order, and security within each territory are all the responsibility of the local Police forces. [1]



Figure 1 - Logo of Belgium Police
([https://fr.wikipedia.org/wiki/Police_f%C3%A9d%C3%A9rale_\(Belgique\)#/media/Fichier:Logo_Police_f%C3%A9d%C3%A9rale.gif](https://fr.wikipedia.org/wiki/Police_f%C3%A9d%C3%A9rale_(Belgique)#/media/Fichier:Logo_Police_f%C3%A9d%C3%A9rale.gif))

1. Federal Police

General information

In 2001, a comprehensive reform created a new Police service in Belgium, with federal and local levels that work independently but collaborate to ensure security and democracy. The National Safety Plan outlines national policy and provides guidance for Local Safety Plans. The Federal Safety Council evaluates the Police services' work and organisation.

Function and mission

The Federal Police collaborates with local Police services to ensure domestic security and uphold democracy. Principles of integrity, impartiality, and responsibility guide them. They are responsible for executing specific missions related to the administrative and judicial Police and providing specialised support to local Police.

Structure and organisation

The Integrated Police is divided into several directorates, each with specific responsibilities. The organisation is headed by a Commissioner General who coordinates the work of these directorates:

- i) Directorate of Administrative Police: Responsible for public order, traffic control, and general security.
- ii) Directorate of Judicial Police: Responsible for criminal investigations and enforcing federal laws.
- iii) Directorate of Intelligence: Responsible for gathering and analysing intelligence to support Police operations.
- iv) Directorate of Special Units: Responsible for specialised Police operations, such as counterterrorism, hostage situations, and bomb disposal.

Education / Training

The Training Board is responsible for initiating, developing, coordinating, evaluating, and harmonising training programs for Police officers in Belgium. It falls directly under the Federal

Police's Directorate of Human Resources and represents national interests in Police cooperation for training. The Board also pilots cross-border cooperation projects in Police training, particularly with France. Training is considered an essential factor in creating a Police policy that respects the values of democratic societies, allowing Police officers to develop their careers positively and reach higher levels of the Police hierarchy.

2. Local Police

The local Police forces, also referred to as "zone Police," are in charge of maintaining law and order within their various regions. In Belgium, there are 189 local Police zones, each with a Police head and officers. To protect the people and uphold security, the local Police departments collaborate closely with the Integrated Police.

The federal Police's special units are in charge of counterterrorism and other high-risk activities, and the railway Police ensure safety on the nation's railways. Specialized Police units are also present in Belgium in addition to the federal and municipal Police forces.

In general, Belgium's Police structure is created to make sure that various governmental branches collaborate to guarantee efficient law enforcement and to uphold public safety. [2]

History

Since it was established in 1830, the Belgian Police have been through many changes. Initially, each city had his own Police. Municipal Police were organised on a provincial basis and put under the Ministry of the Interior in 1925.

The Federal Judicial Police, the Railway Police, the Maritime Police, and the Aviation Police were all combined to form the Federal Police in 1998. The reform's objectives include strengthening Police agency cooperation and consolidating authority.

A new Police reform was implemented in 2001. It seeks to streamline Police organisation and improve coordination among various tiers of authority. After that, municipal law enforcement was arranged into Police districts, which were created when the previous city Police merged.

An updated Police reform that aims to boost federal and local Police cooperation while also enhancing Police efficacy and efficiency was announced in 2018. Greater Police agency specialisation and improved power-level communication will result from this reform. [3] [4]

Child abuse

The Belgian Federal Police has a unit called Child Abuse, which is part of the DJSOC (Directorate for combating Serious and Organised Crime). This unit is in charge of the

investigations of sexual offenses against children. The service collaborates closely with social services and NGOs in order to protect the victims of those crimes.

The investigators are a team of professional trained to work with children and more specifically, children victim of trauma. They have specific techniques of interview to collect information from children and witnesses while being careful not to influence the answer and reduce the victim's stress.

The unit also works to prevent those crimes by giving information and tools to parents, teachers and other professionals who work with children. They also developed an online reporting system for people who prefer to give information online. [1]

Swedish Police

Structure

The Swedish Police Authority is a combination of the National Police, the Regional Police, and the Local Police, and is headed by National Police Commissioner Anders Thornberg.



Figure 2 - Logo of Swedish Police

(<https://www.freepng.fr/png-tn4x3k/>)

Police is in charge of strategic planning over the country and the coordination of Police activities. They also managed specialised units such as the National Operations Department and the National Criminal Investigation Department. The National Police also comprises six National Departments and the Office of the National Police Commissioner.

The Regional Police is responsible for coordinating and managing Police activities within its region, which consists of several counties. There are seven regional Police authorities in Sweden. Each regional Police authority is responsible for regional contingency planning, counter-terrorist capacity, the Operations Centre, and the Police Contact Centre. Specific tasks may be coordinated at the regional level, such as investigating specific types of crime, such as investigating specific types of crime.

The Local Police are responsible for daily Police work in a specific geographical area, such as a municipality or a Police district. There are approximately 95 Local Police Districts and 25 Police Districts in Sweden.

The Swedish Police Authority also comprises one Department of National Operations, which includes a Cybercrime centre (SC3) and one National Forensic Centre (NFC). Each Police region has a regional cybercrime centre (RC3).

Police officers and civilian employees work on the vast majority of forensic work. In cases where investigations require additional expertise, the NFC provides assistance. However,

information was not found on the number of civilian employees versus Police officers working in this area.

Due to some organisational changes made by the Swedish Police Authority, the number of Police districts might change.

The Swedish Police Authority is a large, intricate organisation with many departments and specialised groups that work together to protect the safety and security of the Swedish populace. [2] [5] [6]

History

The Swedish Police force was established in 1850 as a centralized organization to replace the earlier decentralized system. Initially, the Police force was divided into two branches: the city Police and the rural Police. The city Police were responsible for law enforcement in cities and towns, while the rural Police were responsible for the countryside.

During the early 20th century, the Swedish Police force underwent significant reforms, including introducing the "People's Police" concept in 1920, which aimed to make the Police more accessible and responsive to the needs of the people.

In order to replace the previous decentralised structure, the Swedish Police was established in 1850 as a centralised organisation. In order to replace the previous decentralised structure, the Swedish Police was established in 1850 as a centralised organisation. The two first divisions of the Police were the city Police and the rural Police. While the rural Police is responsible of upholding the law in rural regions, city Police is in charge for it in cities and municipalities. In order to become more approachable and sensitive to the population needs, the Police developed "people's Police", which is part of the major changes the Police went too in the early 20th.

The Police force was crucial in keeping the peace and defending citizens during World War II. However, after the war, there was controversy and criticism because some Police officials worked with the Nazi regime.

The Swedish Police force continued to develop and modernise in the years following the conflict by implementing fresh techniques and educational initiatives. The Police improved his participation in international cooperation, especially in the fight against organised crime and terrorism.

The Swedish Police is divided into seven regional Police authorities. It employs 35000 people including Police officers, civilian workers, and volunteers. The Police is responsible for the maintain of law and order, investigates crimes, and protect the population. [4] [5] [6]

National Cyber Crime Center

The Swedish Cyber Crime Center (Swedish: Nationellt cyberbrottscentrum) is a specialized unit within the Swedish Police Authority that focuses on preventing and investigating cybercrime in Sweden. It has its headquarters in Stockholm and was founded in 2012.

To combat cybercrime, the centre collaborates closely with other law enforcement organisations in Sweden and with foreign allies. Its duties include performing cybercrime investigations, analysing cyber threats and trends, and advising and supporting other law enforcement organisations.

The center also works to raise public knowledge of cyber threats and offers guidance and information to assist people and organisations in preventing cybercrime. Additionally, the centre runs a national cybercrime reporting portal where people and organisations can submit incidents and get help and advice.

Overall, the Swedish Cyber Crime Center is essential to Sweden's fight against hacking and to maintaining the safety and security of its citizens and organisations. [7]

Europol

Europol is an EU agency headquartered in The Hague, Netherlands, with a mission to help its member states prevent and combat all forms of serious international and organised crime, terrorism, and cybercrime. Europol works with several non-EU partner countries and international organisations. Its primary threats include terrorism, international drug trafficking, money laundering, organised fraud, counterfeit euros, and human trafficking. Europol supports investigations launched by member states and works to process cases that require international cooperation. It provides regular assessments and analyses of crime and terrorism in the European Union to help partners better understand the crime they are fighting. To store, search, view, and connect information, Europol uses specialised systems. These systems also come with a wide range of innovative tools for preventing crime. The Council of Ministers of Justice and the Interior of the European Union is in charge of supervising Europol's activities. The Council chooses the Director, its Deputy Director, and the Budget Approval Council in collaboration with the European Parliament. An Executive Director heads Europol, currently Catherine De Bolle, who is supported by three deputy executive directors. [9]



*Figure 3 - Logo of Europol
(https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/europol_en)*

EMPACT

EMPACT is an acronym for the European Multidisciplinary Platform Against Criminal Threats, which is an integrated approach to EU internal security that involves various measures from external border controls, Police, customs and judicial cooperation to information management, innovation, training, prevention and public-private partnerships. EMPACT has evolved into an EU flagship instrument for multidisciplinary and multiagency operational cooperation to fight organised crime at an EU level. The goal is to address the most critical criminal risks confronting the European Union systematically and cohesively. This objective will be achieved through enhancing and reinforcing collaboration among the relevant entities of the Member States, EU institutions and agencies, as well as external nations and organisations, including relevant private sector entities. The Council of the European Union decided to permanently continue the EU Policy Cycle for organised and serious international crime, EMPACT 2022+ and the EU's priorities for the fight against serious and organised crime for EMPACT 2022-2025. Those are high-risk criminal networks, cyber-attacks, trafficking in human beings, child sexual exploitation, migrant smuggling, drugs trafficking, fraud economic and financial crimes, organised property crimes, environmental crimes and firearms trafficking. [9]

VIDTF

Victim Identification Taskforce was held at the invitation of EU Member States and other collaboration partners. (VIDTF). At the Europol headquarters in The Hague, victim identification specialists from 11 police agencies and nine nations collaborated over the 12 days. Unprecedented amounts of data were worked on, analysed, and hints that could help localise investigations and identify the victims were looked into. [9]

Interpol



Figure 4 - Logo of Interpol
(<https://www.freepng.fr/png-ir0mh7/>)

Interpol is an international organization whose purpose is to facilitate cooperation and communication between their 195 member countries. Their mission is to make the world safer. They provide wide of range of services. One of them is by creating giant database where the members can share pictures, videos, data and so on. INTERPOL manages 19 Police databases with information on crimes and criminals, from names and fingerprints to stolen passports, and these databases are accessible in real-time to member countries.

In addition to data sharing, INTERPOL also provides technical and operational support to its member countries. This includes investigative support such as forensics, analysis, and assistance in locating fugitives around the

world. Training is also an important part of what INTERPOL does, as it helps officials work more efficiently with the organization's services.

INTERPOL specializes in three global areas that it considers to be the most pressing today: terrorism, cybercrime, and organized crime. Officials working in each specialized crime area run a variety of different activities alongside member countries. This can include investigative support, field operations, training, and networking.

To coordinate all of these activities, INTERPOL has a number of different bodies. The General Secretariat is the body that coordinates the day-to-day activities of the organization. It is staffed by both Police and civilians, and it comprises a headquarters in Lyon, a global complex for innovation in Singapore, and several satellite offices in different regions.

In each member country, there is an INTERPOL National Central Bureau (NCB) that provides the central point of contact for the General Secretariat and other NCBs. An NCB is run by national Police officials and usually sits in the government ministry responsible for policing.

The General Assembly is the governing body of INTERPOL, and it brings all countries together once a year to take decisions. INTERPOL also connects all its countries via a communications system called I-24/7, which allows them to contact each other and the General Secretariat in real-time.

Since crimes are increasingly international in nature, it is crucial that there is coordination among all the different players in maintaining a global security architecture. INTERPOL provides a global platform for cooperation, enabling Police to work directly with their counterparts, even between countries which do not have diplomatic relations. In addition, INTERPOL provides a voice for Police on the world stage, engaging with governments at the highest level to encourage cooperation and the use of its services.

All of INTERPOL's actions are politically neutral and taken within the limits of existing laws in different countries. [10]

ICSE

The International Child Sexual Exploitation (ICSE) image and video database is a powerful tool used by specialized investigators to share data on cases of child sexual abuse. It enables victim identification experts worldwide to analyze and compare images and videos of child sexual abuse, helping them make connections between victims, abusers, and places.

The database uses image and video comparison software, which allows investigators to quickly identify whether a series of images has already been discovered or identified in another country or whether it has similar features to other images. By avoiding duplication of effort and saving time, investigators can focus their efforts on locating victims of child sexual abuse.

With more than 4.3 million images and videos, the ICSE database has become an intelligence and investigative tool for specialized investigators from over 68 countries to exchange information and share data with their colleagues worldwide. By analyzing the digital, visual,

and audio content of photographs and videos, victim identification experts can retrieve clues, identify any overlap in cases and combine their efforts to identify and locate victims of child sexual abuse.

This powerful tool has helped to identify more than 32000 victims of child sexual abuse worldwide. It is an indispensable component in the fight against child sexual abuse. The continue of grow is important to bring criminal to justice and protect children around the world. [10]

NCMEC

The National Center for Missing & Exploited Children (NCMEC), a non-profit organization, was founded by the United States Congress in 1984, after the murder of Adam Walsh in 1981 and the disappearance of Etan Patz in 1979. NCMEC deals with cases of missing and exploited children. The organisation is led by Jon Grosso, and the bulk of its funding comes from the US Department of Justice. NCMEC handles cases involving exploited or missing children under the age of 20. It acts as a resource for parents, law enforcement, educational institutions, and the community to assist in finding missing children and spread knowledge of ways to stop child abduction, sexual abuse, and pornography.

The CyberTipline, a centralised reporting platform for the online exploitation of minors in the United States, is managed by the NCMEC. It examines reports of alleged child sexual exploitation and sends them to task groups looking into Internet Crimes Against Children (ICAC) or law enforcement organisations.

CyberTipline is the primary national reporting mechanism for instances of online child exploitation. It receives reports related to online child exploitation, such as online enticement of children for sexual acts, child sexual abuse material, child sex tourism, child sex trafficking, child sexual molestation, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the internet. In 2018, CyberTipline processed 18.4 million reports related to online child exploitation.

The NCMEC reviews the reports and provides geolocation and identifying information, such as email address, username, or IP address. Although anyone can make a report, certain electronic service providers (ESP) and social media are required to report the presence of child pornography on their systems. The CyberTipline does not mandate ESPs to search for or attempt to identify child pornography actively. However, many ESPs choose to do so.

In cases where a report has an IP outside of the USA, the NCMEC transfers the data to Europol or the concerned country, depending on the agreement that has been made. The NCMEC has also identified the deceased, particularly children, teenagers, and young adults.

The Center has recently backed the PROTECT Our Children Act of 2022, which extends funding for the Internet Crimes Against Children Task Force (ICAC) and assists in investigating

and apprehending individuals who commit sexual offences against children. The NCMEC plays a crucial role in combating online child exploitation and assisting law enforcement agencies and communities in the United States. [8] [11]

Cryptography

History

Cryptographic techniques have been used since ancient times, with symbol substitution appearing in both ancient Egyptian and Mesopotamian writings. The oldest known example of symbol substitution cryptography was found in the tomb of an Egyptian noble named Khnumhotep II, dating back approximately 3,900 years ago. In ancient Sparta, messages were encrypted by writing them on a parchment placed on a cylinder of a particular size, and Indian spies used coded messages as early as the 2nd century BC.

During the Middle Ages, cryptography became increasingly important, and codes of substitution, including the Caesar cypher, remained the norm. Cryptanalysis, the science of deciphering messages and codes, began to catch up with cryptography, and in the Renaissance period, the polyalphabetic cypher was developed to counteract frequency analysis. New methods of encoding information were developed, including Sir Francis Bacon's binary code in 1623. In the 18th and 19th centuries, cryptography advanced with the development of the Jefferson wheel, which served as the basis for American military cryptography during WWII. The Enigma machine was also developed during WWII as an example of mechanical cryptography. It was used by the Nazi and has been broken by Alan Turing in 1942. [8] [12] [13]

How does it work?

A secret code or encryption key is used in cryptography to generate encrypted communications. Cryptography is mainly used to protect a message considered confidential. This method is used in many fields, including defence, information technology, privacy and protection. Many cryptographic algorithms can be used to encrypt (and decrypt for the recipient) the message. Some are considered basic (for example, shifting the alphabet letter to the right or left with a certain number of notes), while others offer almost absolute security. Symmetric cryptography involves multiple people using the same key to encrypt and decrypt messages. It's fast to run and easy to use. The primary drawback of this system is the need for individuals to trade unique keys with one another. This is why authentication of correspondents is essential when a person wants to perform secure transactions.

In order to exchange the cypher key securely, we use asymmetric encryption. This uses two keys for each user: a private key that must be kept private and a public key that is visible to all other users. These two elements are interconnected mathematically. The messages or the symmetric cypher key is encrypted with the public key, and the private key is used for

decryption. After something has been encrypted with the public key, only someone with a private key can decrypt it. To ensure that an on-line identity is not spoofed, the public key needs to be verified by an authentication agency. This can be done by the authentication agency encrypting an individual's public key with the agency's own private key. Possession of the agency's public key can then be used to verify any published public key. Diffie-Hellman is a key exchange protocol that allows two users to exchange a secret key over an untrusted network. This method protects from a man-in-the-middle attack only if an authentication method has been applied before. [8]

Artificial Intelligence (AI)

Artificial Intelligence, commonly referred to as AI, aims to enable machines, particularly computer systems, to simulate human cognitive processes. These processes encompass learning (acquiring information and rules associated with their use), reasoning (applying rules to reach approximate or precise conclusions), and self-correction. Specific applications of AI include expert systems, speech recognition, and computer vision.

The term "Artificial Intelligence" was first coined by John McCarthy, an American computer scientist, at the Dartmouth Conference in 1956, which marked the birth of the field. Today, the term encompasses both Robotic Process Automation (RPA) and physical robotics. It has gained significant visibility in recent times, partly due to Big Data, which refers to the speed, volume, and diversity of data collected by companies. AI, more adept than humans at extracting trends from data, allows businesses to leverage a wealth of information.

Here are some example of AI applications:

- Healthcare: AI improves patient care, diagnoses, and reduces costs.
- Business: Robotic Process Automation (RPA) automates repetitive tasks and enhances customer service.
- Education: AI automates grading, adapts to students' needs, and provides additional support.
- Finance: AI disrupts personal account management and real estate purchasing.
- Law: AI automates legal processes and develops question-answering assistants.
- Industry: Robots are integrated into workflows, transforming the industrial sector.

Method

In order to gather the necessary information for this work, I started by contacting the Federal Police in Belgium. During my bachelor's degree in computer security, I completed my internship at the Federal Police in Belgium. This allowed me to easily reconnect with my former internship supervisor. He put me in touch with Commissioner Yves Goethals, responsible for

the Child Abuse section. After some email exchanges, we agreed on 3 days, from December 28th to 30th, so that I could accompany him in his daily work. He introduced me to all the technical equipment, platforms, and other computer tools used in his work. He also explained their methodology, using some investigations as examples.

Later on, I obtained a contact in the Swedish Police thanks to the intervention of Olga Torstensson. After some email exchanges, it appeared unfortunately impossible to repeat the same experience as with the Belgian Police. Therefore, I wrote a list of questions based on everything I had learned and the notes I had taken during my time at the Federal Police in Belgium, and sent them by email. Superintendent Per-Åke Wecksell was my correspondent and answered my questions several times.

I sent an official interview request to Europol in order to learn more about their ongoing projects (including the project on AI), their role in international communication, and what they are actually contributing to investigations related to online child sexual abuse. Unfortunately, my request went unanswered.

Results

You will find here a comparison between the answers given by Belgium and Swedish Police. It will be followed by two texts explaining the differences and similarities between their answers. Another part will be about their accuracy.

Questions and answers

1. How is the Police in your country structured? Is there a federal and a local Police?
 - a. If so, what are the responsibilities of each structure?
 - b. Do you have a National Forensics Center? If so, how is the work divided between the National Forensics Center and the regular Police?
 - c. How much of the work is done by Police officers and how much by civilian experts?

The answer to this question has been explained previously in the chapters "Structure of the Belgium Police" and "Structure of the Swedish Police"

2. What is the definition of child abuse in your country? What is the legal age of sexual consent?
3. What laws exist in your country that address child sexual abuse online?

Both questions will be answered as one.

Belgium: Translation based on Belgian Law written in French: "Non-consensual sexual act committed against a minor under the age of 16". Legal age of child sexual consent is 16 years old. One exception: can be allowed since 14 if the other person is maximum 3 years older.

Sweden: Child sexual abuse is a collective name for all forms of sexual acts that a child is subjected to by another person. It includes both physical abuse and non-physical abuse. Children under the age of 15 have special protection in the law because they are dependent on adults and are not considered mature enough to understand or consent to sexual acts with an adult or child who is older or more mature. Children between the ages of 15 and 18 are also particularly protected by the law when it comes to sexual acts from persons on whom they are dependent.

The legal age for sexual consent is 15.

Here are the laws that exist about Child Sexual Abuse:

- exploitation of children for sexual posing, sexual harassment
- purchase of sexual acts by children
- intercourse with offspring

- contact with children for sexual purposes, rape of a child and aggravated rape of a child, child pornography offences, sexual abuse of children, Illegal invasion of privacy

4. Can you describe the process for handling cases of online child sexual abuse?

Belgium:

Step 1: Receiving of information through various channels

Step 2: The info is evaluated. If it's punishable and committed in Belgium, an initial Police report is written.

Step 3: The prosecutor decides if the federal or local Police take it up. In 95% of cases, cases are assigned either to the decentralized federal Police or local Police. Local Police can ask for support from federal Police or they can propose their help for long and complex investigations. Support can be: joining for a house search or analysing images (determine if punishable, if any face is recognised, check the ICSE database, ...)

Sweden: The investigations is the same as offline cases. In Barnahus there is cooperation between different authorities (Police, social services, public prosecutor, forensic medicine, paediatrics and child psychiatry) responsible for children who were suspected of being exposed to sexual or physical abuse.

5. Does the Police conduct virtual or online undercover operations?
- a. If so, what are the requirements for these operations?
 - b. Are officers allowed to provoke suspects?
 - c. Is there any specific training or qualifications required for officers to perform this type of work? If so, how many officers have done it?
 - d. Is a warrant required, and if so, what is a warrant deadline?
 - e. Are there any protocols in place for emergency situations?
 - f. Are officers required to work in groups and record their actions?
 - g. Can you provide more detailed information about the process and requirements for online undercover operations?
 - h. When did this type of work become legal in your country?

Belgium: Yes, they are called IVI for "Infiltration Virtuel-eel Infiltratie". It's a mix of Dutch and French meaning "Virtual Infiltration".

- a. If nothing else has worked, if it's a correctional sentence for one year or more and only for crimes and offences.
- b. No, e.g.: Lolita14y is forbidden.
- c. There's mandatory training with 3 different levels. All 3 must be done by any officer who will do IVI. 2 Police inspectors of DJSOC have done the training and more or less 50 in Belgium in total.
- d. There's a warrant needed that has a 3 months deadline.
- e. In case of emergency, the authorisation can be verbal but there must be personal interaction.
- f. Yes, they work in group of 2, every communication must be recorded.
- g. The fictive ID cannot be a already existing one. To do so, they always check the national register.
- h. It is legal since 2016 and was used for the first time in 2021.

Sweden:

- a. No answer
- b. Yes, under certain situations only after a decision from preliminary investigation manager.
- c. No answer
- d. No answer
- e. No answer
- f. No answer
- g. No answer
- h. No answer

6. How does the Police handle cases that involve cryptography?

Belgium: When a file is encrypted, we identify the uploader of the file and request that they disclose their password, which they usually do not do (due to forgetfulness or refusal). Attempts can then be made to technically break the decryption. As for "end-to-end encryption," this is one of the most difficult discussions within the working groups preparing the new CSA regulation. To my knowledge, we cannot compel platforms to break encryption. However, we still receive reports from platforms such as WhatsApp. I assume they intercept illegal material at an earlier stage.

Sweden: There are specialists that are handling those cases and they have special tools. We do not want to reveal these works.

7. Is the Police allowed to use the dark web for investigations? If so, what type of activities are conducted on the dark web?

Belgium: Yes since the cassation judgment of 28 March of 2017 is the darkweb considered as public space. Different kind of investigations are conducted on the darkweb like investigations about drugs, children pornography, ...

Sweden: Swedish Police are allowed to work on the darknet. We do not want to reveal these works.

8. Does the Police use VIZX?
a. What is the process for analyzing images with or without VIZX?

Belgium: Belgium Police uses VIZX as tool to analyse images.

-Step 1: Arriving from CD/DVD/DD, import the data on the system and create folders.

-Step 2: Indexation process: the server separates photos and videos based on their content. Then the new data is compared with the data in the database based on the hash and the photo DNA (= divided the image in 32 pieces and calculate the hash of each of them, then the average of those hashes is calculated). 7 databases are used: 3 Belgian (ChildAbuse, Sensible-Gevoelig, No ChildAbuse) and 4 from interpol ICSE (Offender Only Identified, Unidentified, Victim ID – Distributed, Victim ID – Non distributed)

-Step 3: Manual analyse is done by a Police officer.

-Step 4: Making a report.

Sweden: We use Griffeye but we are trying to move away from solely categorizing the material but now focus on Victim Identification and at an initial stage try to find newly produced material that contains unidentified plaintiffs. We do this in Griffeye via various filters that make it possible to filter on the size of the file, different EXIF values, paths in attachments, etc., etc. Our systems also make it possible to exclude certain types of media files, which means that we get a smaller number of files to analyze/work with.

9. How does the Police obtain information about phone numbers or IP addresses during an investigation?
 - a. Are the procedures the same for both types of information?
 - b. Is a warrant required, and if so, what are the conditions for obtaining one?
 - c. Are service providers contacted directly or via a platform?

Belgium:

- a. No, for telephone number, we use tank (communication platform between Police and providers), and for IP we directly contact the provider
- b. Warrant is needed
- c. For phone numbers, we use a platform, and for IP, we directly contact the providers. A claim signed by a magistrate is forwarded to the ISP. For urgent cases (e.g. ongoing abuse), a Judicial Police Officer may apply an expedited procedure, later confirmed with a Police report.

Sweden:

- a. We request both from service providers and tele companies.
- b. No warrant is required in Sweden.
- c. We directly contact the providers.

10. How does Police handle international cases of child sexual abuse?
 - a. Is your country involved in any international organizations or initiatives such as SIENA and LFE (transfer protocols used by Europol for information exchange), or VIDTF?

Belgium: Yes, Belgium Police use SIENA and LFE for the transfer of file and information. We sending officers at each VIDTF.

Sweden: We work close together with law enforcement and NGOs from all over the world. In certain cases, Europol or Eurojust coordinates cooperation between countries. Europol and Interpol are important to cooperate with in the fight against sexual abuse of children. The Nordic countries' cooperation (formal and informal) on these issues is important.

- a. Yes, all.

11. What is the process for investigating a case of child sexual abuse when the suspect's server is located in another country?
- Is a warrant required?
 - Do authorities in the other country need to grant permission?
 - Do Police need the authorisation of the suspect?
 - What happens in cases where your country has poor diplomatic relations with the other country?

Belgium:

- Yes, when the country is a member of the EU, we use an EAW.
- Yes.
- No.
- We're still sending a request for legal assistance.

Sweden:

- Yes.
- Yes.
- No.
- It is different from case to case. Probably we will need to take the diplomatic way.

12. Does the Police have a direct communication channel with the National Center for Missing and Exploited Children (NCMEC)?
- If so, what is the process for receiving and handling information from NCMEC?

Belgium: Belgium Police receives the reports through Europol.

Sweden: Swedish Police receives the reports through Europol.

13. Does the Police have a psychological support system in place for officers handling cases of child sexual abuse?
- Is this support mandatory?
 - Can officers discuss the images or other materials they have seen as part of their work?

- c. Are there any mandatory physical or psychological evaluations that officers must undergo (e.g.: medical test, shooting test or tests on Police techniques)?

Belgium: Yes

- a. Yes.
- b. Yes.
- c. Yes,
 - 1X/y, they have a meeting with a psychologist
 - 1X/y they have a mandatory medical check-up
 - 1x/y they have a shooting exam
 - 1x/y they have an exam about Police technics (search warrant, handcuffs, ...)

Sweden: Yes

- a. No, it's not mandatory.
- b. Yes, and that could be important to do so.
- c. There are physical and psychological evaluation tests before you are admitted to the Police training, every Police officer has to take shooting tests regularly. There are tests on Police techniques for those who need it for their work.

14. Can you provide information about the International Child Sexual Exploitation (ICSE) database?

The answer to this question has been explained previously in the chapters "Interpol".

15. Can you provide information about the Victim Identification Taskforce on Child Protection (VIDFT)?

- a. Is your country involved in this organization? How many officers are usually sent to participate and are the same officers sent each time?

Belgium: Yes, Belgium is involved and sent each time one officer.

Sweden: Yes, the number of participants varies from time to time. Sweden participates with one officer.

16. Are there statistics available of the number of child sexual abuse cases, including the number of investigations opened, number of offenders identified, number of victims identified, number of cases that went to court, number of guilty verdicts and number of offenders who served time in prison? If so, can you provide these statistics for the last six years (2017-2022)?
- a. Are there any countries with which your country does not share information on child sexual abuse cases?

Belgium: Yes, some statistics exist furnished by the database ICSE, and there is a yearly published Police statistic.

- a. Yes, Belgium does not share investigations with some countries. Their decision is based on the laws applied there.

Sweden: No answer.

- a. There're no countries that Sweden doesn't cooperate with besides Russia and North Korea.

17. Can you provide your thoughts on the AI project presented by EMPACT?
- a. How could this project potentially improve the work of the Police?
 - b. Are the Police allowed to use images seized during searches to train the AI?

Belgium: It is a very interesting project.

- a. It will improve our work by doing an initial sorting.
- b. The legal regulation of AI training will become necessary; we are working on it.

Sweden: This is very interesting and could be of great importance in the future if we get to use the technology.

- a. Hopefully we won't have to judge so many images or videos if we get help from AI.
- b. No.

Differences

The Belgian and Swedish Police forces have different structures. The Belgian Police consists of two entities: the Local Police and the Federal Police. The Local Police is responsible for law enforcement and the protection of the population within its jurisdiction, while the Federal Police has the same duties across the entire territory. The Swedish Police consists of three entities, led by the National Police Commissioner Anders Thornberg: the National Police, the Regional Police, and the Local Police. The National Police is responsible for national strategic planning and coordination of Police activities, as well as management of specialized units. The Regional Police coordinates and manages Police activities in different regions, and the Local Police is responsible for daily work.

In Belgium, the age of consent for sexual activity is 16 years old. In Sweden, it is 15 years old. However, there is a small nuance regarding the law in Belgium. Sexual consent is legal from the age of 14 if the age difference is less than or equal to 3 years. In other words, it is legal between two minors who are 14 years old or older.

In terms of cryptography, Belgium first asks suspects to provide the necessary password for decryption of files and documents. If they refuse, specialists may attempt to break the encryption. Sweden directly calls upon specialists who use specialized tools to decrypt the files.

Both countries use different image analysis software. Belgium uses VIZX and Sweden uses Griffey. Both software programs fundamentally function in the same way, based on filters such as hash, EXIF data, file size, etc. Sweden also wishes to move away from simple image categorization in order to focus more on victim identification and new material with unidentified complainants.

For telephone number identification, Belgium uses a platform called Tank (a communication platform between Police and providers). In the future, they will also use the platform for IP requests. Sweden contacts the provider directly. Another notable difference is the need for a warrant. Sweden does not require one, while in the case of Belgium, it is necessary every time.

Regarding international cooperation, Belgium and Sweden share information with concerned countries with a few exceptions. Sweden does not cooperate with North Korea or Russia. Belgium does not cooperate with certain countries depending on their laws. For example, it does not cooperate with countries that consider sexual relationships with a 9-year-old child, even within the context of marriage, to be legal.

Regarding psychological support and annual evaluations, Belgium and Sweden apply two different policies. In Belgium, psychological support is mandatory, while in Sweden it is only recommended. Belgium also requires all Police officers to undergo an annual shooting evaluation, an evaluation of Police techniques (such as handcuffing), and a medical check-up. Sweden only requires regular shooting exams.

Similarities

In both cases, their investigative processes are identical for online and real-life cases.

Both countries conduct online undercover operations. Unfortunately, due to Sweden's strict confidentiality principle, they did not provide any further details. This means that there is no comparison possible regarding their methods and rules applied.

Regarding the Darkweb, both countries are authorized to conduct investigations there.

For the identification of IP addresses, both countries directly request personal information linked to the IP address in question from the providers.

In terms of international cooperation, it is difficult not to notice great similarities. Both countries have good general relations with the rest of the world. They share information with concerned countries with few exceptions. Both also send experts to each VIDTF. Both countries also receive NCMEC reports via Europol.

When it comes to investigations where one or more servers belonging to suspects are located abroad, both countries apply the same policy. The sending of an EAW to local authorities.

Regarding artificial intelligence, both countries find the project very interesting. They are hopeful that implementing a pre-screening process for data retrieved from suspects' servers and/or computers will facilitate and improve their work in the future.

Accuracy

In order to calculate the relevance score of the responses given by the Belgian and Swedish Police, a rating of 1 to 3 was assigned to each answer. A score of 1 indicates that the response is incomplete or that there was no response, a score of 2 indicates that the response is more or less complete, and a score of 3 indicates that the response is complete. These scores were then added up and converted to a percentage. This provides an idea of the accuracy of the responses.

A list of recommendations, among other things, was drafted based on this accuracy score. Belgium scored 95.23% and Sweden scored 80.95%. These differences are due in part to the fact that Belgium provided more complete answers and was willing to answer all questions. The percentages should not be compared to any other sources, as they were calculated based on the questions written specifically for this work.

Statistics

Belgium

The Belgian Police publish yearly statistics on crime in the country. In order to complete this result part, the category criminal facts from 2012 to 30 June 2022 will be included here. Criminal acts are criminal acts or offences recorded by the Police in a report. These are criminal offences, more specifically offences under the Criminal Code (crimes, offences and contraventions) and infractions under special laws. The results presented here will be those of the categories 'Infractions against morality: Child pornography: Access to child pornography via technology', 'Infractions against morality: Grooming (contact by ICT with minors < 16 years)' and 'Infractions against other moral values and feelings: Cyberlokkung (luring a minor by ICT)'. It is important to note that these statistics are from the end of 2022 and do not take into account the recent change in the law regarding grooming. The age was raised from < 16 to < 18 years.

In order not to bias the graphs, the year 2022 will not be represented with the others, as the data ends on 30 June of that year. [1] [12] [13]

CRIMINALITE ENREGISTREE COMMISE AU NIVEAU NATIONAL Criminalité ICT



Criminalité ICT/online au sens large

Infractions (uniquement si code-fait existe)

	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Fraude: Escroquerie: Fraude par internet	11.709	9.697	11.071	12.776	13.045	14.174	19.264	26.062	37.043	38.940	19.489
Infr. contre les moeurs: Voyeurisme: Diffusion enregistrement nudité ou intimité	1		2	10	130	610	501	616	879	956	488
Infr. contre les moeurs: Grooming (contact par ICT avec mineur < 16 ans):			7	80	133	166	171	144	168	138	58
Infr. contre les moeurs: Pornographie enfantine: Accès pornographie enfantine via technologie			1	8	60	150	102	109	140	110	52
Infr. contre autres valeurs morales et sentiments: Cyberlokkung (leurre de mineur par ICT):		3	8	91	94	86	79	82	113	81	37
Infr. contre la Sécurité de l'Etat: Terrorisme: Diffuser un message qui incite au terrorisme			2	43	42	32	24	18	16	9	6
Infr. contre les moeurs: Incitation à la débauche: Publicité par ICT pour débauche	33	12	27	19	11	7	10	17	20	19	1
Armes et explosifs: Autre: Vente par correspondance/internet d'arme à feu	7	21	8	17	9	11	26	13	6	17	5
Armes et explosifs: Autre: Vente par correspondance/internet d'autre arme	7	4	6	10	12	13	7	7	3	4	1
Infr. contre autres valeurs morales et sentiments: Harcèlement: Harcèlement par téléphone (OLD)											1
Total général crim. ICT au sens large:	11.757	9.737	11.132	13.054	13.536	15.249	20.184	27.068	38.388	40.274	20.138

Figures criminelles (à considérer spécifiquement – ne pas additionner avec d'autres éléments – risque de double comptage!)

	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Cyberharcèlement	5.378	6.060	8.392	8.213	7.911	7.688	7.880	8.027	7.907	8.432	4.141

Figure 5 - Data used for the first graph, furnished by police.be

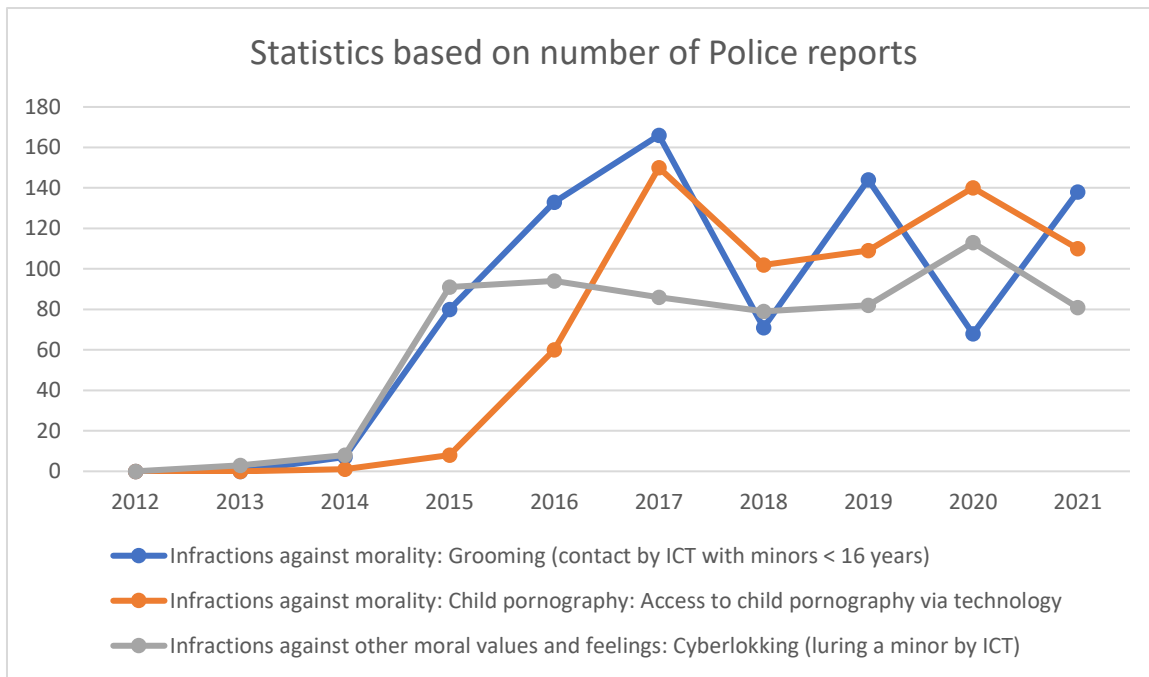


Figure 6 - Statistics based on number of Police reports

The first thing to note is that for these 3 categories, we have no statistics for the year 2012.

It is easy to notice here that before 2015, the number of reports written by the Child Abuse section was less than 20 per category. The year 2015 marks a turning point in these statistics with a general increase in online crime. With regard to cyberlokkung, with the exception of the year 2020 which saw an increase in the number of reports, this crime has a certain stability between 79 and 94 written reports. Unlike grooming, which is on a rollercoaster ride. It is clear that this is a crime that has seen a steady rise to 166 reports in 2017, before dropping back to 71 in 2018. It will rise again in 2019, only to fall again in 2020 and rise one more in 2021. Crimes related to accessing child pornography only really started to rise in 2016, reaching a peak of 150 Police reports written in 2017. Between 2018 and 2021, there will be a certain stability with between 102 and 140 reports per year.

Something that stands out in this graph is the large number of convictions issued in 2017. From 2018 to 2021, the number of tickets for accessing child pornography and for cyberlokkung follow a very similar pattern.

This graph raises several questions. Why do we observe such a strong increase in offenses between 2014 and 2015? Could it be related to the popularity of social networks? Has a law condemning these actions come into force? Why did offenses related to access to child pornography only increase the following year? Were criminals wary of technological tools? Did it take time to set up networks for sharing pedo-pornographic content? Did the Police start to find out where these networks were hiding at that time? Why do we see a spike in grooming approximately every two years? Could the Police be conducting larger-scale operations on this issue every other year? Were there awareness campaigns in those years?

The following statistics have been provided by the Police directly. They come from the ICSE database. They represent the number of investigations opened, the number of offenders identified and the number of victims identified between 2017 and 2022.

	A	B	C	D	E
1	Year	Agency	Number of created investigations	Number of identified offenders	Number of identified victims
2	2017	BE/LEA	17	9	18
3	2018	BE/LEA	24	9	38
4	2019	BE/LEA	30	11	33
5	2020	BE/LEA	40	8	53
6	2021	BE/LEA	55	13	58
7	2022	BE/LEA	18	4	19
8	Totals		184	54	219
9					

Figure 7 - Data used for the second graph, furnished by ICSE database

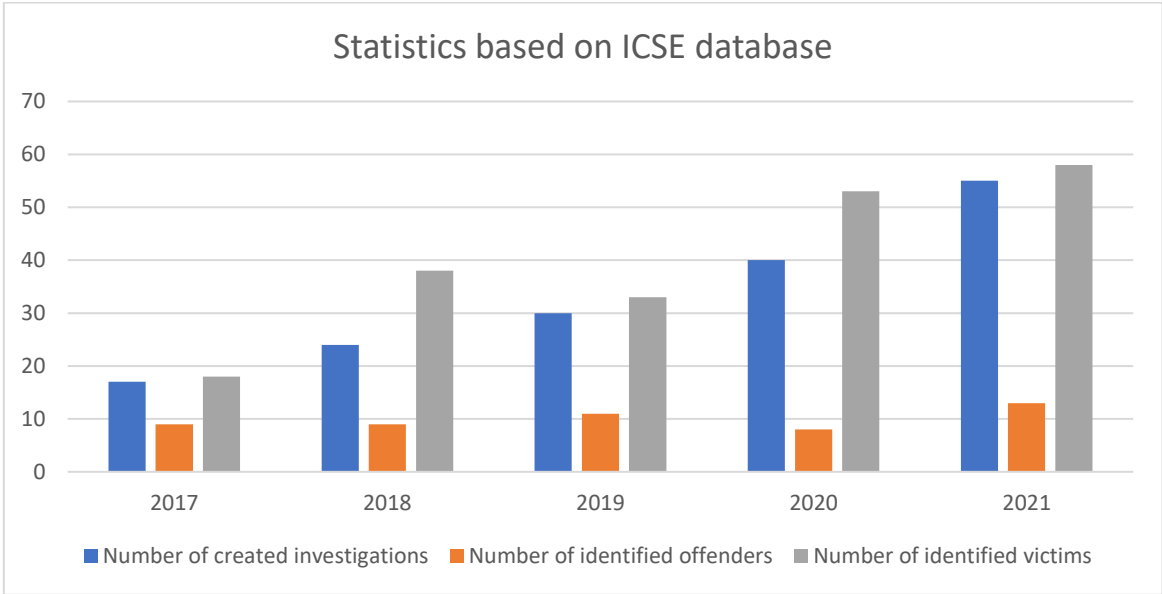


Figure 8 - Statistics based on ICSE database

It is easy to see here that there has been a general increase in victim identification over the years, from 18 in 2017 to 58 in 2021. The number of investigations started is increasing each year with 17 in 2017 and 55 in 2021. The identification of offenders is stable between 8 and 13 per year. It can be noted that the increase in the number of created investigations and the number of identified victims is more or less proportional. 2021 is a record year in terms of new investigations started and the number of victims identified.

This graph also raises its own set of questions. Why is there stability in the number of identified offenders while the number of open investigations and identified victims increases? Is it because more victims are being found per offender? Are the offenders less visible in the images?

Are the offenders located abroad? Is it easier to identify a victim than an offender? Have the offenders learned how to hide better? Is it because the Police prioritize the identification of victims? Why is there an almost constant increase in the number of open investigations? Is there more pedo-pornographic content than before? Does the Police have more resources than before? Is there greater international cooperation?

Sweden

Despite many hours of work, official statistics on online child sexual abuse in Sweden could not be found. One article mentioned that this was due to the fact that online child sexual abuse is considered a crime against the state. However, no other sources were able to confirm or refute this information. Via ECPACT, some numbers can be found, but none of them were relevant for this work.

Recommendation

The recommendations presented in this section are divided into two main parts. The "General" section is intended for the general public as well as international entities, while the "Police" section is intended for the Belgian and Swedish law enforcement agencies. This section will contain two subsections with specific recommendations for each country.

These recommendations are based on information provided by both countries and are intended as ideas for positive developments in the fight against online child sexual abuse.

General

- Establishment of a centralized European reporting unit for online child sexual abuse content, modelled after NCMEC. This unit would allow for easy reporting of pedophilic content circulating within the European Union.
- Improvement of collaboration between GAFAM (Google, Apple, Facebook, Amazon, and Microsoft) and other platforms. The purpose is to have a better collaboration of those platform regarding the removal of content.
- Complete financial coverage for the psychological follow-up of victims.
- Sensitization of legal guardians and teaching staff to identify abnormal behavioural changes in children.
- Establishment of collaboration between schools and a psychologist to provide care within 24 hours of a student being deemed necessary by a teacher.
- Education of young people on the use of the internet and social networks. Raising awareness of dangers, teaching them how to react in case of problems, and encouraging them to speak up and ask questions if something worries or seems suspicious.

These recommendations should help local law enforcement in their investigations. They will also help to prevent these crimes by educating and raising awareness among the population.

In my opinion, if I could only pick two topics, I would say that the first most important is the education of young people in the use of the internet. It is an affordable recommendation and if they are educated, they will know how to react in case of something would happen to them or someone they know.

The second most important recommendation is the establishment of a centralized European reporting unit for online child sexual abuse. Currently, such reports are provided by NCMEC, but only those platforms with headquarters in the United States, who are subject to American laws, report such offenses to NCMEC. This means that platforms like TikTok are not obligated to send a report to NCMEC. In addition, the reports that NCMEC sends to Europol go through the FBI, which doesn't make sense. In order to distribute content within the European Union, all platforms must either have a headquarters in a European Union country or be represented by a platform that has a headquarters in a European Union country. Thus, all platforms are required to comply with the laws established within the European Union, which includes reporting all content of a pedo-pornographic nature to the competent authority. This recommendation will allow for a centralized service.

Police

The purpose of all the recommendations in this section is to help the Police to be more efficient in their investigation in order to be able to identify more victims and offender.

- Increase staffing for the fight against this phenomenon. Use external experts to the Police when needed. Hire personnel already trained in psychology or computer science.
- Implementation of a platform by country containing all user data related to an IP address or phone number. This platform will be fed by internet and telephony providers.

In my opinion, the use of external experts to the Police could allow for time and efficiency gains. External experts only perform content analysis, whereas Police officers have multiple functions, which is a time-saving measure. Moreover, the expert is potentially more competent since they only have one task to perform, while a Police officer is expected to multitask. The implementation of a platform would also help to gain in time and efficiency, by deleting the intermediaries.

Belgium

- Implementation of a three-level training program: basic, intermediate, and expert. The basic level would be a basic training on internet usage, knowing where and how to observe a specific phenomenon, anonymization, etc. The intermediate level is a slightly higher level, relating to the legal aspect of the internet, approach and contact with victims, reporting methods, etc. The expert level is intended for magistrates and Police officers in charge of online sexual abuse. It covers the specific legal aspects of research, content removal, contact with authors, IVI, etc.
- Increase capacity (personnel and IT tools) in charge of the fight against the phenomenon.
- Legislate to authorize Police services to use all legitimate tools available in favour of victims in order to avoid problems with GDPR and allow the use of AI.
- Have internal personnel capable of developing specific search tools for a phenomenon.
- Establishment of a centralized structure for the removal of illicit content.
- Centralization of services (Child Abuse and Child Focus) within the same building or floor to ensure coordination of investigations, follow-up, and reporting.

In my opinion, legislating to authorize Police services to use all legitimate tools available is the most important. It would increase the number of identified offender and victims. This will also accelerate the speed with which investigations progress. Furthermore, this recommendation does not require any financial invest. Centralization of services is also a very easily implementable recommendation. It will help investigators working faster and will also allow victims to be taken care of in one place, without having to go from one place to another for interrogations, physical examinations, psychological support, and so on.

Sweden

- Mandatory psychological follow-up for all personnel involved in investigations regarding online child sexual abuse.

- Mandatory training for Police officers in online child sexual abuse teams, including victim reception and care, as well as learning about the IT tools at their disposal.
- Transparency of the state and Police services regarding this phenomenon. Public access to statistics and the legal framework and procedures of the Police forces.

In my opinion, Sweden should be more transparent involving online Child Sexual Abuse. By doing this, victims will feel that there's a solution, they can get help. It will also probably be increasing the popularity and the trust in the Police among the population. A mandatory psychological follow-up looks also important. The officers of those units are facing highly violent images, and might not always be aware of the consequences on their health and behaviour.

Conclusion

It is clear that the fight against online child sexual abuse is a crucial issue that requires attention. This phenomenon is constantly evolving and demands that procedures evolve as well. The purpose of this work is to highlight this phenomenon, analyse the current ways of addressing it in Belgium and Sweden, and identify areas for improvement.

Several similarities and differences are observable in both countries. Among the differences, we can note the structure of the Police. The Belgian Police has two distinct entities that collaborate, while the Swedish Police has three distinct entities but is directed by a national commissioner. In terms of sexual consent, the legal age is 16 in Belgium and 15 in Sweden. The software used for visual content analysis also differs, with Belgium using VIZX and Sweden using Griffeye. As for procedures for recovering user data via internet and telephone providers, Belgium has a platform called Tank at its disposal, while Sweden contacts the provider directly. Psychosocial support is mandatory for members of the Child Abuse section in Belgium but not in Sweden.

Both countries also have several points in common. They conduct their online and in-real-life investigations in the same way, perform online undercover operations, and have good diplomatic relations with other countries. They have the same policy concerning procedures for data recovery on servers located abroad and share the same view on the AI project.

It is essential to emphasize that prevention is a crucial part of the fight against online child sexual abuse, and it can be achieved through education and public awareness. Psychosocial support for victims is also a crucial point not to be neglected. If victims know that they will be heard and supported, they will more easily come forward to file a complaint, thus facilitating the arrest of an offender before he or she harms another victim.

Increasing the personnel and technical capacity of Police teams is also a crucial point in the fight against this phenomenon. It can be accompanied by other means such as creating a platform that compiles all user data related to IP and telephone numbers, legislating to authorize investigators to use more efficient computer tools, creating a centralized system for the removal of illicit content, centralizing child abuse prevention services, making psychosocial support mandatory for people involved in these investigations, and training them in welcoming victims and using computer tools.

In the future, it would be good to extend this research to the whole of Europe and compare the procedures and results of different countries to improve these services.

This work has encountered limitations due to the sensitivity of the subject, data confidentiality, and a lack of transparency.

It is important to shed light on this subject in light of the current situation in the Philippines. People from Europe and the United States offer money to impoverished Filipino parents in exchange for sexual acts committed by adults (uncles, parents, etc.) on their children in front of a camera.

In conclusion, this thesis has highlighted the crucial importance of international cooperation, the use of advanced technologies, and public awareness in the fight against online child sexual abuse. I hope that these recommendations will contribute to improving the procedures in place and protecting children worldwide.

I would like to finish my work by sharing with you my frustration about this thesis. I have the feeling that I only discovered a very tiny part of this giant complex problem. As Einstein said once “The more I learn, the more I realise how much I don’t know”¹.

¹ (Albert Einstein, unknown year)

References

- [9] Online on the website of *Europol*: <https://www.europol.europa.eu> accessed on February 6, 7, 9, 10, 12, March 14, 16 and 23, 2023
- [8] Online on the website of *Wikipedia*: <https://www.wikipedia.org> accessed on February 6, 15 and 17, March 16, 19 and 25, 2023
- [1] Online on the website of *Police*: <https://www.police.be> accessed on February 6, March 16, 23 and 25, 2023
- [11] Online on the website of *National Center for Missing and Exploited Children*: <https://www.missingkids.org> accessed on February 15, 16 and 18, and March 2, 2023
- [2] Online on the website of *OSCE POLIS*: <https://polis.osce.org> accessed on February 15 and 27, and March 2, 2023
- [5] Online on the website of *Government offices of Sweden*: <https://www.government.se> accessed on February 15 and March 16, 2023
- [14] Online on the website of *Service Public Fédéral Justice*: <https://www.justice.belgium.be> accessed on March 7, 2023
- [15] Online on the website of *Belgiumlex crossroads bank for legislation*: <https://www.belgielex.be> accessed on March 7, 2023
- [7] Online on the website of *Polisen*: <https://polisen.se> accessed on March 7, 16, 21 and 25, 2023
- [12] Online on the website of *Oracle*: <https://www.oracle.com> accessed on March 14, 2023
- [13] Online on the website of *Binance Academy*: <https://academy.binance.com> accessed on March 14, 2023
- [10] Online on the website of *Interpol*: <https://www.interpol.int> accessed on March 14 and 16, 2023
- [3] Online on the website of *Université de Namur* <https://researchportal.unamur.be> accessed on March 16, 2023
- [4] Online on the website of *Police memorial*: <https://www.policememorial.be> accessed on March 16, 2023
- [6] Online on the website of *Riksarkivet*: <https://www.riksarkivet.se> accessed on March 16, 2023
- [16] Online on the website of *LeMagIT*: <https://www.lemagit.fr/> accessed on May 30, 2023