eu2015lu.eu

EUROPEAN CRIME PREVENTION NETWORK

EUCPN Toolbox Series

No. 8

Preventing cybercrime policies & practices

In the framework of the project '*The development of the observatory function of the European Centre of Expertise on Crime Prevention within the EUCPN*'.
EUCPN Secretariat, April 2016, Brussels

With financial support from the Prevention of and Fight against Crime Programme of the European Union
European Commission – Directorate-General Home Affairs

Preventing cybercrime
Policies & practices

Preface

The eighth toolbox in de series published by the EUCPN Secretariat focuses on the main theme of the Luxembourg Presidency and the 2015 Best Practice Conference, BPC, which is “Prevention of cybercrime”.

The first part of this toolbox presents an overview of the existing policies and legislative measures in the EU and the EU Member States.

The second and third part focusses on the good and promising practices which were submitted by 19 Member States to compete in the 2015 European Crime Prevention Award, ECPA. Special attention is being paid to ‘Children and the Internet’, which is an important issue. Furthermore the winning projects of The Netherlands, Luxembourg and Germany will receive extra attention. In the second part of the toolbox, four participating experts, who were invited by the EUCPN Secretariat, gave their view on the good practices which were presented at the BPC ECPA. Finally, an overview of all submitted ECPA projects can be found in the last part of this toolbox.

Legal notice

Authors/editors

Cindy Verleysen, Research Officer, EUCPN Secretariat, Brussels, Belgium
Febe Liagre, Policy and Practice Officer, EUCPN Secretariat, Brussel, Belgium

Co-authors

Janneke Schilder, Tilburg University, Tilburg, Netherlands
Iris Steenhout, Free University of Brussels, Brussels, Belgium
Maria Sanchez, Prevention and Communication Officer, European Cybercrime Centre (EC3), Europol

EUCPN Secretariat

Waterloolaan / Bd. de Waterloo 76 1000 Brussels, Belgium
Phone: +32 2 557 33 30 Fax: +32 2 557 35 23
eucpn@ibz.eu – www.eucpn.org

Acknowledgements

This toolbox has been developed in a close collaboration between the EUCPN Secretariat[1] and the team of the Luxembourg Presidency, who did a fantastic job in the organization of the 2015 Best Practice Conference and the European Crime Prevention Award. We want to thank the Luxembourg Presidency for providing us with input and experts for the development of this toolbox. Therefore, we are very grateful towards Jean-Marie Wagner, Bob Leesch, Randy Topper and the whole Luxembourg team for their input, support and feedback.

Furthermore, we would like to thank all EUCPN National Representatives, Substitutes and Academic Contact Points for their continuous support of our work, for sharing their expertise and for providing information for this toolbox. We would especially like to thank the National Representatives and Substitutes of the 20 Member States who sent us answers to the questionnaire about cybercrime. These answers form one of the inputs into this toolbox.

Also, we particularly like to thank the four experts who were willing to follow the various sessions during the Best Practice Conference and to contribute to content and the conclusions of this toolbox: Ms. Janneke D. Schilder (Tilburg University, Netherlands), Ms. Maria Sanchez (Prevention and Communication Officer, European Cybercrime Centre (EC3) Europol) and Ms. Iris Steenhout (Free University of Brussels (VUB), Belgium).

Furthermore we are very grateful towards all the participants of the workshop we organized in relation to this toolbox: Janneke D. Schilder (Tilburg University, Netherlands), Marine Smeets (Child Focus, Belgium), Iris Steenhout (VUB, Belgium), Ann Mennens (B-CCentre, Belgium), Yves Vandermeer (FCCU, Belgium), Agnese Krike (Inhope), Sabrina Vorbau (Insafe), Eugene Thomas (Cert.be, Belgium), Maria Sanchez (Europol, Netherlands).

Finally, we would like to thank all the participants of the European Crime Prevention Award 2015. Like in the previous editions of the Best Practice Conference and European Crime Prevention Award competition, we were incredibly touched by all participants' commitment and enthusiasm for the work they are doing day by day and for their willingness to share their experiences with co-workers from all over Europe. You truly are an incredibly source of inspiration for everyone involved in the prevention of and combat against cybercrime. Thank you!

The EUCPN Secretariat

[1] With the financial support of the Prevention of and Fight against Crime Programme of the European Union, European Commission – Directorate-General Home Affairs

Table of contents

PART 3:

Introduction

Technology has become integral to virtually every sector of the global economy, including banking, communications and the electrical grid. The promise of today's interconnected world is immeasurable. The benefits that stem from that promise, face very real threats. As technology's benefits expand and evolve, so too will the threats. Attackers see, in the growing promise of our tech-connected world, opportunities to steal or cause major disruption or destruction by exploiting vulnerabilities. As our world becomes increasingly digitally connected, as social media are playing a key role in our daily life communication, criminals are confronting public order and private safety by new modus of operandi in cybercrime and increasing professionalism.

Cybercrime is a borderless problem, consisting of criminal acts that are committed online by using electronic communications networks and information systems - such as crimes specific to the Internet, online fraud and forgery and illegal online content. Whilst the value of the cybercriminal economy as a whole is not precisely known, the losses are thought to represent billions of euros per year. The scale of the problem is itself a threat to law enforcement response capability – with more than 150,000 viruses and other types of malicious code in circulation and a million people victims of cybercrime every day.

Crime repression may be seen as a one prior response to this criminal threat, but carefully measured strategies in crime prevention may turn out as most effective when tackling cybercrime. The European Commission has designed a coordinated policy in close cooperation with EU Member States and other EU institutions. The role of the EU is above all to support Member States in the cybersecurity issues and to make their actions more efficient. The EU considers that the Member States are in the best position to communicate with the civil society and the private actors and to intervene in case of cyber-incidents.

Because of the big losses, the many victims, the scale of the phenomenon,… it is important to focus on this phenomenon. Therefore this toolbox is being developed: to bring together the efforts made at the EU, national and local level to prevent and combat cybercrime. These include the legislative and policy measures, which set the framework in which national and local actors need to work. At the same time, the toolbox wants to disseminate and promote the important work which is being done by the EU Member States.

The toolbox is primarily written for local policy-makers and practioners who may be confronted with this in their daily work. In the third part some examples of practices implemented in various Member States are further explored. By doing this, the toolbox aims to build up and exchange practical knowledge and know-how and to inspire people working in the field of preventing cybercrime to learn from each other.

Toolbox elements

As usual, the theme of the EUCPN toolbox is explored from various perspectives, bundling as much information and knowledge as possible in an easy-to-read document for policy-makers and practioners.[2] This toolbox in the series consists of three parts.

Thematic paper – the first part of the toolbox is a general introduction to the theme of cybercrime. It builds on existing research and provides information on how legislative and policy measures are developed in the international level and in particular in the EU to prevent cybercrime. It offers the framework for the following parts of this toolbox.

Good and promising practices – this part zooms in on the discussion and conclusions of the Best Practice Conference and the European Crime Prevention Award. Four experts each gave their view on the good practices presented in the Best Practice Conference. Furthermore, some provisional conclusions are drawn up about the positive aspects of the good practices as well as some challenges for the futures.

Examples from practices – one of the aims of the EUCPN is to stimulate the exchange of good practices between Member States. The final part of this toolbox, therefore, contains all 2015 European Crime Prevention Award entries.

[2] For the other EUCPN toolboxes, see: http://www.eucpn.org/library/results.asp?category=32&pubdate=

Part 1 Tackling cybercrime in Europe - legislation, policies and practices

Tackling cybercrime in Europe - legislation, policies and practices

Introduction

The aim of this thematic paper is to give a general introduction to cybercrime and how the EU and its Member States are working (together) to prevent this phenomenon. Furthermore an overview of how prevention and the fight against cybercrime is done by international organizations is given.

In the first paragraph we will give a small word of explanation about the phenomenon 'cybercrime', however we will not go into detail to the theoretical approach. More information on cybercrime as a phenomenon can be found in the Theoretical Paper '*cybercrime: A theoretical overview of the growing digital threat*' produced by the EUCPN Secretariat. The second paragraph provides an overview of how policy and legislative measures have been – and continue to be – developed at the EU level. In this part, a brief history of legislation in Europe will be described. Furthermore, the EU policy will be explained. Also, some initiatives will be mentioned in this part, special attention will go to children and the Internet. In the last paragraph, the various legislative and policy measures of the EU Member States will be discussed.

The focus of this thematic paper is on research and European policy. It offers the broader framework for the toolbox' second and third part in which concrete examples of Member States' existing practices to prevent cybercrime will be discussed.

Cybercrime: a new phenomenon?

European societies are currently increasingly dependent on electronic networks and information systems. The last twenty years, the Internet - more broadly cyberspace - has had a tremendous impact on all parts of our society. Our daily life, our fundamental rights, social interactions and economies depend on information and communication technology working seamlessly. An open and free cyberspace has promoted political and social inclusion worldwide; it has broken down barriers between countries, communities and citizens, allowing interaction and sharing of information and ideas across the globe; it has provided a forum for freedom of expression and exercise of fundamental rights, and empowered people in their quest for democratic and more just societies – most strikingly during the Arab Spring.

While the digital world brings enormous benefits, it is also vulnerable. We have to be aware of the increasing opportunities to commit crime facilitated, enabled or amplified by the Internet. The promise of today's interconnected world is immeasurable. However, the benefits that stem from this promise, face real threats. These threats can have different origins - including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes. Cybercrime is increasing in scale and impact, but there is a lack of reliable figures. However, trends suggest considerable increases in scope, sophistication number and types of attacks, number of victims and economic damage. Cybersecurity incidents, intentional or accidental, are increasing at an alarming pace. They could disrupt the supply of essential services we take for granted such as water, healthcare, electricity,...

[3] **European Commission** (2013), Joint Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels: COM (2013) 01 final, 07 February 2013. [http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52013JC0001]

[4] **European Union** (2014), Cyber Security Strategy and Programs Handbook, Volume 1 Strategic Information and Regulations, p. 113.

For many people, being online is no longer the exception but the norm, often without the individual being aware of the dangers. This creates a broader attack surface and multiple areas of peoples' lives for criminals to exploit.

The definitions of cybercrime have evolved experientially.[5] Cybercrime is a term that most people will still define as hacking or a virus. As of today, cybercrime has grown larger than just the latter; cybercrime is a pervasive threat for today's Internet dependent society. The definitions of cybercrime differ depending on the perception of both observer/protector and victim, and are partly a function of computer-related crimes geographic evolution. The absence of a consistent current definition is a primary problem for the analysis of cybercrime. Cybercrime is a container-concept that holds many different crimes. The definition of cybercrime is extremely wide and interpreted in many different forms.[6] In our quest of finding a global definition of cybercrime, we came across many different interpretations. The most understandable interpretation states cybercrime to be a crime that is enabled by, or that targets computers. With a much broader approach and the specificity of the area in which cybercrimes take place, in particular the Internet, the European Commission defined a more comprehensible version: 'Cybercrimes can be defined as any crimes which are committed via the Internet'.

Like traditional crime, cybercrime has different facets and occurs in a wide variety of scenarios and environments. However, fighting cybercrime requires a different approach from the one traditionally taken in respect of most crimes. In contrast to the off-line world where criminals need to be physically present at the crime scene and can normally commit one offence at a time, criminals in cyberspace do not need to be close to the crime scene, they even do not have to travel to the target country, and can attack a large number of victims globally with a minimum of effort and risk by hiding their identity.[7] Housing billions of gigabytes of sensitive information and valuable data, the Internet is very appealing to criminal organizations, which can act anonymously (and can remain unpunished). The information capabilities of the Internet change the nature of crime, as they provide cyber criminals with simple, cost effective and repeatable means of conducting rapid global-scale attacks, while remaining anonymous and/or unreachable for law enforcement.[8]

A brief history of legislation in Europe

Cybercrime and the fight against cybercrime both get more and more attention. Because of the cross-border characteristic of this phenomenon, plenty of initiatives of different international organizations are established. This international approach is needed, because of the excessive focus on the national laws and a lack of a coordinated approach on national level. This shows once again the fact that the national legislation varies widely around the world. For these reasons, it is appropriate that international fora seek for an effective approach for the strife against cybercrime. In this section we will focus on these initiatives.

[5] **GORDON, S., RICHARD, F. (2006)**, *'On the definition and classification of Cybercrime,' Journal in Computer Virology 2006, Volume 2, Issue 1, pp. 13-20.*
[6] **EUCPN**, Cybercrime - A theoretical overview of the growing digital threat, Brussels, 2016.
[7] **Europol** (2014), The Internet Organised Threat Assessment (iOCTA) 2014, The Hague, 2014.
[8] **CLOUGH**, J., Principles of cybercrime, Cambridge, Cambride University Press, 2010.

Organisation for Economic Co-operation and Development

In the eighties, people started to realize that computers could be an object or tool to criminals. Some countries adapted their legislation and on international level, *the Organisation for Economic Co-operation and Development (OECD)* gave guidelines on which computer acts should be punishable (1986).

> OECD is an organization founded in 1960. The OECD has its Secretariat in Paris and has 34 members. The organization aims to improve economic and social well-being of people worldwide. They provide a forum for governments to share experiences and seek solutions to common problems. www.oecd.org

The OECD was the first international organization that drew guidelines in the fight against cybercrime.[9] The OECD published their final report 'Recommendation Concerning Guidelines for the Security of Information Systems', which recommended a harmonization of criminal laws that penalize computer fraud, computer forgery damage to computer data,… Nevertheless, today cybercrime is no longer a priority to OECD. They focus more on cybersecurity, and promote a global coordinated police approach.[10]

Since 2003, OECD has organized multiple meetings which focused on the combat against malware, spam,…[11] In 2008, the OECD published a report, entitled 'Scoping paper on online Identity theft'. In this report, the OECD recommends the development of adequate law enforcement countermeasures to prevent, detect and combat this phenomenon. This report included an analysis of the different legal approaches adopted by OECD member countries to address Identity theft, and examine the implications of creating a separate criminal offence for Identity theft.[12] In 2009, the OECD published a book on 'Computer viruses and other Malicious Software: a Threat to the Internet Economy'. The OECD insists on a wide range of improvements, such as better legislative framework in the fight against cybercrime and a stronger law enforcement.[13]

United Nations

Beside the OECD, the United Nations, UN, took some initiatives in the fight against cybercrime. In 1989 the 'Guidelines on the Use of Computerized personal Data Flow' were adopted by the UN. In 1994 the UN were at the inception of the 'Manual on the prevention and control of computer-related crime'. Furthermore, in 1997, the United Nations Office on **Drugs and Crime (UNODC)** was established.

The 'Tenth United Nations Congress on the prevention of Crime and the Treatment of Offenders' took place in Vienna in April 2000. At this Congress, cybercrime was broken into two categories and defined as:[14]

- in a narrow sense: any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.

---

[9] **JEWKES, Y., YAR, M.**, *Handbook of internet crime, Devon*, Willan Publishing, 2010, 401.
[10] **CLOUGH, J.**, Principles of cybercrime, Cambridge, Cambride University Press, 2010.
[11] See: www.cybercrimelaw.net/OECD.html
[12] **DEBAETS, A., DEENE, J. and SENEL, N.** *'Cybercriminaliteit'*, in VERMEULEN, G., Aspecten van Europees materieel strafrecht, Antwerpen, Maklu-Apeldoorn, 2002, (381) 393.
[13] **OECD**, *'Computer viruses and Other Malicious Software: A Threat to the Internet Economy'*, 2009, 244p.
[14] **CHAWKI, M., DARWISH, A., KHAN, M.A., TYAGA, S.**, *'Cybercrime, digital forensics and jurisdiction'*, Springer, 2015.

- in a broader sense: any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or disturbing information by means of a computer system or network.

In December 2000, with the signing of the United Nations Convention against Transnational Organized Crime in Palermo (Italy), the international community demonstrated the political will to answer a global challenge with a global response.[15] In this meeting a specific panel focused on 'The Challenge of Borderless Cybercrime'.

The **United Nations Office on Drugs and Crime (UNODC)** is a *United Nations office* that was established in 1997 as the Office for Drug Control and Crime Prevention by combining the United Nations International Drug Control Program (UNDCP) and the Crime Prevention and Criminal Justice Division in the United Nations Office at Vienna. It is a member of the United Nations Development Group and was renamed the United Nations Office on Drugs and Crime in 2002. The office aims long-term to better equip governments to handle drug-, crime-, terrorism-, and corruption-related issues, to maximise knowledge on these issues among governmental institutions and agencies, and also to maximise awareness of said matters in public opinion, globally, nationally and at community level.

The 12th UN Congress on Crime Prevention and Criminal Justice, (Salvador, Brasil, April 2010) had as a theme 'Comprehensive strategies for global challenges: crime prevention and criminal justice systems and their development in a changing world'. One point on this Congress was the international collaboration in the fight against cybercrime. The UNODC prepared a working document in which was suggested to consider the development of a global convention against cybercrime.[16] The UNODC emphasized the importance of a global approach and the need of an international collaboration. They mentioned that the authors of internet crimes are mostly ahead of police and justice authorities by developing new modi operandi. Criminal entrepreneurs can operate relatively efficiently due to the innovation enabled by the Internet. This results in a strife between criminal developers and those who try to foil them. And the differences in national legislation hamper the detection of cyber criminals.[17]

This working document offered opportunities to start negotiations aiming at a global convention on cybercrime. Until that moment, the Convention on Cybercrime of the Council of Europe (see later), was the only international text on cybercrime. The proposal was discussed for 10 days at the 12th UN Crime Congress in Salvador, but ended up a stalemate as Russia, China and a number of developing countries could not reach agreement with the US, Canada, the UK and the EU. This proposal was stymied by disagreements over national sovereignty issues and concerns for human rights. As well, the EU and US position was that a new treaty on cybercrime was not needed since The Budapest Convention on Cyber Crime existed already. Further, the US and UK delegates said any agreement for a UN treaty would take too long to

[15] **United Nations Office on Drugs and Crime**, *'United Nations convention against transnational organized crime and the protocols thereto'*, New York, 2004.
[16] **United Nations**, *'Working paper of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice'*, Salvador, Brasil, 22 January 2010, UN Doc. A/CONF.213/9 (2009) [https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf]
[17] **MASTERS, G.**, *'Global cybercrime treaty rejected at U.N.*, SC Magazine 23 April 2010. [www.scmagazine.com]

resolve.[18] Despite this missed opportunity, the UN remains engaged in cybercrime issues. For example, in 2013 a comprehensive study on cybercrime has been published by the UNODC.

Group of Eight

The Group of Eight, or G8, has taken some initiatives on cybercrime. The first initiatives concerning cybercrime were taken in the late '90's. In '97 a meeting was organized by the Justice Ministers of the P8.[19] In the Lyon-Group[20] a Subgroup on High-Tech crime' was established, that worked on the fight against cybercrime. They held 5 meetings that year and have been meeting regularly since. They focus on enhancing the abilities of law enforcement to prevent, investigate, and prosecute high-tech and computer-related crime.

The Group of Eight: governmental political forum, originally formed by six leading industrial countries and subsequently extended with two additional members – one of which, Russia, has been suspended in 2014. Since 2014, the G8, comprises seven nations and the European Union. Every year, the 'G8' holds an annual meeting where economic and political issues are discussed. Also 'political and safety issues' are part of the scope.

That the G8 deals with cybercrime is not surprising: Members of the G8 lose after all lots of money through cybercrime.

The G8 adopted ten principles and a ten-point action plan to combat high-tech crime in 1997. (see below, page 14)

In the early 2000's the G8 stressed the need for an intensive dialogue between the Governments and the private sector. Furthermore, they also put more focus on combating the sexual exploitation of minors online. As a result of this increased attention to cybercrime, a global campaign against cybercrime was launched and a G8 database was established in which information about cybercriminals was gathered.

In May 2004 in Washington DC, during the G8 top meeting of the Ministers of Justice and Home Affairs, the initiative for a comprehensive legislation as envisaged in the Convention on Cybercrime that would enter into force a month later, were clustered. The communique said in this context: *"To truly build global capacities to combat terrorist and criminal uses of the Internet, all countries must continuously work to improve laws that criminalize misuses or computer networks and that allow for faster cooperation on Internet -related investigations. With the Council of Europe's Convention on Cybercrime coming into force on July 1, 2004, we should take steps to encourage the adoption of the legal standards it contains on a broad basis."*

[18] **MASTERS, G.**, '*Global cybercrime treaty rejected at U.N.*', SC Magazine 23 April 2010 [www.scmagazine.com]
[19] Following 1994's G7 summit in Naples, Russian officials held separate meetings with leaders of the G7 after the group's summits.
[20] Lyon Group: a Senior Experts Group on Transnational Organized Crime established in 1995. This group is known as the 'Lyon Group' since its first report was delivered at the Lyon Summit in 1996.

The ten principles to combat high-tech crime (1997)

1. There must be no safe havens for those who abuse information technologies.
2. Investigation and prosecution of international high-tech crimes must be coordinate among all concerned States, regardless of where harm has occurred.
3. Law enforcement personnel must be trained and equipped to address high-tech crimes.
4. Legal systems must protect the confidentiality, integrity and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.
5. Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.
6. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.
7. Transborder electronic access by law enforcement to publicly available (open source) information does no require authorization from the State where the data resides.
8. Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecution must be developed and employed.
9. To the extent practicable, information and telecommunication systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.
10. Work in this area should be coordinated with the work of other relevant international for a to ensure against duplication of efforts.

Council of Europe

The Council of Europe (CoE) Cybercrime plays a very important role in the fight against cybercrime, because of his Convention on Cybercrime. The Convention on Cybercrime was the first, and until today, the only international treaty aimed at combating cybercrime.

Budapest Convention

In the eighties, the CoE started to pay attention to crimes related to new technologies. In 1989, it published a study and a first set of recommendations addressing the need for new substantive laws criminalizing certain conduct committed through computer networks: 'Recommendation No. R(89) 9 of the Committee of Ministers to Member States on Computer-Related Crime'. This Recommendation aimed to undertake the Member States to take into account its own legislative initiatives to report on computer-related crime. In 1995, the CoE published a second study (Recommendation No. R(95) 13), which contained principles concerning the adequacy of criminal procedural laws in this area.[21]

[21] Both Recommendations are available at www.coe.int and www.cybercrime.gov.

Since these recommendations appeared to be too non-committal, it was decided to draw up a binding Convention, which led to the *Convention on Cybercrime* also known as the *Budapest Convention on Cybercrime, or Budapest Convention*.[22] The drafting of this convention took several years of cooperation between European and International experts. **Its solution was to harmonize cybercrime laws and assure the existence of procedural mechanisms to assist in the successful prosecution of cyber criminals.** Cybercrime is a major global challenge, which required a coordinated international response. The Convention needed to be an effective tool in the global effort to combat computer-related crime. The Convention was developed in response to a growing concern for the adequacy of legislation criminalizing certain activities occurring over computer networks. This convention was adopted by the Committee of Ministers of the Council of Europe on 8/11/2001. It was opened for signature in Budapest in 2001 and was entered into force on 01/07/2004. It was the first international treaty seeking to address Internet and Computer Crime by harmonizing national laws, improving investigative techniques and increasing cooperation among nations. As of March 2016, 48 states have ratified the convention, while six states have signed the convention but not ratified it.

If we keep in mind that the aim was to guarantee a response that provides a broad European support against cybercrime, it is noteworthy that not all Member States of the Council of Europe have signed and/or ratified the Convention. Secondly, it is also apparent that Non-European countries - such as US, Canada, Japan, South Africa - signed the Convention. This means that criminals of cybercrimes can be prosecuted outside Europe. It is striking that the CoE went further than the proposed European support.

Furthermore, organisations such as EU, OECD, were involved also. The European Union considers that the Member States themselves are in the best position to communicate with the civil society and the private actors and to intervene in case of cyber-incidents. If these incidents overtake the borders of a State, the EU has to intervene to coordinate the national authorities. In order to facilitate this cooperation, the European Commission incited the Member States to sign the Budapest Convention on Cybercrime. It is notable how many countries signed and ratified this Convention. Such enthusiasm is easy to clarify: Cybercrime is a global problem. Moreover, many countries recognize the need for a uniform regulatory and the Convention let room for discretion to the Member States.

The Convention aims principally at:
- Harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime.
- Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relations to which is in electronic form.
- Setting up a fast and effective regime of international cooperation.

[22] 23/11/2001 - Council of Europe Convention on Cybercrime (CETS No 185)

Obviously, the Convention contains a list of computer-related crimes. However the criminalization of racist statements was not included in the Convention. Nonetheless, it was initially intended to include content-related offenses[23] in the Convention. For the main reason why the treaty contains no provisions on incitement to racial hatred, unlike pornography, we need to look at the United States. Despite the express wish of the European Countries to ban racist websites in the same way as child pornography, the US refused this ban. This would be unacceptable for the US, because of the First Amendment of the US Constitution, which guarantees 'freedom of speech'. Because of that, the provisions on racist material were excluded from the treaty; nevertheless they were included in an additional protocol of the Council of Europe. On 1 March 2006, the Additional Protocol - making any publication of racist and xenophobic propaganda via computer networks a criminal offence - came into force.[24] Those States who have ratified the Additional Protocol are required to criminalize the dissemination of racist and xenophobic material through computer systems, as well as threats and insults motivated by racism or xenophobia. Currently, cyber terrorism is also studied in the framework of the Convention.

This Convention tried to harmonize the national laws about cybercrime. The Budapest Convention does have quite a range of offenses and investigative powers, with some exception clauses and there is no obligation for countries to join this Treaty. The Budapest Convention is the first International Treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, hate crimes, and violations of network security. Its main objective, set out in the preamble, is **to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation**.

In addition, the Convention includes a provision granting a participating state jurisdiction over offenses committed within that state's territory. This allows a state to assert jurisdiction in a computer crime involving a computer system within its territory, even if the perpetrator committed the offense from a remote location outside the state.
Furthermore, the Convention grants a state jurisdiction over a citizen of that state who commits a covered offense outside of the state's boundaries, so long as the offense is also punishable by criminal law in the jurisdiction where it was committed, or if the offence occurred outside of the territorial jurisdiction of any state. Although the Convention tacitly permits some cross-border access to stored computer data without the need to request mutual assistance, 62 such investigations are only allowed when access to the data is publicly available (open source) or when the state conducting the search has obtained "the lawful and voluntary consent of the person who has the lawful authority to disclose the data.

[23] Content-related offenses encompassed criminal provisions dealing with child pornography and racial hatred.
[24] 28/01/2003 - Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS No 189)

The Convention on Cybercrime provides three general principles of international cooperation:

- First, international cooperation will be provided among states "to the widest extent possible."
- Second, the obligation to cooperate extends not only to the crimes established in the treaty, but also to the collection of electronic evidence whenever it relates to a criminal offense.
- Third, the provisions for international cooperation do not supercede preexisting provisions of international agreements on these issues.

These general principles are reiterated by the mutual assistance provisions. The extradition provisions also defer to preexisting treaties or alternative extradition arrangements between party states.

Convention on the protection of Children against Sexual Exploitation and Sexual Abuse

Another considerable subject with an important cyber dimension is the *sexual exploitation and sexual abuse of children*. There was a need to prepare a comprehensive international instrument focusing on the preventive, protective and criminal law aspects of the fight against all forms of sexual exploitation and sexual abuse of children and setting up a specific monitoring mechanism.

On 25 October 2007 in Lanzarote (Spain), the *Convention on the protection of Children against Sexual Exploitation and Sexual Abuse* was concluded and signed. This Convention is the first instrument to establish the various forms of sexual abuse of children as criminal offences, including such abuse committed in the home or family, with the use of force, coercion or threats. This convention is a multilateral Council of Europe treaty whereby **states agree to criminalise certain forms of sexual abuse against children, to criminalise sexual activity with children below the legal age of consent, regardless of the context in which such behaviour occurs**. It mandates the criminalization of child prostitution and pornography. This Convention sets out several measures to prevent child sexual exploitation and abuse, including the training and educating of children, monitoring of offenders, and the screening and training of people who are employed or volunteer to work with children.

The Convention also establishes programs to support victims, encourages people to report suspected sexual exploitation and abuse, and sets up telephone and internet helplines for children. It also ensures that certain types of conduct are classified as criminal offences, such as engaging in sexual activities with a child below the legal age and child prostitution and pornography. The Convention also criminalizes the solicitation of children for sexual purposes ("grooming") and "sex tourism".

With the aim of combating child sex tourism, the Convention establishes that individuals can be prosecuted for some offences even when the act is committed abroad.

The European Union

For the past 15 years, the EU has made some important efforts to develop an adequate legal framework to address the challenge of cybercrime. Already in the late 90's, the European Commission published a Communication on the illegal and harmful content on the Internet.[25] This was a first attempt trying to develop a legal framework to clarify the rules and regulations governing the liability of access and host service providers. In 1999, an action plan for a safer Internet was published, aiming to foster a favourable environment for the development of the Internet by promoting safe use of the Internet and combating illegal or harmful content.

As mentioned earlier, the year 2001 marked an important date in the fight against cybercrime not only at European, but also at global level, with the Budapest Convention. Because the Convention on Cybercrime remains a key instrument providing minimal legal and procedural standards for fighting cybercrime, the EU, on several occasions, acknowledged the importance of this Convention and encourages the Member States which have not yet ratified it to do this as soon as possible.[26] Since the Budapest Convention was not ratified by all EU Members, the need was felt to set some binding rules for EU Member States for computer crime.

So the European Union also started to work at some legislative acts and instruments. The EU started an internal discussion on a new legal instrument to tackle cybercrime. This discussion ended with the adoption in 2005 of the *Framework Decision on attacks against information systems (2005/222/JHA)*. This Council Framework Decision aimed at establishing minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems. Since this latter Framework Decision, there have been a number of increasingly sophisticated and high-profile cyber-attacks so the EU Council considered that further regulation was needed. On 3 September 2013, *the Framework Decision on 'attacks against information systems'*[27] came into force. This Direction was initially proposed in 2010 as a replacement to the EU Council Framework Decision 2005/222/JHA.[28] The new Framework Decision aims to fight cybercrime and promote information security through stronger national laws, more severe criminal penalties and greater cooperation between relevant authorities. Furthermore, it aims to tackle large-scale cyber-attacks by requiring Member States to strengthen national cybercrime laws and introduce tougher criminal sanctions. However, this Directive introduces some new rules harmonising criminalization and penalties for a number of offences directed against information systems. In addition to new offences and tougher penalties, the new Directive aims to facilitate the prevention of cybercrime by improving co-operation between judicial and other competent authorities. Member States are required to use the existing G8 and Council of Europe structure of 24/7 contact points, with an obligation to answer within eight hours any urgent requests for help. Member States also need to collect

[25] **European Commission (1996)** Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions. Illegal and harmful content on the Internet, Brussels: COM (1996)487, 16 October 1996. [http://publications.europa.eu/en/publication-detail/-/publication/1061a860-7528-4258-a132-cf468e5c22ac/language-en]

[26] **European Commission (2007)**. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions. Towards a general policy on the fight against cybercrime, Brussels: Com(2007) 267 final, 22 May 2007, p. 6. [http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52007DC0267]

[27] DIRECTIVE 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA), Directive on attacks against information systems

[28] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

statistics on cyber-attacks. Although this EU Directive cannot be seen as a panacea for all crimes committed on the Internet, it can be considered as an important tool in the fight against cybercrime.

In contrary to the Convention of Cybercrime, which addresses the fight against cybercrime sensu lato, issues related to content-related crimes (child pornography), computer-related offences (fraud and forgery online) and copyright violations were kept out of the EU Framework Decision and addressed by other legal instruments.[29] With these latter legal instruments, we would like to refer to the following Directives and Framework Decisions:

- The Framework Decision on *'combating fraud and counterfeiting of non-cash means of payment'*[30] (2001), which defines the fraudulent behaviours that EU Member States need to consider as punishable criminal offences. The aim of this framework decision was to supplement the measures already taken by the Council to combat fraud involving non-cash means of payment. In particular, it defines the types of fraudulent behaviour that can be considered to be criminal offences punishable in all EU Member States.
- *Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society.*
- In 2009 there was set up a Directive[31] amending *Directive 2002/22/EC* on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. This *ePrivacy Directive* was created whereby providers of electronic communications services must ensure the security of their services and maintain the confidentiality of client information.[32]
- In 2011, a Directive on *'combating the sexual exploitation of children and child pornography'* was adopted replacing *Council Framework Decision 2004/68/JHA*.[33] The latter Framework Decision (December 2003) had as purpose to approximate the laws and regulations of the Member States in relation to police and judicial cooperation in criminal matters, so as to combat the sexual exploitation of children and child pornography. It aimed at establishing minimum rules concerning the definition of criminal offences and sanctions in the area of child pornography on the Internet. It introduced a Framework of common provisions on criminalization, sanctions, aggravating circumstances, assistance to victims and jurisdiction. The purpose of the Directive *of 13 December 2011 of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography*[34] was to harmonise throughout the EU criminal offences relating to sexual abuse committed against children, the sexual exploitation of children and child pornography.

[29] Council Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography, the Council Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment and Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society.
[30] Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment.
[31] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.
[32] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
[33] Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography
[34] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography. [http://eur-lex.europa.eu/legal-content/EN-NL/TXT/?uri=URISERV:230806_2&from=NL.]

Furthermore, it aimed to prevent pedophiles, already convicted for an offence, from exercising professional activities involving regular contact with children. This Direction addresses the new developments in the online environment better, such as grooming. The Directive lays down minimum sanctions. The new rules include provisions aimed at combating child pornography on-line and sex tourism. This because combating online child sexual abuse is a key part of an EU Directive to tackle the broader problem of child sexual abuse. For example, Article 5(3) lays down a maximum term of at least 1 year of imprisonment for knowingly obtaining access, by means of information and communication technology, to child pornography. Offences and sanctions in the Directive include the solicitation of children online for sexual purposes: proposing, via the Internet, to meet a child for the purpose of committing sexual abuse and, also via the Internet, soliciting the child to provide pornographic material of themselves (Article 6 of the Directive). EU countries must also ensure that child pornography web pages hosted within their territory are promptly removed and must strive to remove those hosted abroad. Furthermore, under certain conditions regarding transparency and Internet user information block access to these web pages in their territory (Article 25).

- On 7th December 2015, the European Parliament and the Council reached an agreement on the Commission's proposed measures to increase online security in the EU. The *Network and Information Security (NIS)Directive*[35] is the first piece of European legislation on cybersecurity. Its provisions aim to make the online environment more trustworthy and to support the smooth functioning of the EU Digital Single Market.[36] The proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union was put forward by the European Commission in 2013. Two years later, the Parliament and the Council have agreed on a set of measures to boost the overall level of cybersecurity in the EU. The new rules will: improve cybersecurity capabilities in Member States, improve Member States' cooperation on cybersecurity, require operators of essential services in the energy, transport, banking and healthcare sectors, and providers of key digital services like search engines and cloud computing, to take appropriate security measures and report incidents to the national authorities.

In summary, Europe gives a basic framework of minimum requirements where the national substantive and procedural criminal law must meet. Certain behaviors and acts with computers should be punishable and the police must be able to carry out certain actions for the investigation in a digital environment. But how exactly this has to be converted into the legal system, is left to the national legislature.

Cybercrime Legislation is particularly a landscape of collaboration based on harmonization of national substantive and procedural law where possible, but especially on legal and practical promotion of legal aid. The EU Framework Decisions set minimum charges in the European Union, but do not go in on investigative powers. In addition, there is a non-binding European policy that aims to help the Member States in to fight against computer crime and adjoining areas. Nevertheless, the role of the European Union is above all to support Member States in the cybersecurity issues and to make their action more efficient.

[35] The original text of the Directive, as proposed in 2013, see: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1666
[36] For more information about the EU Digital Single Market, see: http://ec.europa.eu/priorities/digital-single-market/

Interventions are made by the competent national authorities and the European Union brings mainly a financial support to facilitate the cooperation between States. The International, and particularly European, approach to cybercrime legislation is an attempt to bring the national legislation closer together, but - because of the importance of national sovereignty in the field of criminal law - in many respects there are no international binding regulations.

> *'Given the complexity of the issue and the diverse range of actors involved, centralised, European supervision is not the answer. National governments are best placed to organise the prevention and response to cyber incidents and attacks and to establish contacts and networks with the private sector and the general public across their established policy streams and legal frameworks. At the same time, due to the potential or actual borderless nature of the risks, an effective national response would often require EU-level involvement.'*
>
> Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013)

European policy on the fight against cybercrime

In light of the expeditious increase in cybercrime, the European Commission prepared the ground for a comprehensive policy to tackle cybercrime in 2007.[37] The Commission had identified different particular problems, such as a growing vulnerability to cybercrime risks for society, business and citizens, an increased frequency and sophistication of cybercrime offences, a lack of a coherent EU-level policy and legislation for the fight against cybercrime, a need to develop competence and technical tools (e.g. training and research), the lack of awareness among consumers and others of the risks emanating from cybercrime,… In a communication *'Towards a general strategy on the fight against cybercrime'* the Commission presented a general policy to a better coordination in the fight against cybercrime. The objective was to strengthen the fight against cybercrime at national, European and international level. In the light of identified needs and the limited powers of the European Commission and the European Union in the field of Cybercrime, this policy focuses on actions to improve international cooperation and coordination in general, to reinforce operational cross-border law enforcement cooperation and to strengthen public-private cooperation in the field of fight against cybercrime.

The following actions were planned by the Commission: An improvement of the operational law enforcement cooperation by strengthening and clarifying responsibilities between Europol, Eurojust and other structures. The coordination of training programs for EU countries' law enforcement and judicial authorities involving Europol, Eurojust, the European Police College (Cepol) and the European Judicial Training Network (EJTN).

[37] **European Commission (2007)**. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions. Towards a general policy on the fight against cybercrime, Brussels: Com(2007) 267 final, 22 May 2007. [http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52007DC0267]

Furthermore they wanted a better political cooperation and coordination between the EU Member States by creating a permanent EU contact point for information exchange and an EU cybercrime training platform. Moreover a political and legal cooperation with non-EU countries via the Council of Europe's 2001 Convention on cybercrime, the G8 Lyon-Roma High-Tech Crime Group and Interpol-administered projects was attempted. Also an improved public-private sector dialogue to create mutual confidence and share relevant information seemed an important action, just like the standardization of the legislation and definitions in the area of cybercrime of the EU Member States. The following actions were mentioned: developing measures and indicators of the extent of cybercrime, raising awareness of the dangers and the costs of cybercrime and EU research programs, like for example the Internal Security Fund-Police.

The achievement was a Directive on combating the sexual exploitation of children online and child pornography[38], the *EU's Cybersecurity Strategy*, the establishment of the *European Cybercrime Centre and a Directive on attacks against Information Systems*[39].

Cybersecurity Strategy of the European Union

In February 2013, the High Representative of the Union for Foreign Affairs and Security and the European Commission presented the 'Cybersecurity Strategy of the European Union: An

This Strategy made clear the priorities for EU international cyberspace policy:

- Freedom and openness: the strategy outlines the vision and principles on applying core EU values and fundamental rights in cyberspace.
- The EU's laws, norms and core values apply as much in cyberspace as in the physical world: responsibility for a more secure cyberspace lies with all players within the global information society, from citizens to governments.
- Developing cyber security capacity building: the EU engages with international partners and organisations, the private sector and civil society to support global capacity building in third countries. This includes improving access to information and to an open internet, and preventing cyber threats.
- Fostering international cooperation in cyberspace: preserving open, free and secure cyberspace is a global challenge, which the EU is addressing together with relevant international partners and organisations, the private sector and civil society.

The EU vision presented is articulated in 5 strategic priorities:

- Achieving cyber resilience
- Drastically reducing cybercrime
- Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)
- Develop the industrial and technological resources for cybersecurity
- Establish a coherent international cyberspace policy for the European Union and promote core EU values

[38] See above: a brief history
[39] See above: a brief history

Open, Safe and Secure Cyberspace'.[40] This strategy sets out the EU's approach and vision on the best way to prevent and respond to cyber disruptions and attacks. It was the EU's first comprehensive policy document in this area. It covered the internal market, justice and home affairs and foreign policy angles of cyberspace.

European Agenda on Security for the period 2015-2020

In February 2013, the High Representative of the Union for Foreign Affairs and Security and the European Commission presented the 'Cybersecurity Strategy of the European Union Above the EU Cybersecurity Strategy of the European Union (see above), the *European Commission has set out an European Agenda on Security for the period 2015-2020*[41], to support the Member States' cooperation in tackling security threats and step up our common efforts in the fight against terrorism, organised crime and cybercrime. The European Agenda sets out the concrete tools and measures, which will be used in this joint work to ensure security and tackle these three most pressing threats more effectively.

The Agenda and the Cybersecurity Strategy for the European Union provide the overall strategic framework for the EU initiatives on cybersecurity and cybercrime.

The key objectives of the Commission in the field of cybersecurity:
- Increasing cybersecurity capabilities and cooperation
- Making the EU a strong player in cybersecurity
- Mainstreaming cybersecurity in EU policies

European CyberCrime Center

In 2013, the same year as the publication of the Cybersecurity Strategy of the European Union, the European CyberCrime Center (EC3) was created. In April 2010, in adopting an Action Plan to implement the concerted strategy to combat cybercrime, the Council invited the European Commission to draw up a feasibility study on the possibility of creating a CyberCrime Centre to perform a number of tasks in the fight against cybercrime. Based on this study, published in February 2012[42], on 28 March 2012, the European Commission adopted a Communication 'Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre'.[43] To this extent, it has to be noted that the 2009 Council Decision establishing Europol already conferred to the EU Agency the competence to cover computer crime[44] and that the Europol Organised Crime Threat Assessment, OCTA 2011[45] identified cybercrime as a criminal phenomenon

[40] **European Commission (2013)**. Joint Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels: COM (2013) 01 final, 07 February 2013. [http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52013JC0001]

[41] See: http://europa.eu/rapid/press-release_IP-15-4865_en.htm

[42] **Robinson, N., Disley, E, Dimitris, P., Reding, A., Culley, D., Penny, M., Botterman, M., Carpenter, G., Blackman, C. and Millard, J.**, 'Feasibility study for a European Cybercrime Centre', Final Report, UK, February 2012. [http://ec.europa.eu/dgs/home-affairs/e-library/docs/pdf/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre_en.pdf]

[43] **European Commission (2012)**, Communication from the Commission to the Council and the European Parliament. Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre, Brussels: COM (2012) 140 final, 28.3.2012. [http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/communication_european_cybercrime_centre_en.pdf]

[44] Article 4 of Council Decision 6 April 2009 establishing the European Police Office (Europol) (OJ L 121 of 15 May 2009, p. 37)

[45] **Europol** (2011), 'EU Organised Crime Threat Assessment, OCTA 2011', The Hague, 2011. [https://www.europol.europa.eu/sites/default/files/publications/octa_2011_1.pdf]
Europol (2011), 'Internet Facilitated Organised Crime, iOcta 2011', The Hague, 2011. [https:/www.europol.europa.eu/sites/default/files/publications/iocta_0.pdf]

which required high levels of intelligence coordination and analysis in the framework of law enforcement cooperation in order to gain accurate insight and provide targeted responses.

EC3 is established to strengthen the law enforcement response to cybercrime in the EU and to help protect European citizens, businesses and governments. Its establishment was a priority under the EU Internal Security Strategy. EC3 is situated within Europol, in order that it would be able to draw on Europol's existing law enforcement capacity, but also to expand significantly on other capabilities, in particular the operational and analytical support to Member States' investigations. EC3 focuses on cybercrimes committed by organised groups, particularly those generating large criminal profits such as online fraud, on cybercrimes which cause serious harm to the victim such as online child sexual exploitation and on cybercrimes, including cyber-attacks, affecting critical infrastructure and information systems in the EU. The EC3 provides analysis and intelligence, support investigations, provide high level forensics, facilitate cooperation, create channels for information sharing between the competent authorities in the Member States, the private sector and other stakeholders, and gradually serve as a voice for the law enforcement community.

Main initiatives, funds, projects and organisations in the fight against cybercrime

Above these goals mentioned in the strategy (2007) which are achieved, the many legislative measures, the policy in the fight against cybercrime, there are many other networks, working groups, initiatives taken,… in Europe.

Working groups and Agency's

Coordinate actions between several States is always complex because of the various national habits, policies and laws that often conflict. The goal of these networks and working groups is to overcome the difficulties in order to arrive at a common, harmonized position. This is the case of the *CyberSecurity Coordination Group (CSCG)*, an organization (created in 2011) acting as a single point of contact for pan-European interchange on Cyber Security Standardization and giving a set of recommendations and advices to the Commission and the Member States in the area of Cyber Security Standardization. Additionally, the Coordination Group liaises actively with the European Union Agency for Network and Information Security, ENISA, and the Multi-Stakeholders Platform on ICT Standardization. Most important, the CSCG's efforts towards the harmonization of Cyber Security in Europe are targeted at the high level, aiming to strengthen strategically the European digital economy and to provide a solid security platform for continued growth in Europe's Digital Single Market. The Group focuses on the definition of a European roadmap on Cyber Security Standardization and will actively support global initiatives on cyber security standards that are compliant with EU requirements in view of development of trustworthy ICT products, systems and services

We mentioned already the *European Union Agency for Network and Information Security, ENISA.* ENISA, founded in 2004, is the most important network focusing on cybercrime on

EU-level. ENISA is the centre of expertise that supports the Commission and the EU Member States in the area of information security. They facilitate the exchange of information between EU institutions, the public sector and the private sector. ENISA has the responsibility to support the European Public Private Partnership for Resilience (EP3R), which provide the link between the public and private bodies in Europe. ENISA has been involved in raising awareness through publishing reports, organising expert workshops and developing public-private partnerships. For instance, it is ENISA which permits to set up Cyber-Europe.[46]

ENISA and EUROPOL signed (June 2014) a strategic cooperation agreement to facilitate closer cooperation and exchange of expertise in the fight against cybercrime. The purpose of this agreement is to enhance cooperation between Europol, EC3, and ENISA in order to support the EU Member States in preventing and combating cybercrime. This cooperation includes the exchange of specific knowledge and expertise, elaboration of general situational reports, reports resulting from strategic analyses and best practice and strengthening capacity building through training and awareness raising, to safeguard network and information security at EU level.

In addition to ENISA, at International level, the *EU-US Working Group on Cyber Security and Cybercrime* permits to share the European experiences across the Atlantic and vice-versa. Raising awareness is one of the areas the EU-US Working Group on Cybersecurity and Cybercrime is taking forward, and is also essential in the context of the *Safer Internet Programme*. The Safer Internet Programme funds a network of NGO's active in the field of child welfare online, a network of law enforcement bodies who exchange information and best practices related to criminal exploitation of the Internet in dissemination of child sexual abuse material and a network of researchers who gather information about uses, risks and consequences of online technologies for children's lives.

The European Union also gave rise to the *European Union Computer Emergency Response Team (CERT-EU)* in 2012, consisting of IT security experts from the main European Institutions. The EU Institutions have decided to set up this Team for the EU Institutions, agencies and bodies after a pilot phase of one year and a successful assessment by its constituency and its peers. CERT-EU collaborates when the need arise with the national emergency response teams from the Member States or with private IT security companies.

International Network against CyberHate, INACH, is an organisation dedicated to combatting hate speech, racism and other forms of cyber hate online. The mission is to unite and empower organizations to promote respect, responsibility and citizenship on the Internet through countering cyber hate and raising awareness about online discrimination. Respect for the rights and reputations of all Internet users.

[46] ENISA manages the programme of pan-European exercises, Cyber Europe. This is a series of EU-level cyber incident and crisis management exercises for both the public and private sectors from the EU and EFTA Member States. The Cyber Europe exercises are simulations of large-scale cybersecurity incidents that escalate to become cyber crises. The exercises offer opportunities to analyse advanced technical cybersecurity incidents but also to deal with complex business continuity and crisis management situations. See: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

Funding and projects

With regards to cybercrime 8 projects were funded under the *AGIS programme*[47] and 25 under the *ISEC programme*, (Programme Prevention of and Fight against Crime)[48], for a total amount of €14.760.000. This represents 13,60% of the grand total of all programs. Cybercrime is the second largest A2-funded area behind THB. 'Operational cooperation' accounts for the largest share of the funding with 44,5%, 'training' attracts almost 30% of the funding, 'study and research' 12,3%, 'awareness campaigns a bit less than 7%, 'exchange of information and best practices' 4,5% and 'data collection less' than 2%. The number of projects, and the money which is awarded to them, shows the importance of this topic. Furthermore, the subdivision gives an overview on the priorities of the EU Commission.

To reinforce cybersecurity, the European Union proposes IT prevention projects. A 2009 text from the Commission about the *Critical Information Infrastructure Protection* (CIIP) emphasizes the importance to strengthen cybersecurity, for example through pan European cyber crisis cooperation exercises called Cyber-Europe. Cyber-Europe 2010 gathered 30 States from EU and EFTA – European Free Trade Association), including 22 participants and 8 observers. Cyber-Europe 2012 introduced private actors and European Institutions. 29 States went to that 2012 version, including 4 observers. The 2014 edition claimed to be even more important with nearly 400 cybersecurity professionals and 200 organizations participating. The goal of these actions is to familiarize with cyber-incidents and to improve the trust and cooperation between participants.

Additionally, *the Internal Security Fund (ISF)*, set up for the period 2014-2020, is a fund that must promote the implementation of the Internal Security Strategy, law enforcement cooperation and the management of the Union's external borders. The ISF Police, one component of this fund, must contribute to ensuring a high level of security in the EU and aims at supporting actions addressing internal security challenges, in line with the relevant strategic objectives set by the EU Internal Security Strategy, adopted in 2010. Raising the levels of security for citizens and businesses in cyberspace is one of those objectives.

Finally, one of the most important programs of the EU is called *Horizon 2020*, a research and innovation program of which a part will be devoted to the financing of cybersecurity and to the improvement of the information and communication technologies.

Conferences, events and initiatives

A well-known event is the International Forum on Cybersecurity. This is a platform aiming at promoting a pan-European vision of cybersecurity as well as strengthening the fight against cybercrime. It started in 2007: as the need for proactive response to the fight against cyber criminality became more apparent, the France's National Gendarmerie launched the first

[47] AGIS: Framework programme concerning police and judicial cooperation criminal matters. See: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33177

[48] ISEC has a budget of EUR 600 million for the period 2007–13 and contributes to citizens' security through projects that prevent and combat crime. Terrorism, human trafficking, child abuse, cybercrime, illicit drug and arms trafficking, corruption and fraud are a particular focus. The programme has four key strands: crime prevention, law enforcement, witness protection and support and victim protection.

International Forum on Cybersecurity, FIC.
The annual *Internet Governance Forum*[49] (IGF) is a multi-stakeholder platform that serves to bring people from various stakeholder groups together as equals, in discussions on public policy issues relating to the internet. While there is no negotiated outcome, the IGF informs and inspires those with policy-making power in both the public and private sectors. At the forum, delegates discuss, exchange information and share good practices with each other. The IGF facilitates a common understanding of how to maximise internet opportunities and address risks and challenges that arise. The IGF is also a space that gives developing countries the same opportunity as wealthier nations to engage in the debate on internet governance and to facilitate their participation in existing institutions and arrangements. Ultimately, the involvement of all stakeholders, from developed as well as developing countries, is necessary for the future development of the internet.

European Cyber Security Month is an EU advocacy campaign that promotes cyber security among citizens and advocates for change in the perception of cyber-threats by promoting data and information security, education, sharing of good practices and competitions. The European Union Agency for Network and Information Security (ENISA), the European Commission DG CONNECT and Partners are deploying the European Cyber Security Month (ECSM). This event, linked to prevention, is set up every October since 2012.

On a global level, we would like to mention the *Stop.Think.Connect campaign*[50], which is the first-ever global public awareness campaign developed to help all Internet users keep their data, personal information, communications, and transactions safer and more secure online.

Particular focus on the protection of children in the fight against cybercrime

The EU tries to protect children, who are particularly vulnerable to the dangers of the Internet. The Digital Single Market Strategy aimed to have every European digital. Therefore, we need to take in account that children have particular needs and vulnerabilities on the Internet, which must be addressed specifically so that the Internet becomes a place of opportunities for children to access knowledge, to communicate, to develop their skills and to improve their job perspectives and employability . Therefore online safety for children needs to be guaranteed. As mentioned before, the EU has created several legislative measures to protect especially children in the fight against cybercrime.

In November 2011, the *Council Conclusions on the Protection of Children in the Digital World* highlighted that a combination of policies is required to deliver a Better Internet for Children. Actions are developed at National, European or Sectoral level. They need to be included in an EU-wide strategy, which develops baseline requirements and avoids fragmentation. Regulation remains an option, but, where appropriate, it should preferably be avoided, in favour of more

[49] See: http://www.intgovforum.org/cms/
[50] See: http://www.stopthinkconnect.org/
[51] Key priorities of the EU e-Skills strategy 'e-Skills for the 21st century' COM (2007)496.
[52] The Convention on the protection of Children against Sexual Exploitation and Sexual Abuse, Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, the Directive of 13 December 2011 of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography

adaptable self-regulatory tools, and of education and empowerment.
In September 2012, the EU worked out a *Strategy for a Better Internet for Children*[53]. Because children are increasingly exposed to the Internet at a younger age, through a growing range of devices, the EU thought it was necessary to develop a proper strategy to encapsulate their needs. This strategy brings together the European Commission and Member States with mobile phone operators, handset manufacturers and providers of social networking services to deliver concrete solutions for a better Internet for children. This strategy aims to give children the digital skills and tools they need to fully and safely benefit from being online. It also aims to unlock the potential of the market for interactive, creative and educational online content. The strategy proposes a series of actions grouped around the following main goals:

Safer Internet Day, SID, is organised by Insafe (see later) in February of each year to promote safer and more responsible use of online technology and mobile phones, especially among children and young people across the world.

- Stimulate the production of creative and educational online content for children as well as promoting positive online experiences for young children
- Scaling up awareness and empowerment including teaching of digital literacy and online safety in all EU schools
- Create a safe environment for children through age-appropriate privacy settings, wider use of parental controls and age rating and content classification
- Combat child sexual abuse material online and child sexual exploitation

The tasks will be carried out, mainly through the implementation of the *Connecting Europe Facility*, the instrument for co-funding the digital service infrastructure for making a better internet for children, but also through other programmes such as H2020.

In December 2012, a *Global Alliance against Child Sexual Abuse Online* was launched: this Alliance was a joint initiative by the EU and the US, gathering 54 countries from around the world to fight together Child Sexual Abuse. This Alliance is a vehicle for further actions from the Member States supported by the Commission and the EC3. In his Cybersecurity Strategy (2013) the Commission asks Europol, EC3, to initially focus its analytical and operational support to Member States' cybercrime investigations, to help dismantle and disrupt cybercrime networks primarily in the areas of child sexual abuse, payment fraud, botnets and intrusion.

The work on the harmful effects of the Internet for children, is already supported financially since 1999 through special programmes. *The Safer Internet Programme* aims at empowering and protecting children and young people online by awareness raising initiatives and by fighting illegal and harmful online content and conduct. It launches calls for proposals to select and finance projects aimed at creating a safer online environment for young people. This programme funds a network of NGO's active in the field of child welfare online, a network

[53] **European Commission**, '*Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European Strategy for a Better Internet for Children.*'

of law enforcement bodies who exchange information and best practices related to criminal exploitation of the Internet in dissemination of child sexual abuse material and a network of researchers who gather information about uses, risks and consequences of online technologies for children's lives.

The first Safer Internet Programme was launched in 1999 in order to support projects and events, as well as to promote industry self-regulation and international co-operation.
Following the adoption (2012) of the earlier mentioned European Strategy to Make the Internet a Better Place for Children, it became known as *Better Internet for Kids, BIK*. Over the years, the activities covered awareness raising, fighting illegal content, filtering and content labelling, involving the civil society in child online safety issues and creating a solid database of information related to the use of new technologies by young people. The *Global Safer Internet Day* and *Safer Internet Forum* are annual events, associated with this programme. The continuation of this programme, is provided under 'Connecting Europe Facility'.

An important part of this programme is the *Safer Internet Centres (SIC)*, which are present in 30 European countries. They give advice and information to children, parents and teachers. In addition, these centres host hotline services which receive reports on online illegal content, this brings us to *INHOPE*.[54]

INHOPE, an active and collaborative network of 51 hotlines in 45 countries worldwide[55], dealing with illegal content online and committed to stamping out child sexual abuse from the Internet, is worth giving an extra word of explanation. The International Association of Internet Hotlines was founded in 1999, with funding and support from the European Commission under the Safer Internet Programme.

Safer Internet Forum, SIF, is a key annual international conference in Europe where policy makers, researchers, law enforcement bodies, youth, parents and carers, teachers, NGOs, industry representatives, experts and other relevant actors come together to discuss the latest trends, risks and solutions related to child online safety.

The Hotlines offer the public a way of anonymously reporting Internet material, they suspect to be illegal, including child sexual abuse material. This Hotline will ensure that the matter is investigated and if found to be illegal the information will be passed to the relevant Law Enforcement Agency and in many cases the Internet Service Provider hosting the content. The key functions of this Network are: exchange expertise, support new hotlines, exchange reports, interface with relevant initiatives and educate and inform policy makers at the International level. The goals of INHOPE: establish and support effective national hotlines, to train and support new Hotlines, to foster ongoing Internet Safety awareness and education and the establishment of effective common procedures for receiving and processing reports.

INHOPE works together with *INSAFE*, through a network of SICs across Europe – typically comprising an awareness centre, helpline, hotline and youth panel.

[54] See: http://www.inhope.org/gns/home.aspx
[55] For a full list of member Hotlines: http://www.inhope.org/gns/our-members.aspx

Safer Internet Centres, SIC, (www.betterinternetforkids.eu/) raise awareness regarding online risks amongst children, parents, teachers and caretakers. They are made up of awareness centres, helplines *(INSAFE)* and hotlines *(INHOPE)* and a youth panel, and are present in all the Member States, Iceland, Norway and Russia. Main activities of the SIC:

- *raising awareness related to potential risks young people may encounter online*
- *offer advice to young people about staying safe online and dealing with issues such as cyber bullying, via the helplines.*
- *develop information material*
- *organize events such as the Safer Internet Day, their biggest yearly international event*
- *organize information sessions for parents, children and teachers.*
- *set up youth panels (http://paneuyouth.eu/youth-panels/pan-eu-youth-panel/) to be consulted for the development of awareness raising activities, material and campaigns.*

Each year, every national SIC invites one of their national youth panelists to attend the Pan-European Youth Panel. Here, young people between 12 and 18 years old, are brought together to discuss current issues related to Internet and modern media. As a participant in the Pan-EU Youth Panel, you can get the opportunity to inform the Awareness Centres, industry representatives, policy makers and other interested parties how young people today are using digital media and to identify the risks, benefits and the issues around internet safety that matter to you and your friends the most.

INSAFE[56], the *European Network of Awareness Centres* is a key contributor of the Safer Internet Programme. They promote a safer and better use of Internet. Its mission is to empower citizens - children and young people - to use the Internet, the mobile phone, as well as other online technologies, positively, safely and effectively. The Insafe Network, founded in 2006, and comprised of 30 national awareness centres (27 Member States, Iceland, Norway and Russia), develops materials, organise campaigns and deliver information sessions for children, young people, parents, caretakers, teachers and social workers to enable children and young people to make positive use of online technologies, and develop their own strategies for staying online. They want to raise awareness about reporting harmful or illegal content and services. Particular emphasis is given towards the elimination of child pornography.

Insafe partners work closely together to share best practice, information and resources. The network interacts with industry, schools and families in the aim of empowering people to bridge the digital gap between home and school and between generations. Insafe partners monitor and address emerging trends, while seeking to reinforce the image of the web as a place to learn. Through close cooperation between partners and other actors, Insafe aims to raise Internet safety-awareness standards and support the development of information literacy for all.

[56] More information, resources and best practices on www.betterinternetforkids.eu/.
[57] Safer Internet Center, see above.

Each country in the Insafe network has a *National Awareness Centre*[57] which is responsible for implementing campaigns, coordinating actions, developing synergy at the national level, and working in close co-operation with all relevant actors at European, regional and local level. Members of the Insafe Network provide helplines where parents and children can obtain advice, information and assistance on online safety issues that may be causing them concern, how to deal with harmful content, harmful contact (grooming) and harmful conduct (cyberbullying or sexting). The helplines can increasingly be accessed via a variety of means: telephone, email, web forms, Skype and online chat services. Additionally, an important aspect for this network is the youth participation, giving young people a chance to have their voices heard about the technology issues that matter to them.

The European Schoolnet coordinates the Insafe Network. This Schoolnet has also set up the *eSafety Label*, a European-wide accreditation and support service for schools. The aim is to develop and maintain high standards of eSafety in schools across Europe. The services include a system of accreditation, self-assessment, and personalised action plan, a wide range of resources on eSafety advice and guidance, and an online community for user to exchange ideas and experiences.

Better Internet for Children 'www.betterinternetforkids.eu' is an easy to use platform. The website is a gathering of good practices. It focuses on:

- Awareness: national awareness centres focus on raising awareness and understanding of safer Internet issues and emerging trends. They run campaigns to empower children, young people, parents, teachers with the skills, knowledge and strategies to stay safe online and take advantage of the opportunities that internet and mobile provides
- Helplines: provide information, advice and assistance to children, youth and parents on how to deal with harmful content, harmful contact (such as grooming) and harmful conduct (such as cyberbullying or sexting). Helplines can increasingly be accessed via a variety of means – telephone, email, web forms, Skype and online chat services. http://helplines.betterinternetforkids.eu
- Hotlines: a mechanism that allows any member of a public to report suspected illegal content online (core focus on child sexual abuse material). The hotline will ensure that the matter is investigated and if found to be illegal the information will be passed to the relevant Law Enforcement Agency and where appropriate Internet Service Provider. INHOPE is a membership association/an umbrella organisation bringing hotlines together to combat child sexual abuse material online.
- Industry: Industry partners are key stakeholders in the Better Internet for Kids agenda, working with the European Commission and Safer Internet Centres across Europe to ensure that products and services are safer by design, and that appropriate measures and responses can be given to any issues identified. Many industry partners also develop awareness-raising campaigns and materials. Child Focus has also contact with different companies.
- Research: Research partners are key stakeholders in the Better Internet for Kids (BIK) agenda, providing a body of knowledge and evidence on issues affecting children and young people online today. Armed with this knowledge, we are able to identify emerging trends and shape appropriate responses and create effective resources for the challenges presented.
- Youth: the participation of the youth in the Better Internet for Kids agenda allows young people to express their views and exchange knowledge and experiences concerning their use of online technologies, as well as tips on how to stay safe. They also advise on Internet Safety and empowerment strategy, help create innovative resources and disseminate eSafety messages to their peers.

In the Resources Catalogue you can find resources available from all the countries of the Network (videos, games, …). The Better Internet for Kids guide to online services aims to provide key information about some of the most popular apps, social networking sites and other platforms which are commonly being used by children and young people and adults today.

As described in this part of the Toolbox, there are already many International and European initiatives which have the purpose to fight and prevent Cybercrime. However, the EU Member States remain the ones who have to adopt measures to enforce these rights and to make the fight effective. In the next part, we will look at what the different EU Member States do to prevent and fight Cybercrime.

The EU tries to protect children in particular, because they are vulnerable to the dangers of the Internet. Since a lot of the BPC-ECPA projects focused on children and/or youth, it became clear that the Member States just like Europe gives a particular attention to this vulnerable group.

Legislative and policy measures in the EU Member States

After looking at the different International and European weapons against cybercrime, we will now look at what the EU Member States do with these international and European conventions and legislations. This is especially important since the conventions are general guidelines. It is up to the MS to implement them into their policies and their legislation. As already discussed in the previous part, almost all countries have ratified the Budapest Convention.

Members of Council of Europe	Signature	Ratification	Entry into Force
Albania	23/11/2001	20/06/2002	01/07/2004
Andorra	23/04/2013		
Armenia	23/11/2001	12/10/2006	01/02/2007
Austria	23/11/2001	13/06/2012	01/10/2012
Azerbaijan	30/06/2008	15/03/2010	01/07/2010
Belgium	23/11/2001	20/08/2012	01/12/2012
Bosnia and Herzegovina	09/02/2005	19/05/2006	01/09/2006
Bulgaria	23/11/2001	07/04/2005	01/08/2005
Croatia	23/11/2001	17/10/2002	01/07/2004
Cyprus	23/11/2001	19/01/2005	01/05/2005
Czech Republic	09/02/2005	22/08/2013	01/12/2013
Denmark	22/04/2003	21/06/2005	01/10/2005
Estonia	23/11/2001	12/05/2003	01/07/2004
Finland	23/11/2001	24/05/2007	01/09/2007
France	23/11/2001	10/01/2006	01/05/2006
Georgia	01/04/2008	06/06/2012	01/10/2012
Germany	23/11/2001	09/03/2009	01/07/2009
Greece	23/11/2001		
Hungary	23/11/2001	04/12/2003	01/07/2004
Iceland	30/11/2001	29/01/2007	01/05/2007
Ireland	28/02/2002		
Italy	23/11/2001	05/06/2008	01/10/2008
Latvia	05/05/2004	14/02/2007	01/06/2007
Liechtenstein	17/11/2008	27/01/2016	01/05/2016
Lithuania	23/06/2003	18/03/2004	01/07/2004
Luxembourg	28/01/2003	16/10/2014	01/02/2015
Malta	17/01/2002	12/04/2012	01/08/2012
Moldova	23/11/2001	12/05/2009	01/09/2009
Monaco	02/05/2013		
Montenegro	07/04/2005	03/03/2010	01/07/2010
Netherlands	23/11/2001	16/11/2006	01/03/2007
Norway	23/11/2001	30/06/2006	01/10/2006

Members of Council of Europe	Signature	Ratification	Entry into Force
Poland	23/11/2001	20/02/2015	01/06/2015
Portugal	23/11/2001	24/03/2010	01/07/2010
Romania	23/11/2001	12/05/2004	01/09/2004
Russia			
San Marino			
Serbia	07/04/2005	14/04/2009	01/08/2009
Slovakia	04/02/2005	08/01/2008	01/05/2008
Slovenia	24/07/2002	08/09/2004	01/01/2005
Spain	23/11/2001	03/06/2010	01/10/2010
Sweden	23/11/2001		
Switzerland	23/11/2001	21/09/2011	01/01/2012
Former Yug. Rep. of Macedonia	23/11/2001	15/09/2004	01/01/2005
Turkey	10/11/2010	29/09/2014	01/01/2015
Ukraine	23/11/2001	10/03/2006	01/07/2006
United Kingdom	23/11/2001	25/05/2011	01/09/2011

Non-Members of Council of Europe	Signature	Ratification	Entry into Force
Argentina			
Australia		30/11/2012	01/03/2013
Canada	23/11/2001	08/07/2015	01/11/2015
Chile			
Colombia			
Costa Rica			
Dominican Republic		07/02/2013	01/06/2013
Israel			
Japan	23/11/2001	03/07/2012	01/11/2012
Mauritius		15/11/2013	01/03/2014
Mexico			
Morocco			
Panama		05/03/2014	01/07/2014
Paraguay			
Peru			
Philippines			
Senegal			
South Africa	23/11/2001		
Sri Lanka		29/05/2015	01/09/2015
Tonga			
United States of America	23/11/2001	29/09/2006	01/01/2007

Table 1: Chart of signatures/ratifications of Convention on Cybercrime. Status on March 2016[58]

As of March 2016, 48 states have ratified the Budapest convention, while six states have signed the convention but not ratified it. Nevertheless, since all countries are themselves responsible for the implementation, this has a consequence that there can be much variation between the *policies and legislation of different countries*.

[58] See: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

To address the question to the various policy and legislative measures by the EU Member States, the EUCPN Secretariat sent out a questionnaire to all Member States. The underneath analysis is based on the information obtained through the questionnaire. 15 EUCPN National Representatives filled in the questionnaires. To receive a more complete image of this topic, we supplemented this information with information we found in literature.[59]

In this questionnaire, we asked if cybercrime is a priority in their country, which is mostly positive answered. Because most of the Member States ratified the Budapest Convention, but still are responsible for the implementation, we asked them to give us more information about their legal framework for Cybersecurity.

State	Answer
Austria	The legal situation regarding criminal offences in the core area of cybercrime is based on the translation of the Convention on Cybercrime. CETS No.185 (2002), the Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems (2008) and the Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (2016) into national law. Therefore, the main cybercrime offences in the Penal Code are the unlawful access to a computer system (Sec. 118a PC), the unlawful interception of data (Sec. 119a PC), the damaging of data (Sec. 126a PC), the interference with the functioning of a computer system (Sec. 126b PC) and the misuse of computer programs or access data (Sec. 126c PC). In general, it is an aggravating circumstance if an offence is committed by misusing the personal data of another person. Aside of that, there is a law waiting for adoption regarding the NIS-Directive. It will be named “IT-Sicherheits Gesetz” (IT-Security law). Our law will be almost equivalent to the german “IT-Sicherheits Gesetz”.
Belgium	Belgium has a law on cybercrime, which is focused on more general offences (fraud and cybersecurity)
Bulgaria	Under the national legislation cybercrimes are dealt with in Chapter “IX A” of the Criminal Code of the Republic of Bulgaria, “Computer Crimes”, incl. Art. 319a - 319e, the Law on Copyright and Related Rights, the Law on Marks and Geographical Indications NIPIES (National System for the exchange of information in the field of intellectual property) the Gambling Act. Coordination is carried out by Europol within the already established ties with the European Cybercrime Centre. Since 2007 activities were implemented within the “Check the Web” project of Europol, which continue after the transformation of the project and its expansion to в Internet Referral Unit;
Czech Republic	Sec. 7 of Act No. 418/2011 Coll., on the Criminal Liability of Legal Persons and Proceedings against Them, stipulates that legal persons are criminally liable for the following offences from the Criminal Code (including offences in the field of cybercrime): • *Section 182 Breach of Secrecy of Correspondence;* • *Section 230 Unauthorised Access to Computer Systems and Information Media;* • *Section 231 Obtaining and Possession of Access Device and Computer System Passwords and other such Data;* • *Section 232 Damage to Computer Systems and Information Media Records and Interference with Computer Equipment out of Negligence;* • *Section 209 Fraud;* • *Section 192 Production and other Disposal with Child Pornography;* • *Section 193 Abuse of a Child for Production of Pornography;* • *Section 193a Participation in a pornographic production;* • *Section 193b Establishing illicit contacts with children;* • *Section 201 Endangering a Child´s Care*
Estonia	As a country that is largely dependent on the Internet, cybersecurity and the fight against cybercrime are key priorities in Estonia. At the same time, special attention is paid to the protection of fundamental rights and freedoms and responsible Internet governance. There is a robust legal framework in place in Estonia, with substantive criminal law covering the full range of offences related to cybercrime, including the illegal use of another person’s identity which is also provided for in the Penal Code. The Penal Code is kept under review and amended as new trends emerge. Estonia has implemented the Freezing Order Framework Decision, the Framework Decision on attacks against information systems and the Confiscation Order and the Directive on combating sexual abuse and sexual exploitation of children and child pornography and expects to ratify the Lanzarote Convention in 2018. Estonia is party to the Budapest Convention, and other relevant Council of Europe Conventions, UN Conventions, EU instruments on MLA.

[59] See: http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf
See: www.enisa.europe.eu

State	Answer
France	Cybercrime is a priority in France. The Prime Minister conducts the French cyber security policy and sets out the rules regarding the enforcement of the security of the information systems. All French authorities are in charge of cyber security, there is no specific cybercrime on which France focuses.
Germany	During the past 2 years, the organizational structure of the law enforcement authorities has been adjusted to fit the changing information technology landscape. For the German Federal Criminal Police Office (Bundeskriminalamt), almost every criminological phenomenon is affected by the use of the internet and modern information technology. There is a distinction between Cybercrime and the general usage of information technology to commit any kind of crime mentioned in the German Criminal Code. Cybercrime is defined as crime which cannot be committed without the usage of computers and which always targets information technology or digital data. These crimes are defined in the German Criminal Code as follows: Section 202a Data espionage, Section 202b Phishing , Section 202c Acts preparatory to data espionage and phishing , Section 202d Handling stolen data, Section 263a Computer fraud , Section 269 Forgery of data intended to provide proof, Section 270 Meaning of deception in the context of data processing, Section 303a Data tampering, Section 303b Computer sabotage. For the Criminal Code sections, a Cybercrime subdivision was set up within the “Serious and Organised Crime” Division in the organisational structure of the German Federal Criminal Police Office (BKA). Other crimes committed using IT/ computers (e.g. eBay fraud, sextortion, drug trafficking over the internet) are handled within the competent subdivisions, with professional support from the Cybercrime subdivision if necessary. Alongside the law enforcement agencies, the Federal Office for Information Security was established in ‘91. This federal agency is in charge of managing computer and communication security for the German government. Its areas of expertise and responsibility include the security of computer applications, critical infrastructure protection, internet security, cryptography and the certification of security products. Alongside the sections of the Criminal Code for tackling Cybercrime, the IT Security Act was introduced in July 2015, focussing on the improvement of security in information technology and the protection of critical infrastructure. This Act is the most specific framework dealing with Cybersecurity, but there are other legal frameworks which contain partial sections dealing with Cybersecurity.
Greece	Established a special legislative committee to ratify the Budapest Treaty, signed on 23.11.2001, but not yet ratified. Furthermore, this committee's work includes the transposition of the Directive 2013/40/EU “on attacks against information systems”. It is expected that the committee’s draft will be delivered soon.
Hungary	The basic values are enshrined in the **Fundamental Law** of Hungary specifically freedom, security, rule of law, international and European cooperation, in a separate field within security and economic policy. The special act for Cybersecurity is **Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies**.
Italy	Following the adoption of the Prime Minister’ “Decree Containing Strategic Guidelines for the National Cyber Protection and ICT Security” of the 24th January 2013, the Cybersecurity Working Group was established on the 3rd of April 2013 under the auspices of the Committee for the Security of the Republic, Chaired by the Department for intelligence and Security (DIS), and developed this National Cybersecurity Strategy Framework. The Cybersecurity Working Group saw the active participation of all the Administrations already represented in the Committee for the Security of the Republic (Ministries of Foreign Affairs, Interior, Defence, Justice, Economy and Finance, Economic Development), and included the Agency in charge for the Italian Digital Agenda as well as the Cybersecurity Unit within the Prime Minister’s Office. The point of departure of this National Cybersecurity Strategic Framework was, in 2013, an assessment of current’s cyber threat. Italy has dedicated law quite to all cybercrime’s fields, but in case of need in the preamble of the Decree of 24.01.2013[60], was listed the most relevant legislative acts. According to Budapest Convention Article 35[61] Italy has designated as SPOC the National Cybercrime Centre for Critical Infrastructures Protection. In relation to cyber terrorism, in particular art. 7a Anti –terrorism Law N.155 (of 31 July 2005) established the competences falling on the Ministry of the Interior and its subordinate Postal and Communications Police Service, with focus on undercover investigations on cyber terrorism and Preemptive interceptions. In relation to child sexual exploitation and crime related, Law 3 August 1998 n. 269 and Minister of the Interior Decree, January 19, 1999 Law n. 38 of 6 February 2006, established the exclusive competence of the National Centre for combating on line child pornography.
LUX	The LU Penal Code covers this issue by several articles.

[60] See: http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2013-03-19&atto.codiceRedazionale=13A02504&elenco30giorni=true

[61] 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-days-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

State	Answer
NL	NL is preparing a new bill of law on cybercrime. The new law is intended to take measures to address the rapid developments in the field of technology, internet and cybercrime, in order to e.g. undo data encryption, deal with illegal actions on the internet or fight child pornography online. The proposed bill will introduce legislation on: • the performance by the police and judicial authorities of remote investigations of computers of criminals within the Dutch jurisdiction and, if necessary, copy data or make the data inaccessible. It concerns the 'investigation in an automated work' which provides investigators with the authority to perform various investigative actions, subject to stringent conditions, when investigating serious offences. This may involve, under circumstances transborder access to data. • the possibility to oblige persons suspected of possessing and disseminating in child pornography or of terrorist activities to cooperate in opening encrypted files on their computer. The public prosecutor will then issue a so-called decryption order to the suspect. The police and judicial authorities will then obtain access to protected data. Here too, there are stringent safeguards, including prior court review. Ignoring a decryption order from the public prosecutor is punishable by a prison sentence. • the criminalization of handling stolen computer data. The minister wants to prevent that e.g. third parties receive stolen information from hacked computers and subsequently place it on the internet. • the criminalization of repeated online markets' fraud. • the "grooming" of children, creating the possibility of investigating these crimes by undercover policemen. The Netherlands are currently preparing a law for the full implementation of EU Directive 2013/40 on attacks on information systems. The Dutch law is already largely consistent with this directive, for example the criminal offences are already laid down in the Dutch Criminal Code by earlier revisions of Dutch law in 1993 and 2006. The new legislation will primarily increase the penalties for certain offences. Specifically, the minimum penalties are increased. The punishments of certain offences to a maximum sentence of two years will be regulated. Moreover, 3 aggravating circumstances will be added. The sentence will be increased to a maximum of three years if a botnet is used when committing the offence, and to five years if it causes serious damage or is directed against vital infrastructure. Internationally, the Netherlands assumes a vanguard role in harmonizing legislation governing international investigations, for instance in the Council of Europe.
Romania	Romania ratified the Budapest Convention and transposed its provisions into the national legislation through the Law 161/2003. Since February 1st cybercrime is foreseen in the Criminal Code (a new Criminal Code came into force on February 1st). The legal framework focuses on: • Crimes committed against an information system • Crimes committed with the help of an information system • payment crimes • Child pornography
Slovakia	Although the law does not recognize the term "cybercrime", current criminal legislation (§ 122 paragraph 2 point a) of Act no. 300/2005 Coll. Penal Code) defines a crime committed as a public as an offense which is committed through a computer network. Penal Code takes into account the recommendations and commitments made by the Slovak Republic resulting from the Convention on Cybercrime. Accordingly, following articles of the Convention on cybercrime are considered as cybercrime: Article 2 – Illegal access Article 3 – Illegal interception Article 4 – Data interference Article 5 – System interference Article 6 – Misuse of devices Article 7 – Computer-related forgery Article 8 – Computer-related fraud Article 9 – Offences related to child pornography Article 10 – Offences related to infringements of copyright and related rights
Slovenia	At the moment cybercrimes are defined in the Criminal Law and some procedures in our Criminal Procedure Code.

Policymakers of the Member States have a key role to play in ensuring that both public and private entities are well equipped to face the cybersecurity challenges of an ever more connected world. They can achieve this by establishing appropriate legal and policy frameworks, and through promoting cybersecurity awareness and cooperation with the different actors involved in working towards cyber resilience. A strong Cybersecurity Strategy is critical for managing national level cyber risks and developing appropriate legislation to support these efforts. Therefore we asked the Member States if they have a *national cybersecurity strategy*, in what year it was adopted and if possible to receive more information about their strategy.

State	No	Yes	Answer
Austria		X	Adopted in 2013. https://www.bka.gv.at/site/3327/Default.aspx https://www.bka.gv.at/DocView.axd?CobId=50999 It is a part of a broader ICT security initiative of the Austrian government, as set out in the National ICT Security Strategy 2012.[62]
Belgium		X	Adopted in 2012. https://www.b-ccentre.be/belgium-has-national-cyberstrategy/ The legal framework for cybersecurity remains somewhat unclear, and the information available on the implementation of the strategy is limited.[63]
Bulgaria	X		A final draft of such strategy has been developed, which will be discussed by the Council of Ministers. The legal framework for cybersecurity in Bulgaria is limited.[64]
Croatia	X		
Cyprus		X	Adopted in 2013. It includes a commitment to update key elements of the legal framework for cybersecurity.[65]
Czech Republic		X	Adopted in 2011, for the period 2011-2015. On 16th February 2015, a new National Cyber Security Strategy was adopted for the period '15-'20, hereinafter as 'Cyber Security Strategy'. This strategy is followed by the ***Action Plan***. The ***Action Plan*** specifies tasks, competence and the time frame for meeting the objectives set out in the Cyber Security Strategy including combating cybercrime. http://www.govcert.cz/en/info/strategy-a-action-plan/
Denmark		X	Presented in December 2014 a National Cyber and Information Security Strategy, containing 27 government initiatives for 2015 – 2016.[66]
Estonia		X	Was one of the first countries to develop a national cybersecurity strategy (2008), followed by the release of the updated strategy in 2014 (period 2014-2017). Objective of latter strategy: increasing the capacity of the state in the area of cyber security and raising the awareness of the population of cyber risks. Estonia has a wide range of legislation that covers information security and cybersecurity. https://www.mkm.ee/en/objectives-activities/information-society/cyber-security
Finland		X	Published in 2013. This is complemented by a strong overall legal framework encompassing a range of important cybersecurity issues.[67]

[62] See: http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf
[63] See: http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf
[64] See: http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf
[65] See: http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf
[66] See: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/danish-cyber-and-information-security-strategy/view
[67] See: http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf

State	No	Yes	Answer
France		X	Since 2008, France drafted 4 high-level policy documents, which serve as a comprehensive strategy in regard to cybersecurity: • White Paper on National Defence and Security of 2008; • In 2011 France published a national Cybersecurity Strategy. This has a strong focus on defence and national security issues.[68] • White Paper on National Defence and Security of 2013; • New French national Digital Security Strategy presented on October 2015. The Bockel Report (2011) evaluated the accomplishments that France has made in addressing cyber-related issues since the White Paper. The work notes that the creation of the National Network and Information Security Agency (ANSSI) (2009) as the central coordinating authority for cyber security was an important step. One of the tasks given to the ANSSI under the supervision of the SGDSN was to draft a cyber security strategy. This was issued in February '11 and titled 'Information systems defence and security. France's strategy.' In 2012, President Hollande urged a reinterpretation of France's cyber posture, emphasizing the financial constraints and geopolitical challenges, which subsequently prompted a new White Paper on National Defence and Security in 2013. The '13 White Paper underlines the effort that needs to be made to achieve a secure cyberspace and calls for resources to be dedicated to this domain. The Cyber Defence Pact, presented on February 7th 2014, emphasizes the latest objectives drafted following the 2013 White Paper and the Military Planning Act in December '13.
Germany		X	Adopted in February 2011. Germany has a comprehensive cybersecurity strategy, complemented by a strong cybersecurity legal framework. This strategic document neither focuses on specific kinds of crime in Cybercrime nor on a specific audience.
Greece	X		The Directorate of Cyber Defense/General Headquarters of National Defense, with the participation of HDPS representatives, is presently elaborating a relevant text which will be soon completed and forwarded for approval to the Hierarchy. The legal and institutional framework that supports cybersecurity is limited.[69]
Hungary		X	The Government Decision No. 1035/2012 on Hungary's National Security Strategy, adopted 21/02/2012. The Government Decision No. 1139/2013 on the National Cyber Security Strategy of Hungary, adopted 21/03/13. The Strategy specifically focuses on children. Hungary regards the creation and maintenance of an environment allowing the healthy development of children as a basic element of cybersecurity and treats it as a priority in all affected areas, achieving, at the same time, the objectives of the European Strategy for a Better Internet for Children. Particular emphasis is laid on encouraging the creation of prevention of the harassment and exploitation of children, and the establishment of a secure online environment. For this purpose, Hungarian non-governmental organisations with a proven record in online child protection are regarded as key partners.
Ireland	X		National legal and policy framework is very limited, when it comes to cybersecurity. A cybersecurity strategy is being developed. There is no clear timeframe for its release or adoption.[70]
Italy		X	Adopted in 2013. https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf
Latvia		X	Published in 2014. It contains a clear set of concrete objectives matched with specific implementation dates. It has a strong legal framework for supporting cybersecurity, an important pillar of which is the Law on Security of Information Technology adopted in '10.
Lithuania		X	Published in 2011, however information on its implementation remains limited.
LUX		X	The National Cybersecurity Strategy II was approved in March 2015. http://www.hcpn.public.lu/actualites/Actualisation-de-la-strategie-nationale-en-matiere-de-cybersecurite/index.html. The Strategy focuses on all types of cybercrime, affecting the National Security and on a general audience.

[68] See: http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf
[69] See: http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf
[70] See: http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf

State	No	Yes	Answer
Malta		X	Has to develop a comprehensive legal and policy framework for supporting cybersecurity, although its Digital Malta Strategy and e-government plan promise the elaboration of a cybersecurity strategy.
NL	X		Has a sophisticated and mature legal and policy framework for cybersecurity, which includes the National Cyber Security Strategy 2. Adopted in 2013, it is the second strategy, as the country's cybersecurity framework is renewed every two years. The NCSS2 describes the overall national priorities for cyber security. Various actions on the basis of the other objectives of this Strategy, next to tackling cybercrime, are actions which can be regarded as actions aimed at prevention, at capacity building, both in the public and the private domain, as well as at raising public awareness.
Poland		X	Adopted in 2013 - with clear goals. Most of the recommendations are still being implemented. The legal framework for cybersecurity was still not fully developed in January 2015.[71]
Portugal		Draft	Has not developed a comprehensive legal and policy framework for cybersecurity, and its cybersecurity strategy has not been elaborated.[72]
Romania		X	Since 2013. It presents the objectives, principles and action directions for assuring the knowledge, prevention and fight against threats, vulnerabilities and risks on cybersecurity. The Strategy covers all sort of cybercrimes in general. It promotes cyber security through awareness raising programs among general population, public administration, private sector, educational programs on computer use among children in schools,…
Slovakia		X	Adopted its first, 5-year cybersecurity strategy in 2009. The Government of the Slovak Republic through its Resolution no. 328/2015 at its 167 meeting held on 17th Jun 2015 adopted Conception of the Cyber Security for the years 2015 – 2020. Strategic goal: the government considers open, safe and secure national cyber space, i.e. build confidence in the reliability and safety of the particularly critical information and communications infrastructure. The stated objective: should be achieved by adopting a number of key measures. In addition to the creation of institutional and legislative framework, the mechanisms of the cyberspace security management should be established, as well it should start with education in the field of cyber security. http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-187874?prefixFile=m_
Slovenia	X		The National Cybersecurity Strategy is in final stage. It must also be adopted by government and some specific action plans must be made, which will probably focuses on specific crimes and audience
Spain		X	Adopted Strategy in 2013. It is a comprehensive document, which sets objectives and targeted lines of actions. It is compatible with, and references to both the National Security Plan and existing security laws. These plans and laws work together as a package.[73]
Sweden	X		A national cybersecurity strategy is being developed. There are no laws in Sweden that specifically deal with cybersecurity.

As is obvious, no single entity or group of stakeholders can secure cyberspace alone, no individual or group is without responsibility for playing a part in cybersecurity. Not only the government, organisations of all sizes, consumers,… need to take steps to secure their systems. Education and raising awareness both play a huge role, which requires educational and awareness-raising campaigns. Like mentioned earlier, the EU has expressed a strong commitment to cybersecurity education and awareness raising and acts upon this commitment. We asked the Member States who have yet implemented national education strategies to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age. Furthermore we asked if their country has already set up major awareness campaigns. Several MS answered that comprehensive commitments to cybersecurity education, are included in their National Strategic Frameworks (Italy, Austria, France). Slovenia is working on including

[71] See: http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf
[72] See: http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf
[73] See: http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf

this topic in their National Cybersecurity Strategy. All the MS (that filled in the questionnaire) answered that they have material designed to raise public awareness of risks when using the Internet, Social Networks,… that they have several awareness campaigns,…

Conclusion

Once again, this chapter shows the importance of the fight against cybercrime. In less than two decades, the Internet has grown from a curiosity to an essential element of modern life. However, the rapid expansion has far exceeded regulatory capacity and the absence of authority has left space for many abuses. Cybercrime has an international dimension, therefore fighting cybercrime calls for international cooperation. Various international and European organizations, institutions, agencies,… have already made (joint) efforts.

Despite the fact that cybercrime is not an absolute priority for the OECD, it was the first international organization that wrote guidelines in the fight against cybercrime. There above, the OECD released numerous reports in this context. Also, the United Nations play an important role in this context and the G8 has taken some initiatives on cybercrime. The Council of Europe draws all the attention with his Convention on Cybercrime: the first, and until today, the only international treaty aimed at combating cybercrime. The importance of this treaty cannot be overemphasized. However the EU has started later than the rest of these institutions (presumably because the wanted to avoid overlaps with the initiatives of the Council of Europe), the EU has played an important role in the fight against cybercrime.

In 2013, the 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace' was presented, which sets out the EU's approach and vision on the best way to prevent and respond to cyber disruptions and attacks. It was the EU's first comprehensive policy document in this area. Another noteworthy initiative was the creation of the European CyberCrime Center, EC3 in the same year as the publication of the Cybersecurity Strategy of the EU. Above all these legislative measures, initiatives, the creation of the policy in the fight against cybercrime,… there are many other networks, working groups, initiatives taken,… in Europe.

Finally it is important to mention that children have particular needs and vulnerabilities on the Internet, which must be addressed specifically so that the Internet becomes a place of opportunities for children to access knowledge, to communicate,… Children are particularly vulnerable to the dangers of the Internet and their online safety needs to be guaranteed. The EU has created several legislative measures to protect especially children.

After looking at the different International and European weapons, initiatives, strategies,… against cybercrime, it is important that the EU Member States work with these international and European conventions, legislations, initiatives,… This is especially important since the conventions are general guidelines: it is up to the Member States to implement them into their policies and their legislation. In this chapter we could read that the Member States indeed recognize the importance of the fight against cybercrime.

Part 2

Good and promising practices:
Best Practice Conference and the European Crime Prevention Award

Good and promising practices: Best Practice Conference and the European Crime Prevention Award

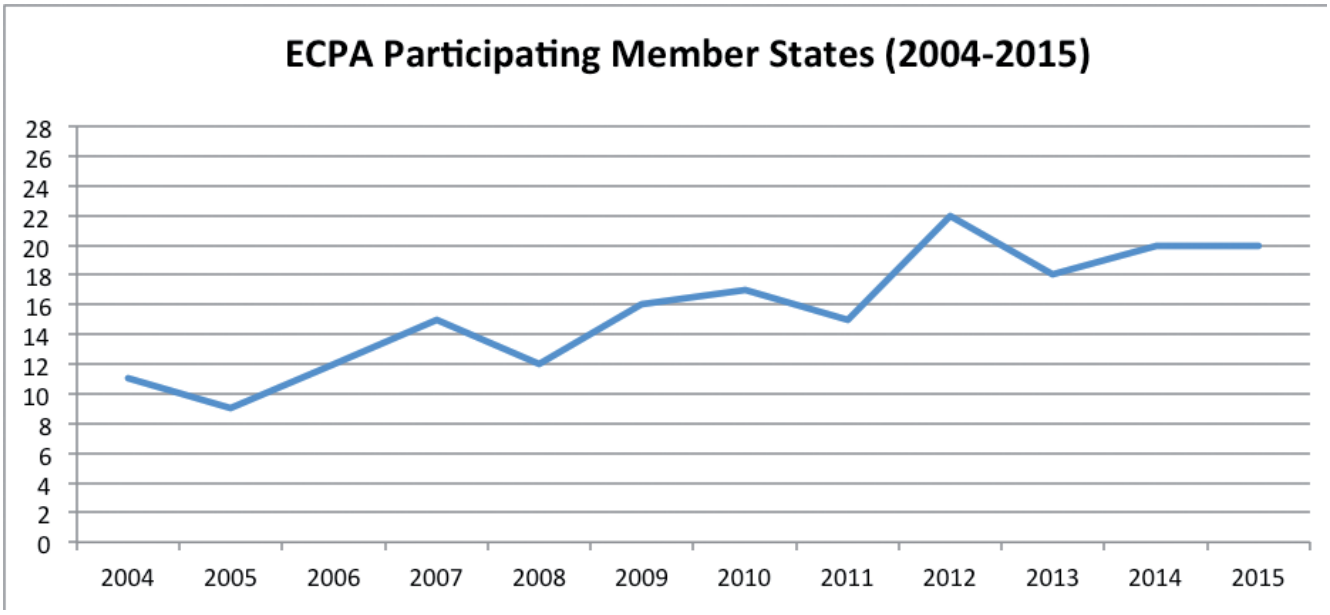
Introduction

The Best Practice Conference (BPC) is organized each year in December, bringing together practitioners and policy makers from all over Europe to share their experiences.

Since 2004, the BPC has been linked to the competition of the European Crime Prevention Award (ECPA). The ECPA competition aims to publicly award good or promising practices in the field of crime prevention through an assessment by a jury made up of experts from various Member States.
The ECPA is open to all EU Member States who can submit any theme-related project, initiative or package of measures which was successfully implemented to prevent crime and which complies to the following criteria (EUCPN, 2015, Annex II):

1. The project shall focus on prevention and/or reduction of everyday crime and fear of crime within the theme.
2. The project shall have been evaluated and have achieved most or all of its objectives. Evidence of impact in reducing crime or increasing safety shall rate over evidence of other kinds of outcome.
3. The project shall, as far as possible, be innovative, involving new methods or new approaches.
4. The project shall be based on co-operation between partners, where possible.
5. The project shall be capable of replication by organizations and groups in other Member States. Therefore, submissions should include information on the financial costs of the project, the source of funding, the implementation process and relevant source material.

Figure 1 shows the number of entries for the ECPA since 2004. (source: EUCPN website)



With the attendance of around 150 participants from all over Europe each year, the BPC and ECPA can be regarded as cost-effective instruments to quickly and directly circulate good crime prevention ideas from other cities, municipalities, countries and organisations, which

are faced with similar challenges. Since 2012, the winning initiative is awarded a financial sum of €10.000 and the two honourable mentions receive €5.000 each.[74] The complete Rules of Procedure of the ECPA can be downloaded on the EUCPN website.[75]

General overview of the ECPA 2015 theme and entries

This year's BPC was organised by the Luxembourg Presidency on 17-18 December 2015 in Luxembourg City, Luxembourg. The general theme was '**Cybercrime**'. In the call for entries, which was launched in July 2015, cybercrime was defined as *a phenomenon that is increasingly affecting our modern society. Cybercrime is one of the key priorities for the Serious Organized Crime Priorities 2014-2017 of the EU Policy Cycle. Furthermore, European police statistics reveal a substantial increase of the phenomenon. There above, on a regional level with neighbouring Member States (Belgium, Germany, France), the topic figures on the agenda of several crime prevention cooperation groups and seminars.*

In total, 19 Member States countries submitted a project. On top of that, some Member States shared 'additional projects' - 6 in total – related to the prevention of cybercrime. These additional projects did not compete for the award, but where presented purely to share information and exchange good practices.

The ECPA Jury

On 11-12 November 2015, the ECPA Jury met in Luxembourg City, Luxembourg, to assess this year's entries. As prescribed, the jury is composed of up to eight members – no more than two per Member State of the (i) current EU Presidency (ii) the former EU Presidency and (iii) the two incoming Presidencies. This year's jury was attended by:

- Mr. Jean-Marie Wagner and Mr. Bob Leesch from Luxembourg
- Mr. Andis Rinkevics from Latvia
- Mr. Haiko Smid from the Netherlands
- Ms. IVANCOVA Eva from Slovakia

The Jury was chaired by Mr. Jean-Marie Wagner, EUCPN Chair during the Luxembourg Presidency, and support was given by Ms. Febe Liagre of the EUCPN Secretariat.

In part 3 of this toolbox, facts sheets of all ECPA entries are included. The next paragraphs will first look closer into the three projects which were particularly honoured by this year's jury members.

[74] EUCPN, 2015, Rules and Procedures for awarding and presenting the European Crime Prevention Award, Brussels.
[75] www.eucpn.org

The three honoured projects

All projects were found remarkable by the jury and were praised for their efforts to prevent cybercrime. Nevertheless there are three projects that stood out and received an award. These three projects were:

The ECPA 2015 winning project is the Dutch project 'SME Cybersecure' of 'MKB Nederland' (The Netherlands). Subsidised by the Dutch Ministry of Security and Justice, MKB-Nederland (together with other partners) developed a project to make entrepreneurs more aware of the impact of cybercrime on their businesses. A lot of Small Medium Sized companies (SME's) do not realise that their websites and databases are potential targets. To make SME's more aware of their own cybersecurity, the project organises an awareness campaign based on a roadshow through the country. During this roadshow SME's are given the possibility to improve their cybersecurity by offering 300 free 'social' hacks, giving them a clear insight into their vulnerabilities and the measurements they can take to improve their cybersecurity. The partnership with KPN (Telco) offers SME's a professional service with a discount, which means SME's can immediately take action to improve their cybersecurity. Moreover, the partnership with the Association of Insurers offers SME's a clear insight into insurances for cybercrime.

The German Project 'Media Heroes' of the 'Freie Universität Berlin' was awarded as the 1st honourable mention. "Medienhelden" is a universal, manualized, theoretically based, and carefully evaluated (process, impact, implementation evaluation) preventive intervention program for the school context (7th-9th graders), including teachers and parents. Objectives are: Prevention of cyberbullying/-victimization and promotion of online self-protection skills and social skills. The program relies mainly on social learning and cognitive-behavioral methods and works with activating methods (peer-to-peer and peer-to-parent-tutoring). The program is intended for implementation in classrooms and covers ten weeks with sessions of 90 minutes each as part of a curriculum. A shortened one-day-version (4 sessions of 90 minutes) was also developed. The program manual provides school teachers with all materials needed to carry out the program. A longitudinal, randomized control

study proved the positive effects of the program (e.g. reduction in cyberbullying, improved skills/empathy). A train-the-trainer approach is available for the purpose of implementation, offered by licenced external enterprises and partners.

The Luxembourg project 'Bibi and Friends' of the Service National de la Jeunesse' was awarded as the 2nd honourable mention. With "Bibi", the little bee, and his friends, children from the age range from 3 to 6 years learn how to safely take their first steps on the internet. They can listen to the stories online or have them read by their parents offline. Easily accessible for both parents and kids, these stories are full of hints and ideas on how to successfully protect yourself or your children from potential online threats. Out of the first three stories, two deal with online crime prevention: false identity and online fraud. The website is complemented by printed booklets, and also by complementary handcraft activities.

For a more detailed description of these and all other projects submitted, please see Part 4 of this toolbox, or go to the EUCPN website.[76]

Provisional conclusions of the 2015 Best Practice Conference – European Crime Prevention Award.

As mentioned before, this year's Best Practice Conference brought together policymakers, researchers and practitioners from all EU Member States who are active in the field of cybercrime. The most important aim of the BPC was to create the opportunity to share and disseminate experiences and knowledge and present good practices in preventing cybercrime. This year, presentations were given by various international organisations, such as Europol, Insafe and Inhope. Furthermore, a presentation was given by Prof. Antonio Mauro. The variety of participants to the BPC made sure that the BPC was a good networking event.

Furthermore, two workgroups were organised in which the ECPA entries were presented. In each of these sessions, two experts - invited by the EUCPN Secretariat - followed the presentations and gave their point of view and opinion of all the projects. The sessions were led by Bob Leesch (Luxembourg Presidency) and Febe Liagre (EUCPN Secretariat). In the first session Janneke Schilder (Tilburg University, Netherlands) and Maria Sanchez Prevention and Communication Officer, European Cybercrime Centre (EC3) Europol) followed the presentations of the projects, Iris Steenhout (Free University of Brussels (VUB), Belgium) accompanied the second session.

[76] EUCPN Website, all the ECPA entries can be found here: http://eucpn.org/search/knowledge-center?f[0]=im_field_doc_subject%3A9&f[1]=im_field_doc_subject%3A25&f[2]=im_field_doc_year%3A34

In session 1, the projects from Croatia, Denmark, Finland, Germany, Italy, Luxembourg, Poland, Romania, Spain and Sweden were presented, while in session 2 the projects from Belgium, Czech Republic, Latvia, France, Hungary, Estonia, The Netherlands, Portugal and Slovakia were discussed. The 3 experts were invited to make written reports. Each of them made a synthesis about their findings and opinions of the presented projects. All four experts had different views and attention points; therefore we decided to put their reports in this toolbox.

Session 1, written report from Janneke D. Schilder[77]

All proposed projects in session 1 focused on **online safety of children**. Although most of them took a multi perspective approach (parents, children and educators), they can be divided into three main categories. Namely, the projects of Germany, Luxembourg, Spain, Croatia, and Romania focused directly on educating children concerning risks online, whereas Poland, Italy and Denmark provided tools for educators, social workers and website moderators to prevent harm online. Both Finland and Sweden distinguished themselves from the other projects by their focus on perpetrators of online sexual abuse. Hereby it was stressed that the term child pornography is not an appropriate term since child abuse is behind all material.

To start with the latter projects from Finland and Sweden to prevent perpetrators from sexually abusing a child online, both aim to prevent perpetrators from offending in different ways. Namely, Finland's project is directly focused at the motives and the well-being of perpetrators themselves. Therefore, they set up a self-help module online that is freely and anonymously accessible for all who feel attracted to minors. The module was partly developed with the help of people who were convicted of child abuse so that the perpetrators perspective is embedded in the program. Therefor this program seems a good tool and it deserves extra support since developments to give support to the child predators themselves is looked upon as controversial. However, if we want to prevent children from being sexually abused online, it is important to give attention to the perpetrators as well. Sweden was the other program that aimed to prevent online predators from harming children online, although it took a completely different approach. Namely, this project aimed to prevent only sexual abuse by blocking money transfers associated with sexual abuse via a cooperation of banks in Sweden. This cooperation between almost all banks in Sweden works sufficiently, although they do face a problem with electronic money, such as bitcoins. Future plans are made to tackle the problem of electronic money as well and other countries are encouraged to start such a cooperation between banks in order to prevent money transfers related to online sexual abuse. Although this is a good initiative, I feel that since paedophilia will remain to exist they will find other ways to access child abuse material so this should just be an extra way to tackle the problem in combination with personal attention for the perpetrators themselves.

[77] - Luna, R., & Finkelhor, D. (1998). *School based prevention programs: Lessons for child victimization prevention*. Retrieved October 21, 2014 from. http://www.unh.edu/ccrc/pdf/CV30.pdf.
- Schilder, J. D., Brusselaers, M. B., & Bogaerts, S. (2015). The Effectiveness of an Intervention to Promote Awareness and Reduce Online Risk Behavior in Early Adolescence. Journal of Youth and Adolescence, 1-15.

Poland, Italy and Denmark provided *tools for educators, social workers and website moderators to prevent harm online*. All focused on different groups of people who are related to educating/-helping children. First, Poland aimed at training for teachers on high schools to recognize and to deal with cyber bullying. Since this is still a relative new topic for teachers, also accentuated by the generation gap, this is a valuable program for teachers in Poland. Included in the program was also informing children and parents about the problems related to cyberbullying. I believe that schools are a perfect medium to transfer knowledge towards all parents and children independent of social class so this is an important part of this particular project. *The Italian project* is also a tool to increase knowledge concerning risk and deviant behavior online, however this project is only aimed at increasing knowledge for the people around children and thus not directly helps to promote the online safety of children. The project included a dictionary with all kinds of risky online phenomena. Although it is valuable for social workers, educators and parents to know about these terms, I don't believe that this will help in preventing online risks in children since this is more of a tool to look up terms and legal consequences that you don't know of, instead of informing caregivers/-professionals about risky behavior and giving practical advice on how to prevent or deal with them. I feel that this kind of tool is helpful in countries were the knowledge about the internet is relatively undeveloped. The last proposed project in this category is Denmark. This project took a different approach to increase the safety of children on websites. Namely, this was done by informing and training moderators of websites were children are active in chat boxes. Although this seems like a small part of children's online risks, this initiative does seem to get a relative amount of attention by Danish websites. Moderators can follow the course partly online and one day of face to face training is included. The course is also given in English which makes it easy for moderators from other countries to join the course. It still seems to be difficult to get moderators to follow the course, but the ones that do gave positive responses and feel better equipped to recognize and respond to problems online such as bullying and grooming.

A vast amount of projects *aimed directly at the children* themselves to decrease online risks. Most of the proposed projects (Germany, Spain, and Romania) aimed at adolescents in the beginning of high school (around twelve years of age). Croatia also included children in the last phase of primary school and the project by Luxembourg focused on young children from six to eight years of age. I feel that the latter is tapping into an important issue, since surveys show that children in the EU go online at increasingly younger ages, so it seems like a good initiative to start early with educating children in an appropriate way about internet safety. The simple and appealing books that were created for this project can be read by parents which will also involve parents in learning and promote talking to their child about online issues in a very simple way. The book is available in French, German, English, and Dutch and can be developed in several other languages which makes it easy to use in other countries. Additionally, they also organize camps and fairs for children were they can do all kind of things with Bibi, the main character of the book; like drawing or playing so that it's not just the book which makes it more likely for the children to remember the lessons learned in the book. This is a great initiative, however it is important that the impact on children's awareness and behavior will get tested scientifically to know whether it will have the expected impact. Without this it will only remain a

guess whether it works or not. I feel that this is important before it will be disseminated towards children all through Europe or outside.

Pantellas Amigas is another project that focused on somewhat older children and adolescents and is already implemented in a lot of Spanish speaking countries. The main part of the project are video clips on YouTube that address a certain kind of risky behavior on the internet. The clips are very appealing and are shared among youngsters themselves. I think that this is a very strong aspect of this project, youngsters will send it when they feel that it is interesting for them and their peers. Since some video's had over one million views it works very well to spread information through YouTube which can be a good example for other projects. Additionally, it shows that youngsters have a need for information about these topics. However, for this project I will have to stress again that it is important to examine the effects of the project. Nothing is known about the effects on children/adolescents when seeing such movies. From former studies, (Schilder, Brusselaers, & Bogaerts, 2015) we can learn that just informing children about online dangers will not make them less likely to behave risky online. Additionally, in a study by Luna and Finkelhor (1998) it is summed up what an effective intervention program should entail and what not. Among the aspects that an intervention program for children should not focus on is danger. However, this is exactly what Pantellas Amigas does. Despite the fact that this project is a success on YouTube, I think it is important to start a study concerning the effects of the project. Although I stress the importance of more research for these two projects specifically, it is important for all the proposed projects concerning intervention on children's behavior.

Another project that focused on the children themselves, was the Croatian project. They select a group of excellent students and train them to become lab detectives. They learn how to behave online and how they can report illegal content. I liked the innovative idea of giving the responsibility to the children to look for, and report, illegal content. However I feel that it is also a risky way to increase online safety: children will learn about all kind of illegal material and activities on the internet, which might make them wiser than they already are. On the other hand, the students are specifically selected, so it can be expected that these are not the students who are likely to engage in risky activities after hearing about them. Additionally, this raises another point: the project is specifically aimed at a small group of students who receive a training in online safety which after they function as a contact person for other children. This might place them in a position of too much responsibility which cannot be expected of children/adolescents and it might not be effective in reaching the other children. Although this idea is innovative to give certain children the 'job' to be the contact person and to keep an eye on online safety, I feel that it is better to focus on interventions for all children in addition and to be hesitant with learning children too much about online risky activities.

Another project that focused on children themselves was the project by Romania. They asked high school students to think of a play that involves online risks. Adolescents were free to choose the topic related to online risks. An advantage of this approach is that they can freely think about what they think is important and it will make them probably more involved and

enthusiastic. On the other hand, as an organizer you will not have influence on the content of the eventual play. It was not clear to me whether they provided general guidelines and/or topics, but this could be a possibility. The best plays were presented at a festival which received a large amount of media attention and promoted the awareness of the problem. I feel that these kind of events are valuable additions to other intervention projects implemented in the school curriculum.

There was only one proposed intervention project for children that was *evidence based*: the German project Media heroes. This project is the result of years of scientific research by professor Scheithauer concerning the development of an intervention that aims to reduce cyberbullying. Results showed that this project is effective in reducing cyber bullying among adolescents. Two versions of Media heroes exist: a short version with one project day and a long version of ten weeks which is implemented in the curriculum of the school. Both showed to have an effect, however the effect in the latter was bigger and lasted for a longer period. I think that this project should be an example for the other projects to include scientific research on the effects of the interventions.

Currently, a study to prevent online risk behavior in primary school children (4-12 year olds) will start in February in the Netherlands and will scientifically examine the effects on risk behavior of media lessons in primary school (nationaalmediapaspoort.nl). Hopefully these initiatives will provide more evidence based projects in the future so that we know whether an intervention is effective before we implement them among children and/or adolescents.

We can conclude that many of the projects were focused on online safety of children and adolescents, which is in line with recommendations made by the European Commission. There were a few innovative aspects in the proposed projects: the Luxembourg project focused on very young children, which seems important because of the young age at which children tend to go online. A vast amount of projects focusses on a multi-disciplinary approach including parents, educators, and children, which will make it more likely that interventions will have an effect. Although many intervention projects for children seem promising, only the German project is evidence based. It is stressed that more projects should take the evidence based approach. Additionally, Finland and Sweden take another approach in online protection of children by focusing on online perpetrators instead. Especially Finland deserves attention since this controversial projects helps men with paedophilic feelings to anonymously follow an online course to prevent themselves from online abuse of children.

Session 1, written report from Maria Sanchez

The *Croatian project* presented the status of Internet today and a general view about how does it look like, setting up the basis to show its complexity, and its design mainly for adults. If adults connect online every day and they have problems and issues understanding it, it is even worse for children who are constantly connected via their mobile devices. This project was designed to increase the children's knowledge (also their parents and educators), the

connection between online and off-line world and the consequences of the actions. Children are targeted by cybercrime as much as adults (phishing, malware, etc.), plus they are the direct victims of a range of serious crimes, such as sexual extortion or child sexual abuse. They are also contributing to the expansion of Internet radicalisation content, by sharing videos and messages. They are an active part of the Internet ecosystem, and need to equally receive proper education to understand the risks and the rules. This long term project (2012 – 2020) is updated every year to adjust the content and learn from previous experiences, containing 10 recurrent activities: interactive workshops, selection of web detectives, lectures for parents and the general public, posters, video clips, training for teachers and other professionals, participation in the Safer Internet Day and nurturing of international cooperation. The consolidated structure and detailed description would make this project a good model for further implementation, either at national level or also international, since the materials created and technics used can be translated and reproduced in other countries, and the messages and goals are universal: online safety for youngsters and the adults around them. The project has been running for 4 years, which ensures the model and participants have developed experience and best practices that could be transferred. It has also been evaluated by qualitative and quantitative methods, which provides an indication as well of the success thereof. The project has had media coverage, expanding the messages and making it very visible for the community.

<u>To take into account:</u>

- Budgetary needs: besides the human resources, the project relies on interactive work with children and use of technology (digital classrooms, online training, creation of videos and quizzes, etc.), which imply charges and therefore the need to find financial support. This means that, while the programme and the results obtained may be excellent, in order to further replication at EU level there is a need to find proper funds before.
- Cultural and legal framework adjustments: the programme is designed specifically for Croatia. If further implementation is considered, the material and messages are to be assessed and customized to other national needs.
- National partners and support: due to the magnitude and ambition of the project, it would require national efforts to find equivalent partners in other Member States willing to engage and cooperate, although the successful formula and universal goals pursued are certainly a good business card.
- Internal expansion before going International: At this point the project is running only in a particular region in Croatia. This means that the results and feasibility are tested at a relatively small scale.
- The power of working with schools and law enforcement: in order to reach out to children, it is key to establish this kind of programmes as part of the regular curricula at the schools. Technology is a constant element in the 21st century, computers and other electronic devices as well as a permanent way for society, businesses and governments to interact at a personal, professional and administrative level. The new generations need to get familiar with technology, and it is important for them to learn from specialists (law enforcement and experts from the private and public sector). Also, it is important to show them the options, not only the criminal possibilities, but also the professional careers available in case they are interest on the matter.

The project from *Denmark* aims to ensure that moderators in direct contact with children in chats rooms have clean records and receive the necessary training to ensure the children remain safe while chatting and away from predatory behaviour, but they also behave appropriately when talking and interacting with each other. The project consists of 3 approaches: face-to-face education, e-learning modules and cooperation with Safe the Children. The SNS providers participating in the project receive an official certificate, what ensures the standards and reliability of the site. The training is offered for free to all the SNS provides, which guarantees equal treatment among the various companies in the business, good to build up their own reputation as well. More than 600 moderators have followed the training already. Cooperation of Safe the Children Denmark is key in the delivery of this project.

To take into account:

- This project is original and more important than it might look like at first sight. One of the most common environments to identify children to groom and further either sexually extort or abuse, are the chat rooms. Counting with the presence of an adult who is capable of identifying suspicious behaviours and to mediate when so needed is an excellent prevention initiative. Also when it comes to liaising in conflicts and to teach online behaviour.
- Denmark is the EU country where children start using mobile devices at the earliest age. Chat rooms are probably a well-known reality, while perhaps they are not so visible in other Member States. This could imply a lack of interest from other countries, while in reality it may make it there even more necessary, since the lack of control and attention may attract more predators and conflict than in other countries with more technological tradition in this sense.
- According to the Safe the Children Denmark website, they have presence in other 120 countries, which could facilitate the further implementation of this project, as well as the Safer Internet Centres.
- If the number of providers of SNS for children is on the rise as stated in the project description, this project should be promoted and boosted as much as possible, raising awareness among the business on the consequences of having chat rooms for children unattended or not properly handled.
- Material is already available in Danish. As always, there is the need to translate and adjust to the cultural reality.

This Finnish project was innovative, original and unique, targeting adults with the intention to help them combat their sexual interest or urge for sexual actions towards children. The material is free to consult in the website croga.fi, in Finnish language. The access is anonymous, and it can be consulted individually or with the help of a professional. The added value is that the content was elaborated (and evaluated and updated) with the support and cooperation of people currently sentenced for these behaviours; hence reflecting real cases and experiences highlighting the damage suffered by the victims and the possibilities to get rehabilitated. The combination of this input together with the consultation of experts on physiology and rehabilitation ensures quality and adequate content. The project has also been combined with media attention, and it is expected to be further broaden with training courses on the matter for

law enforcement and judges and a social media campaign. More than 15.000 individuals were reported to have consulted the material.

To take into account:

- This project was based in the British self-help material croga.org, and adapted to the Finland reality applying the latest research and clinical practices, which means that there is already a successful case showing the possibilities of implementation in different countries. Germany and The Netherlands were mentioned to have similar initiatives as well.
- This project shows that child sexual abuse can be prevented if we invest on in and dedicate resources to help those people with sexual inclination towards minors.
- There is a need to consider the best strategy and way to promote this type of websites, in order to reach out to the potential target audience so they become aware of their options.
- Technology and the use of "protected" environments such a TOR have increased and encouraged the production and consumption of child sexual abuse material. Offenders feel anonymous and more willing to interact and "feed" their interest.
- The need to prevent the use and circulation of online child sexual abuse material is common to all Member States.

The German project was specifically developed to target the problem of cyberbullying at the school, creating a 10 weeks prevention intervention programme which combines the prevention and reduction aspect with the promotion of online self-protection skills. A shorter version (4 sessions of 90 minutes) is also available. The project had an impressive delivery control and content evaluation, from both participating students and teachers.

To take into account:

- This was the only project that presented an exhaustive evaluation and evaluation results, being capable of demonstrating positive results and the decrease of cyberbullying among the selected teenagers.
- The materials developed did not only focus on teaching concepts and online safety, but also stressed the effect on feelings and real consequences, directly targeting to increase empathy among the peers.
- The reported budget for this extensive and well researched project was 110.000 Euro. The programme materials are not free of charge (39,90 Euro per book).
- Versions in Spanish (soon) and English (1 to 2 years) will be made available.

The connection between *the Italian project* and cybercrime prevention is perhaps less influential in the final outcome of reducing criminal activities. However, it is a useful tool, translating the criminal activities into legal and punishable consequences, as an easy way to inform the population via official resources. It is more an informative tool, very valuable for research and consultation, than a strong prevention mechanism. The cooperation with private industry (important partners like Google or Telecom) and public intuitions (Postal Police and Italian Association of Judges dedicated to Children and Family) was very relevant in order to locate the link to the website in visible places, so regular Internet users could become aware of its existence.

To take into account:

- It requires constant monitoring for terms update and creation of new entries as cybercrime evolves. 55 words are currently included.
- It is highly unluckily that a child will decide on its own to consult this type of lexicon. The technical vocabulary used, plus the references to legal articles are not suitable to explain to minors the consequences of online criminal activities.
- On the contrary, it can be a very valuable initial tool for adults with enough educational grounds as well as for researchers, university students and professors and social and judiciary professionals.

  Practical example: Grooming: Online soliciting of a minor, via chat or social networks. A cyberpredator singles out a young victim, then creates a bond which is at first only friendly, then it becomes confidential, then intimate and turns into sexual exploitation. It is a long and interactive process, in which the predator plays to the victim's psychological needs.
- The project is only usable in Italy (due to the legal references), it's extension to other countries would require a deep assessment of the national legal codes in order to find the links, as well as to determine which conducts are punishable, since not every country applies the same patterns (i.e. the consequences of acting as "money mule" vary in different EU states from initial warning, to social services, to fines or even imprisonment).

The Luxembourg project is a great pedagogic creation, very well tailor-made for the target audience to understand and follow the stories, while transmitting valuable basic messages and educating the children with words and stories according to their age and knowledge of the world. It involves the interaction with parents and educators, in a way that makes the links between both groups solid, setting the trust basis for the future. It also provides advice, teaching the adults how to react against certain online situations, completing the education process and making Internet, even more, part of their daily lives in a natural and stress-free way.

To take into account:

- It would be fantastic to design and create following up material, for instance from 7 to 10, from 11 to 14 and from 15 to 17, adjusting vocabulary, characters and stories, but continuing with the education in a realistic way that children can understand and feel themselves identified with. This would cover the whole child's life, as part of the school curricula, and a common generational culture, since every kid will know and grow up with the same stories and lessons learned.
- Growing up with technology shall become a natural habit. I am a strong believer of introducing online safety as part of the normal education, in close cooperation with parents and schools. We will not be able to eradicate cybercrime, but we will teach the population on the correct use of mobile devices, identification of threats and victimization, and further report and reaction in the event damage occurs.
- Children's education starts with parents' education.
- The fact that Luxembourg is a small country probably facilitates the potential global roll-out and stabilisation of this type of campaigns, reaching out a high number of citizens in a

relatively easier way than in Germany or France, for instance (also in terms of budget to be invested).
- The contents are already available in 6 languages, which prove the interest from other countries in testing the model.

The Polish project focused on cyberbullying. Schools are nowadays the most natural environment where bullying starts. What traditionally would end after class, nowadays it continues online 24/7, with the possibility to even give it a global dimension due to the use of social networks. Bullying becomes cyberbullying, and the psychological consequences on the victims may be truly traumatic, unable to disconnect from the problem. This project focuses on the figure of the teacher as a central role to influence the children's behaviour. As a consequence, a specific training has been designed to transmit them psychological and pedagogical skills, as well as technological knowledge to be able to put the problem into perspective and to be familiar with the technologies and platforms that can serve as driver. The training material and the courses for teachers are complemented with workshops for students, educational meetings for parents, a Handbook for teachers, educators and psychologists and a Facebook awareness page.

To take into account:
- Cyberbullying is a crime in Poland, it might not be in other Member States. The project content stresses very much this fact, informing about the legal consequences and raising awareness among the children.
- The dimension of cyberbullying probably justifies having a dedicated programme focused exclusively on its prevention, separated from the rest of general online security education.
- The need to educate children on correct behaviour online and off-line shall be a combination of efforts between parents and educators. Both groups are to be duly informed on the problem, consequences, how to identify it and how to counter-measure it. Ideally, what a teacher initiates during school hours shall be continued by the parents when the children arrive at home. Otherwise the efforts might be only partial. Perhaps the role of the parent and its training could be further reinforced on this project.
- The evaluation performed in the project focuses more on assessing the training materials and delivery than on the results achieved (did the cyberbullying decreased or not?).
- Poland is looking for other Member States to partner together to apply for EU funds.

The Romanian project combines the educational and preventive side with the involvement of the target audience, inviting them to develop their artistic creativity to represent the theme at hands by means of drafting and implementing a theatrical script, and to further engage with law enforcement officers with questions and answers. An innovative way to learn by enjoying, even if at small scale (only in Bucharest). It gave the children the possibility to put in perspective and to image real situations/scenarios to represent the content. No specific evaluation information provided as to the level of knowledge acquired. No in depth description of the contents presented to take as basis to write the script.

To take into account:

- First of the projects presented that is led by law enforcement (young cybercrime prevention and victimization as one of the priorities of the Romanian police during the last 5 years).
- This project was not only about online security, copyrights and it's infringements was also part of the scope.
- This project was run without funding; it only counted with the self-less support of the participating institutions, bodies and companies. In-kind contributions and voluntary work.
- It was the first time that a cybercrime prevention related project took place in this country.

The project from *Spain* offers a wide portfolio of components: awareness campaigns, interactive games, booklets and guides for teachers and educators, intervention protocols for victims, blogs and complaint forms. It is a growing project, initiated to combat sexting, it has incorporated more (yet related) areas: cyberbullying, grooming and sexual extortion, which shows the flexibility of the founding company and its willingness to expand and to tackle the global problem of correct use of new technologies. These types of crime can seriously affect adults, both economically and psychologically, but the same activities targeting minors can be even more severe and traumatic. Prevention is a key component: it shows the very origin of these crimes, and also the modus operandi, making the population aware of the various (apparently naïve) forms in which they can be approached. Not only that, it focuses on how to fight back and how to report it, in the event a person becomes a victim. Pantallas Amigas acts as link between the people reporting to be affected by the situations reflected in the videos and the Spanish police, playing a key role not only in the education side but also providing assistance to the victims and intelligence leads to law enforcement.

To take into account:

- All existing material created under this project is available online, free of charge, and at the service of any country or company that may want to make use of it (respecting the copyrights, of course).
- Pantallas Amigas has already created versions of some of the products in other languages (English, French and Arab). Their willingness to expand and cooperate with other countries was offered and stated in several occasions during the presentation and in the margins of the conference.
- Some of the videos have reached more than 12 million views in YouTube, which ensures that format and messages are well received by the target audience.
- It is the only presented project that went viral in social media. Reaching these levels of visibility and reception among the population is a huge and unusual success, and a clear sign of working in the right direction in the digital age.
- Sexual extortion is an area currently under assessment among the law enforcement European and International working groups, with close involvement from both Europol and INTERPOL. Pantallas Amigas cooperates regularly with the Spanish National Police as well as with some countries in South America. Europol and INTERPOL have also initiated conversations to launch a potential global campaign with their support and materials.

The Swedish project implemented a mutual exchange of knowledge between the banking sector and the Swedish Police, which have developed a working method to impede the online payment of child sexual abuse material via credit cards. The way to do it is by finding the point of sale of this material in order to shut down the seller's ability to receive payments. A key success of this project was to focus on the selling companies instead of in the buyers, to overcome the banking secrecy and data protection regulations.

To take into account:

- It is commonly acknowledged that the term "child pornography" is incorrect and misleading, and other references such as "child sexual abuse material" should be used instead.
- The work of the Financial Coalition against Commercial Sexual Exploitation of Children matches the global goal of the European Financial Coalition (EFC), also intended to combat the commercial sexual exploitation of children online. The possibilities for cooperation and further implementation of the Swedish model in other EU countries could be further assessed and promoted with the support of the European Banking Federation.
- The engagement and support of the banks is indispensable to establish this model at a national level. Without the banks it is not possible to prevent the payment of this kind of material through the financial system.
- The commercial distribution of child abuse material has shifted mainly towards TOR, where users feel more secure and anonymous. The arrival of crypto currencies to the markets, especially Bitcoins (the preferred virtual currency for criminals according to the Internet Organised Crime Threat Assessment 2015 – Europol), could bring difficulties to follow up and identify transactions, since the participation of the banks is not direct.

We can conclude that all projects were related, one way or the other, to protect children online and to create a safer Internet environment for them. Cybercrime universal problems were targeted, such as cyberbullying (Germany, Poland), online safety (Croatia, Luxembourg and Romania), sexual extortion (Spain). However there were some specific projects, such as legality side (Italy), forums (Denmark), paedophiles (Finland), commercialization of child sexual abuse material (Finland) Finally, we need to take account of the cultural differences and the budgetary needs to translate the content.

Session 2, written report from Iris Steenhout

The Hungarian project offers a Threat Assessment of Bullying Behavior in Youth in Internet. An EU funded effort of a collective of EU experts. They've developed a toolkit, videos, books for teachers and a video game. The project wants to increase the wellbeing of youngsters and reduce and prevent antisocial behavior 'and ultimately stop crime'. Students and teachers are targeted by the project. A measurement tool (toolkit) has been put in place to measure the amount and forms of involvement in cyberbullying & the effectiveness of solutions learned during the project.

A plethora of tools has been developed & researched. The efforts and results on a school basis where measured via a monitoring form. A network of participating teachers was formed and introduced a form of peer assessment as well. The goal to 'ultimately stop crime' is clearly a bit too ambitious to tackle by ways of this project.

The strong points of this project:

- Well researched starting point
- Assessment during the project
- Measurement effectiveness after the project
- Wide network of experts that made it possible to deploy on a wider scale
- Already developed for wide application within the EU
- The link online/offline is made during project. This is needed since bullying can't be studied as a rather online or offline phenomenon

Points that should be mentioned:

- This was proposed by Hungary, but is a collective effort

It think this is an ambitious project that was successfully developed. Can be a serious helping hand in raising awareness regarding cyberbullying, which is not seldom without consequences.

The Estonian project wants to raise awareness on cybersecurity, focussing on the topics social engineering, privacy, network, internet, hacking and malware. It uses a gamification approach to obtain its goal. This can be used in a class context or among youngsters. The cards are free for download and can be adapted (with mentioning of Digital Safety Lab). The game tries to prevent specific cybercrimes (fraud, identity theft, sensitive data stealing, (D)DOS,…) and does so by showing how to keep a clean computer, avoid data from being stolen, avoid ID theft & social engineering. Extensive research was put into the making of the game. Focus was mainly on Estonia, the cards are free for download and can be adapted to other contexts as well. The simplicity of the game rules made it easy to use. To date the game was tested on about 10000 students and used by a community of 600 ICT users. It was downloaded about 200 times. Evaluation of results is based on qualitative measurement (oral feedback & email) and reveals a 'mainly positive feedback'. It is therefore hard to tell whether all goals are successfully obtained.

Strong points:

- Well designed and extensively researched game design
- Easy to adapt to other context, but most issues tackle pretty global problems
- Free

Weaker points:

- I would advise a more quantitative & longitudinal approach for measuring the effects
- Is quite technical at times, but then again this can be adapted due to the free nature of the game that also allows modification

This project offers an easy to use tool and aid to raise awareness. It can be adapted/translated to the specific needs/knowledge of the target group.

The French project wants to raise awareness amongst youngsters concerning Internet and social media use. They target 6 themes, specifically: defamation, identity theft, sexting, cyberbullying, pictures of parties & evenings and real life encounters. The project stems from the notion that more and more youngsters & parents came to the tête à tête team with questions on social media and the internet. The centre builds on previous popularity. It receives over 17000 visitors a year, from which 12000 come spontaneously. This had a major advantage in the popularity of the project. It made it possible to reach numerous young people. The interactive setup and virtual friends step right into the world of the youngsters and help to empower them regarding the 6 themes. It also reduced the fear of crime from the parents. It is however not very clear to what extend the goals where reached. It was said that performance is measured on the number of group requests, group visits, analysis of evaluation sheets, assessment reports, reception reports & the number of visitors. No concrete numbers are given though. This makes it impossible to see the impact.

Strong points:

- The centre can build on an extensive knowledge base
- The centre profits from previously gained popularity
- The interactive setup connects directly to the world of youngsters/parents

Weaker points

- To keep it's attraction, this project will need continuous attention. Empowerment requires more than a 'one time' contact. It needs regular contact points to maintain focus of youngsters. However, the setup does provide the infrastructure to do so. Others themes should be easy to implement.

This is an excellent project that could easily be transfered to other countries. It is advised to expand to other EU countries, since the questions amongst/dangers for youngsters are quite parallel.

In *the Belgian project*, police department AMOW (Asse, Merchtem, Opwijk & Wemmel) decided to step into the extension of offline communication between youngsters, namely online communication, as a reaction on the high number of youngsters being confronted with cyberbullying. AMOW decided to use the popular Facebook channel and started a page. Youngsters can add the Netflik to their friends list and talk via personal message about the problem. The 'Netflik' tries to assess the situation and proposes a solution. This solution can be rather low level: get in touch with school, AWEL, parents or school that is responsible. For more serious threats, the youngster is advised to take contact with the local police station for an official complaint. The 'Netflik' tries to raise awareness in an offline context as well, by talking in classes, a promotional film,… The project has raised awareness on the problem. It gained a lot of press coverage, but schools were introduced into the project as well. Another target was

to discourage the bullies and clarifying that they can be prosecuted. Finally the project aims to encourage and empower the victim. Victims get a direct line with someone at the police force that will listen to them. All three goals signal success. A longitudinal study is however advised to make sure these goals will keep getting reached in the future as well.

Strong points:

- Over 800 users already used the 'netflik' approach. Taken into account the limited region of the police force this is impressive.
- It is an ambitious project for a local police force to take on. After all they have limited resources and decided to give this problem the attention it needs.

Weaker points:

- It should be stated that this project is limited to the geographic boundaries of the AMOW police department. It is however impossible to translate geographic boundaries to local boundaries. A broader network of 'Netfliks' is therefore strongly advised.
- The 'Netflik' can be visible in the friends list of the youngster, which can lead to counteractions. Combined with a lower self-esteem due to continues cyberbullying this can trigger negative effects as well
- There are limited resources available. Situations online can escalate very quickly. It is advised to perform a resource assessment.
- I would advise to start a longitudinal study on the effects of the 'Netflik' project to ensure that the performed actions keep meeting the goals that were set up at the start of the project.
- Another advise would be to broaden the scope: use other popular communication channels used by youngsters. This can tighten the gap to get in touch.
- Clear protocols have to be in place on how to tackle crime. It was not clear if the police officer handling the messages has a criminological/psychological/communication background and will always be able to assess the real potential danger of a problem.

Kozinets (2010) already stated that a part of social life has moved to an online content. An integrated approach by the police is required to tackle criminal behavior online as well. The Belgian project builds a good foundation for such an integrated approach. It can however be opened up to other communication channels and geographical areas, as the internet has no boundaries. One police zone has set the example, but can only do so much. Ideally every local police force has skilled people to handle cybercrime as a whole. This will be a necessity as our social life keeps expending to the online world. Not limited to, but also targeting, youngsters of course. This requires not only familiarity with the medium (not a given in all police forces), but also a form of media wisdom (Van Boeschoten, 2010). Are the tools used the right tools to reach your audience? Finally, it is advised that the key persons handling the requests have a strong psychological background to assess the problem.

The Portuguese project wants to raise awareness amongst – especially - youngsters concerning cybercrime prevention and aims to 'strengthen the moral and ethical values from which cyberspace must be build'. Promoting collaboration and cooperation between institutions &

organizations is a second goal. Finally powering 'the innovation environment' in the field of cyberspace is a third goal. The project is still ongoing, but the goals are not clearly determined. What do we have to understand by 'strengthen the moral and ethical values from which cyberspace must be build'? Who determines this? The commercial companies that support the project? Or the National Guard? Another serious flaw is that the project starts from a database of registered crime incidents by the National Guard. Not only is there a big dark number on reported crime, specific forms of cybercrime are seldom reported. This can create the wrong picture and tackle completely different problems from the ones that need attention. There's a complete lack of measuring the results and thus no way of telling this approach works or not.

A strong point is the collaboration with other institutions, but this can be a weak point as well. Other weaker points of this projects were:

- Moral in its setup, but without a clear definition of the goals to reach. It is not possible for one initiative to set the standards for cyberspace
- No measurement of results, neither is there a cost-benefit analysis in place
- Does not take the dark number into account

I would recommend extreme caution when it comes to pushing morals onto the public. This can backfire, especially when setting them in a cyberspace context. Minimal measurement tools should be put in place.

The Dutch project wants to raise awareness amongst entrepreneurs on cybersecurity. It is based on a roadshow: a buss is placed in the middle of business areas and a promo team invites entrepreneurs into the bus. Advisors of both KPN and the Dutch Association of Insurers provide the entrepreneurs with information on cybersecurity. On top of this, MKB offered 300 'ethical hacks' where entrepreneurs can let their sites checked on security issues. They also formed a partnership with KPN to offer a discounted professional service to SME's, giving these SME's (small and medium enterprises) the opportunity to work on their cybersecurity right away.

The social hacks had the power to point out the seriousness of the topic 'cybersecurity'. A good knowledge base was established and a network was formed - as well before, during as after the project – to get the information to the SME's. An option is offered to take action right away. Even though not all 'ethical hacks' where used, the project was a success. It did show how vulnerable entrepreneurs are in this connected world. The project formed an excellent starting point to build upon for future projects.

Strong points:

- Shows the need for this kind of projects
- Shows how vulnerable a particular SME is by an 'ethical hack', thus entering directly into the world of the entrepreneur and exposing their risk
- Collects knowledge to build descent knowledge base that can be searched later
- Offers the opportunity to tackle the problem

Weaker points:

- Broader scope to get directly in touch with the entrepreneurs could be advised. Even though it is remarkable and attention drawing to put an orange bus in the middle of a commercial centre, it is a bit naïve to expect that entrepreneurs can drop what they are doing to get informed on the spot. Other ways of communication (magazines, PR in local and national media) are more effective.

This is an excellent project that could easily be ported to other countries. It is advised to expand to other EU countries, since a lot of entrepreneurs (also from SME's) have sites in several EU countries. The possible risk goes broader than the Dutch borders. A lot can be gained from the exchange of information and knowledge of similar organizations.

Provisional conclusions: challenges and good practice evidence

Although the theme of the Luxembourg Presidency was 'cybercrime' in general, we can conclude that by far the largest part of the projects are focused on '*online safety of children and adolescents*'.

Generally speaking, it should be said that the prevention of cybercrime should be focused on three target groups: the children themselves, their parents, caretakers and teachers, and the third target group are the predators themselves. Because of the importance of this topic and the focus of Europe on the online safety of children, it is important to **support prevention activities with NGO's and educational sectors** to *fight child sexual exploitation online* and to train parents and their kids on the risks and dangers youngsters may face in the Internet world. Other interesting projects focused on children or youngsters will be mentioned and explained further in this conclusion.

We could see a few innovative aspects in the proposed projects, such as the focus on very young children which seems important because of the young age at which children tend to go online. Some proposed projects made use of innovative measures, like the creation of interactive games, awareness campaigns on Youtube,… Or there were some projects that took another approach in online protection of children by for example focusing self-help for on online perpetrators. Some proposed projects made use of innovative measures, like the creation of awareness campaigns on YouTube, interactive games,…

Despite great efforts being done to tackle cybercrime by a great variety of international agencies and by the EU Member States, there are still quite a few challenges lying ahead. In the following paragraphs we will give a short overview of some challenges and good practice evidence.

Belgian Better Internet Consortium (B-BICO project) is a EU-funded project (January 2015 - June 2016) under the Connection Europe Facility Programme (CEF). The B-BICO project is an innovative project that capitalises on existing knowledge, expertise and resources related to e-safety and education and the promotion of a better Internet for children in the whole territory in Belgium.

It has the ambition to create a Consortium of all Belgian actors and stakeholders involved in e-safety and online media literacy. This Consortium will work on advocating a Better Internet for children and young people. All of this is based on a qualitative mapping of existing initiatives in Belgium. Such a Consortium must gather and streamline all experts and expertise, but also concretely work together by taking joint initiatives. The ultimate goal is to protect and promote children's rights in the online environment. The target group of this Consortium and the project in general are in the first place children and young people. Some initiatives might be taken directly for them, others will target their parents, teachers and other educators or the industry partners which provide them with the platforms they use online. In line with the latest European Strategy, the focus of B-BICO is a **better** use of the Internet instead of a safer us of the Internet: work better with the skills they have. Their work will be realised on several levels and via different actions: prevention, awareness raising nature, training but also reactive response on violation of those rights.

- *Awareness-raising* activities and tools will be developed for young people about the better and safer use of internet to increase, amongst others, the development of competences such on critical thinking and media literacy.
- *Training:* Both Child Focus and Média Animation will capitalize on and further deploy its training programmes for professionals (teachers and social workers) parents and vulnerable users.
- *Prevention:* Child Focus will continue to operate its e-safety helpline via which parents, professionals, teenagers and children can obtain advice on how to deal with harmful contact (grooming), harmful conduct (sexting) or harmful content and uncomfortable or scary experiences of using online technologies. If needed, refer the reports to the appropriate organisation in charge of such topics.
- *Reactive response:* Child Focus continues to operate the hotline www.stopchildporno.be.
- By actively cooperating with members of European networks (INSAFE, BIKNET, INHOPE …), partners of this project will exchange information about best practices, participate in meetings, design, and implement a European approach.
- *Youth* will have an active role in awareness raising campaigns, tools development, analysis of trends and dissemination process.

The project builds on three building blocks: technical safety, safe use and a better use of the internet. These are all core businesses of the cross-community partnership of this project.

More projects should take the **evidence based approach**, like we could see in the German project. It needs to be stated that there is not enough emphasis on the **results of the initiatives taken**. It is not always easy to know if certain measures are efficient or not. Therefore, it stays important to perform evaluations of project, even though this is often considered difficult, money- and time-consuming. However, this does not always has to be extensive, even basic evaluation can contribute to a better understanding of what works. This is explained in the 3rd toolbox of EUCPN '*Evaluation of Crime Prevention initiatives.*'

EU Child safety online, funded by the European Commission ISEC Fund. For this project the Tilburg University (NL) work together with the Middlesex University (UK), Royal College (Ireland) and LUMSA University, Kore University of Enna and the Institute FDE in Mantua (Italy). This is an international, multidisciplinary team working across academia, law enforcement and industry in order to advance understanding of online childhood sexual abuse. The seek to draw together the evidence base on online offender and victim behaviour including online grooming, possession, collection and distribution of indecent child images, identification of policing and industry best practice in prevention. This is a research to get a view on the victims and how to prevent.
http://www.euchildsafetyonlineproject.com

The necessity **of setting up partnerships with the scientific and academic world** was stressed by the conference. With these partnerships new procedures and research methods can be established. Furthermore unprecedented forms of cybercrime, for instance in the areas of encryption technologies or artificial intelligence can be tackled by setting up these partnerships with the scientific and academic world.

Investment in primary prevention, such **as awareness raising, training and education** is essential. There were multiple projects who deal with this. Giving correct information to possible future victims, especially children, is considered highly important. However, we could learn that just informing children about the dangers, will not make them less likely to behave risky online. An effective intervention program should not focus on danger, which we could see in some proposed projects. Partnerships with universities could contribute to discovering what works and not. Continuing on the topic that it is not effective just informing children, it is noteworthy to mention that the use of interactive games, awareness campaigns on YouTube,… can work well. The Spanish project shows that it can work to spread information through YouTube, since some video's had over one million views. Clips can be very appealing, can be shared among youngsters, youngsters can and will send them when they feel that it interesting for them,… which are very strong,

iRespect, a tool that has been made in partnership of Child Focus, B-CCentre, EMSO & 'digital champion', is an awareness raising tool for children to make children aware of the consequences of their online choices. This tool includes a pedagogical kit. Its focus is on Online Privacy, intimacy, respect, cyber-harassment, challenges, e-reputation, etc.
http://www.childfocus.be/sites/default/files/irespect.pdf
http://www.childfocus.be/sites/default/files/irespect_0.pdf

Child Focus (the Belgian Foundation for Missing and Sexually Exploited Children) developed tools to encourage dialogue between children and educators. In 2012, Child Focus developed Jungle Web to reach all children through an educational and family-orientated tool, with the focus on vulnerable groups. It wants to stimulate dialogue between parents and children on a simple, but funny manner. It uses attractive visuals. It focuses several themes such as grooming, chatting, streaming, cyber-harassment, phishing, use of smartphones, e-reputation,... etc. It works with questions and challenges. Through this tool we want to encourage parents to talk about the internet with their children and so eradicate the digital divide we want to stimulate the exchange of knowledge in a positive environment and make it as easy as possible.
http://www.childfocus.be/sites/default/files/instructie_fiche_0.pdf
http://www.childfocus.be/sites/default/files/fiche_explicative.pdf

What works: playing games! Not just giving the children the information. For example: Child Focus will never go into a classroom, but teach teachers, officers,… They have to present it to the classes. On that way the peers know how to handle it.

positive and effective characteristics. The use of interactive games is another strong aspect in this project. Gamification can produce measureable results. The Romanian project, where high school students were asked to think of a play that involves online risks, is another good example of this. Gamification should be applied more often in prevention projects, especially because just informing (children) about the dangers suffices not always and will not make (children) less likely to behave risky online. Involve the audience group more, activate them, inform your audience by playing games,… are important and interesting examples which should be used more often in prevention projects.

Above the latter examples of primary prevention, **general awareness** raising by public campaigns is an important work in the prevention of cybercrime. We need to promote the large and continuous media campaigns promoting digital security. They can help avoid data breaches of sensitive personal data. Or they can claim for an intelligent use of computers, smart phones, social media and communication apps. Furthermore, the dissemination of projects and results should be further strengthened in order for policymakers to learn from each other. We hope to contribute to this through this toolbox.

An example of a general awareness campaign is the **Safer Internet Day**: organised by Insafe in February of each year to promote safer and more responsible use of online technology and mobile phones, especially among children and young people across the world. In 2016 the Safer Internet Day will be celebrated on Tuesday 9th February, with the theme of 'Play your part for a better Internet'.

Like mentioned in the theoretical paper, cybercrime is an underreported phenomenon, so it is important to increase the police reporting. Police data is under-reported for various reasons: fear of negative publicity, lack of incentive, perception that the police response will be ineffectual, no prospect of restitutionary damages, victims not realizing that they have been victimized. Many countries have strategies and approaches to increase the reporting of cybercrime, as shown in *figure 1*. Beside the underreporting of cybercrime by the police, it seems important that the police needs to be trained in relation to cybercrime. Professionals need to have decent knowledge about the dynamics and different profiles of the victims and perpetrators.

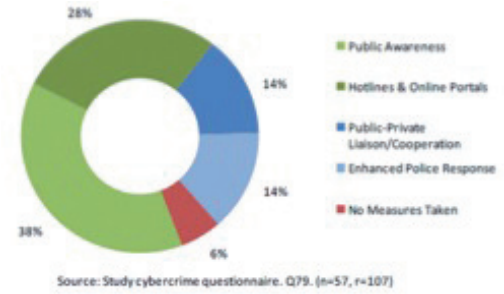


Figure 1: Measures taken to increase reporting cybercrime to police **Source**: UNODC

First Responders, the Belgian project of FCCU (Federal Computer Crime Unit, Federal Police) – based on the e-learning tool developed by the French 2CENTRE (UTT), which aims to teach police officers what they have to check and search. The first responders of the Local Police in Belgium receive an increasing amount of complaints about cyberrelated crime. To make these police officers better acquainted with digital evidence and cybercrime, a cybercrime training was launched for local police officers. Nowadays, all police officers should be able to handle potential digital evidence (identify and seize) and handle common crime cases facilitated by Internet usage. This will also allow them to give correct information to victims, who are making an official complaint, in regards to preserving the evidence. The project teaches them this by e-learning, in order to address a large audience efficiently, the product remains available as reference manual and updates can be facilitated if planned at creation time. In this Belgian project existing resources on national and international level are used.

Nevertheless, improving **data collection and registration** will support the development of more efficient action plans. One outcome of the cybercrime communication 'Towards a general policy on the fight against cybercrime'[78] may be that more information on crime is collected and that the statistics have to be improved. For many reasons, there are no reliable statistics on cybercrime. Cybercrime is a vast area and covers innumerable crimes and no common statistics system exists. Because of the difficulties arising when trying to define and identify cybercrime, cross-national comparative statistics on cybercrime are much rarer than for other crime types.

Furthermore, the conference stressed the necessity of lobbying **for harmonized legislative changes** at EU level, to fix common standards in policing against cybercrime and to discard the criminal use of virtual currencies, such as Bitcoin in particular. In the project of Sweden, for example, we could see that they do face a problem with electronic money, such as bitcoins.

[76] **European Commission (2007)**. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions. Towards a general policy on the fight against cybercrime, Brussels: Com(2007) 267 final, 22 May 2007. [http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52007DC0267]

The project of Sweden stressed the importance of establishing **strong coordination with banking sector and payment industry**. This project aimed to prevent online predators from harming children online, so this project focused – as the most projects - on 'online safety of children'. However, working together with the banking sector and payment industry can be really important too to reduce the risks of payment fraud and to encounter efficiently new forms of malware attacks.

As in many things, a **multi-disciplinary and multi-agency approach** can be considered very important. Governments have a significant role in ensuring a free and safe cyberspace. However, the private sector owns and operates significant parts of cyberspace, and so any initiative aiming to be successful in this area has to recognize its leading role. **Partnerships between government, private sector, agencies, the non-profit sector,…** whatever the level, are highly recommendable. Therefore, the project of Sweden is one example of a successful collaboration between public authorities, the private sector, and the non-profit sector. However, this cooperation needs to be encouraged even more. Furthermore, providers should also be made aware of the criminal activities that happen in their cyberspace. The Danish project gave a good example of how providers of chatrooms could be made aware of these risks and could even contribute in the prevention of future risks.

On the other hand, the private sector does not only have to recognize its leasing role in preventing cybercrime, since this phenomenon is, after theft, the biggest criminal threat to companies. However companies still take this form of crime not seriously. To stress the importance of the impact of cybercrime on companies, it was important that at least one, the Dutch, project focused on cybercrime as criminal threat to companies. Despite the general focus on 'online safety of children and adolescents' in the conference, the award went to the Dutch project, an awareness campaign based on a roadshow through the country, to make entrepreneurs more aware of the impact of cybercrime on their businesses. It is a fact that most of the projects which were submitted for the ECPA, focused on 'online safety for children'. Also Europe attaches high importance on this phenomenon. However it should not be forgotten that there are other forms of cybercrime that deserve our attention as well. Is has to be stressed that companies do not always react good on cybercrimes: first they want to solve the problems themselves, but it should not have anything to do with the secrets of the company. So sensibilisation is very important in this.

Cybercrime is a phenomenon that every EU-country faces and which is a cross-border crime. Therefore, the exchange of ideas, knowledge, practices and research is extremely important. As an EU-wide Network, the EUCPN plays a significant role in exchanging information, knowledge and practices between the Member States. By doing so, Members can learn from each other in finding other and better ways in preventing and tackling cybercrime. Additionally, the EUCPN also serves as a platform where specific questions for information can be directly asked to all Members.

Part 3 Overview ECPA 2015 projects

Overview ECPA 2015 projects

"Net Cop" (BE)

Short description:
The police department AMOW is initiating the battle against cyber bullying on social media. The 'Net Cop' will be answering high school students' questions on her 'netflik amow' Facebook page, giving them advice on how to deal with cyber bullying.

Teenagers can send a friend request to the 'Netflik AMOW'. After the request is accepted the person can talk to her over Facebook's private messaging system. Then, an evaluation of the message is made and transferred to other organisations as JAC (Youth Advisory Centre), Awel (Child and youth call centre) or other social partners. If things are really serious the youngster is advised to press charges with police. The Net cop can also advise the youngster to better secure their Facebook profile.

Start/duration:
The project started on 24 April 2015 and is still running.

Background research:
The project is based on a survey executed by a student Social Work of the Odisee High School Brussels on the subject 'Cyber bullying on social media'. She interrogated 1350 students, aged between 12 and 18 years old, studying in Asse and Opwijk. The results of this survey showed that a staggering 13% of the students had already been victim of cyber bullying, and 5% admitted to have been the cyber bully.

Then the students were asked by means of which communication form they would like to be informed of the measures they can take to prevent cyber bullying. A great part of the students indicated that they prefer to be informed by a police officer by means of social media.

Budget:
The project is low cost: the creation of a profile on Facebook or social media is free; other small costs are the making of flyers and posters (5000 euros), IT (500 euros, …

Finally, one person has to manage the incoming mails and make sure that the right social partner is addressed.

Type of evaluation:
The general public was enthusiastic about the project. Proof lies in the attention the project got in local and national media. The schools and social services were also enthusiastic and wanted to work together to optimise the flow of messages and help. Many students also showed their interest and were excited that they were listened to and asked for their opinion. It is almost impossible to measure an outcome or impact on short term.

By the end of October 2015, all the film performances in the schools will be completed and then they will be evaluated.

Actor conducting evaluation/timing:
Internal: Police department AMOW (cities of Asse, Merchtem, Opwijk and Wemmel)
External: participating partners.

Type of data collection method:
urvey executed by a student Social Work of the Odisee High School Brussels on the subject 'Cyber bullying on social media'

Further information:
General information on the project: http://eucpn.org/document/net-cop

Other related links: Police department AMOW www.amow.be

https://www.facebook.com/Netflik-Amow-990605580981012/timeline/

http://www.expatica.com/be/news/country-news/Flander-Net-cop-to-fight-cyber-bullying_471288.html;

http://deredactie.be/cm/vrtnieuws.english/News/1.2319288

E-Bezpečí (E-Safety) (CZ)

Short description:
E-Bezpeci is a national certified project dealing with a comprehensive solution to the issue of risky behaviour on the Internet. It specializes in prevention, education, research and intervention.

Topics:
a) cyberbullying and sexting,
b) cybergrooming ,
c) cyberstalking and stalking,
d) risks of social networks and other potentially risky virtual environments,
e) misuse of personal data in an electronic media,
f) netolism.

The basic starting point of the project is field work with various target groups, lectures, implementation of preventive educational events, etc. Lectures/discussions map specific hazardous phenomena, offers the possibility of prevention strategies and defences against invaders. The target groups of the project are primary school pupils (aged 8 years), teachers, social phenomena prevention officers etc.

Annually about 6,500 pupils and students, 500 parents and 300 teachers pass through project training. Annually, the project team implements 150-200 training events. Total of 33 000 pupils underwent E-Bezpeci project training.

Start/duration:
The project started on 01 January 2008 and is still running.

Background research:
It was a quantitative analysis of risky behaviour among children in the Internet environment on a sample of over 10,000 respondents. The results were recorded in the RIV system (http://www.isvav.cz/projectDetail.do?rowId=GP406%2F08%2FP106).

The results were published in the form of several publications - Risks of electronic communication I, II, Risk of internet communication III, IV, series of infographics, etc.

Analysis was conducted by a team of the Centre for the prevention of risky virtual communication Palacky University in Olomouc (analysis takes place regularly on an annual basis).

Specifically, data was obtained from respondents aged 11-15 and 16-17 years, with measured:

a) the incidence of cyberbullying (forms, platforms) from the perspective of the victims,
b) the incidence of cyberbullying (forms, platforms) from the perspective of the attackers,
c) sexting and its occurrence,
d) cybergrooming, personal meetings with strangers,
e) the sharing of personal data on the internet,
f) the perception of truth and lies on the Internet,
g) social networks and web services that children use most frequently.

The outputs are regularly published in the media nationwide, but also in journals.

Budget:
The project is implemented through its own resources, facilities Palacky University in Olomouc, grant resources, the Ministry of Education, Ministry of Interior, the City of Olomouc, Ostrava, Olomouc Region financial subsidies, financial subsidies to the private sector - eg., T-Mobile, Vodafone, Seznam.cz, Google, etc.

Type of evaluation:
Evaluation includes more than 100 items, eg. if the program is accessible, professional care for clients, coordinating cooperation with public report, program evaluation, monitoring, maintaining and developing the quality provided by the program, an external evaluation, the existence of a code of rights of clients, professional quality of project team staff, collaboration with others, measures to deal with unexpected situations etc.

All parts of the project are judged to be of high quality, fulfilling all the criteria required for the project according to standards of primary prevention programs. The last evaluation took place in November, 2014.

Actor conducting evaluation/timing:
Evaluations are conducted by external evaluators:
1. The Ministry of Education
2. Police officers
3. Professionals in educational and psychological counselling.

Internal evaluation is then carried out 2 times a year by project managers.

Type of data collection method:
quantitative analysis.

Further information

General information on the project: http://eucpn.org/document/e-safety
Other related links: **Website of project** - www.e-bezpeci.cz

Another part of project
www.sexting.cz
www.napisnam.cz
www.netolismus.cz
www.ditevohrozeni.cz
www.prvok.upol.cz

Social networks
facebook.com/ebezpeci

Annual Reports (2014, CZ)
http://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/70-vyroni-zprava-2014

Videos from education
https://www.youtube.com/user/ebezpeci

Our activities in media:
E-Bezpečí
http://e-bezpeci.cz/index.php/tiskove-zpravy/

Seznam BLOG
http://seznam.seznamblog.cz/post/

Seznam se bezpečně!
http://seznamsebezpecne.cz/novinky/vyzkum-rizikoveho-chovani-deti-v-prostredi-internetu-2014

Žurnál UP
http://www.zurnal.upol.cz/nc/pdf/zprava/news/2593/

Reflex
http://www.reflex.cz/clanek/zajimavosti/57784/

TV Prima Zprávy
http://play.iprima.cz

TV Nova
http://tn.nova.cz/clanek

Eurozprávy
http://izeny.eurozpravy.cz/aktuality

IDNES
http://olomouc.idnes.cz/

O2 Active
http://zpravy.o2active.cz/detail.aspx?id=227180
Finanční noviny

News HUB
http://cz.newshub.org/

Google CZ (G+)
https://plus.google.com/118251399271079540989/posts/8U3iFEhLtEv
https://www.facebook.com/googlecz?hc_location=timeline

BBC Studio ZET
http://www.zet.cz/
http://www.prvok.upol.cz/index.php/news
http://www.upol.cz/nc/en/news/clanek/hi-lets-meet-in-person-40-of-teens-would-agree-to-such-an-online-request/

Medienhelden (Media Heroes) (DE)

Short description:

"Medienhelden" is a universal, manualized, theoretically based, and carefully evaluated (process, impact, implementation evaluation) preventive intervention program for the school context (7th-9th graders), including teachers and parents. Objectives are: Prevention of cyberbullying/-victimization and promotion of online self-protection skills and social skills. The program relies mainly on social learning and cognitive-behavioral methods and works with activating methods (peer-to-peer and peer-to-parent-tutoring). The program is intended for implementation in classrooms and covers ten weeks with sessions of 90 minutes each as part of a curriculum. A shortened one-day-version (4 sessions of 90 minutes) was also developed. The program manual provides school teachers with all materials needed to carry out the program. A longitudinal, randomized control study proved the positive effects of the program (e.g. reduction in cyberbullying, improved skills/empathy). A train-the-trainer approach is available for the purpose of implementation, offered by licenced external enterprises and partners.

Start/duration:

The development and evaluation of the project at Freie Universität Berlin started 2010 and was finished in 2011/2012.

Background research:

The context and state-of-the-art was analysed carefully before initiating the project:

- A thoroughly review of the scientific literature regarding cyberbullying and opportunities to prevent cyberbullying, -victimization and traditional bullying/victimization respectively.
- Our reviews revealed that cyberbullying victims and perpetrators are often peers from the school environment, and that there is a lack of evaluated preventive interventions for the school environment. Thus, we consulted school teachers to analyse the needs and requirements for cyberbullying prevention at schools.
- We conducted focus groups with adolescents to analyse the needs and requirements for cyberbullying prevention at schools from their perspective.
- As German representative of the EU COST Action IS0801 "Cyberbullying: coping with negative and enhancing positive uses of new technologies, in relationships in educational settings" (https://sites.google.com/site/costis0801/) we consulted with representatives of the participating 28 states.

Review and focus group results have been published as well as guidelines for preventing cyberbullying in the school environment (https://sites.google.com/site/costis0801/guideline).

Budget:
The research and development project, including longitudinal evaluation was supported by a research grant from the DAPHNE III program (see Item 19) and including about 110.000€ (including own costs).
The implementation project includes different financing options to pay the direct train-the-trainer costs, with training courses available via external enterprises (e.g. see http://www.medienhelden-ausbildung.de/).

The program materials are available via a book publisher (39,90€).

Type of evaluation:
A process evaluation, inter alia using standardized questionnaires, has been conducted internally.

Actor conducting evaluation/timing:
Internal: Freie Universität Berlin

Type of data collection method:
The research team had weekly internal meetings, regular skype, telephone and (every 3-5 months) personal meetings with members of the entire ECIP project consortium. The research team was in close contact with participating schools/teachers to keep to the tight schedule. Staff members had to complete hourly time sheets during the project phase. These measures helped to keep to the tight schedule and barriers and other obstacles would have been evident in a timely manner to mitigate the
situation by

Further information
General information on the project: http://eucpn.org/document/medienhelden-media-heroes

Other related links:
1. German project website (research/development project):
   www.medienhelden-projekt.de (German)

2. European research project: www.bullyingandcyber.net/en/ (English), chose "ECIP" (European Cyberbullying Intervention Project) on the left bar on the website.

3. Examples of websites by implementation partners:
   - Austria: www.medienhelden.at (German)
   - Germany: www.stravio.de/index.php?id=22 and www.medienhelden-ausbildung.de (both German) - see also http://www.stravio.de/uploads/media/Flyer_medienhelden.pdf

4. Program manual (including all of the implementation materials) (German):
   Schultze-Krumbholz, A., Zagorscak, P., Siebenbrock, A., & Scheithauer, H. (2012). Medienhelden: Unterrichtsmanual zur Förderung von Medienkompetenz und Prävention von Cybermobbing. München: Reinhardt Verlag. Available via publisher's website www.reinhardt-verlag.de/de/titel/51405/Medienhelden/978-3-497-02281-6

The program is supported by „WEISSER RING".

5. Description in "Grüne Liste Prävention" (German):
   www.gruene-liste-praevention.de/nano.cms/datenbank/programm/51

6. See enclosed selected manuscripts (publications describing the program and the evaluation study) (English)

7. List of selected publications: (English and German)
   - Chaux, E., Velásquez, A.M., Schultze-Krumbholz, A., & Scheithauer, H. (revision submitted). Effects on traditional bullying of the cyberbullying prevention program Media Heroes. Aggressive Behavior.
   - Schultze-Krumbholz, A., Schultze, M., Zagorscak, P., Wölfer, R., & Scheithauer, H. (2015). Can a classroom-based preventive intervention reduce cyberbullying? – Long-term effects of the "Media Heroes" program. Aggressive Behavior, Online First, 1-10. doi: 10.1002/ab.21613
   - Schultze-Krumbholz, A., Zagorscak, P., Wölfer, R., & Scheithauer, H. (2014). Prävention von Cybermobbing und Reduzierung aggressiven Verhaltens Jugendlicher durch das Programm Medienhelden: Ergebnisse einer Evaluationsstudie. Diskurs Kindheits- und Jugendforschung, 9 (1), 61-79.
   - Schultze-Krumbholz, A., Zagorscak, P., Wölfer, R., & Scheithauer, H. (2014). Das Medienhelden-Programm zur Förderung von Medienkompetenz und Prävention von Cybermobbing: Konzept und Ergebnisse aus der Evaluation. Praxis der Kinderpsychologie und Kinderpsychiatrie, 63, 379-394.
   - Wölfer, R., Schultze-Krumbholz, A., Zagorscak, P., Jäkel, A., Göbel, K., & Scheithauer, H. (2014). Prevention 2.0: Targeting cyberbullying @ school. Prevention Science, 15, 879-887. doi: 10.1007/s11121-013-0438-y

Moderator education / Digital Playground (DK)

Short description:

Moderator Education

Online moderators on social networking sites for children (SNS) can play a crucial role in preventing abuse and conflicts in chatrooms, as they have direct contact with children.

The “moderator Education” aims to empower online moderators to better prevent online harassment, bullying and online sexual abuse by teaching moderators how to understand and how to take action in three risk areas: sexual abuse and grooming, cyber bullying and online conflicts. The education uses three approaches to contributing knowledge and skills: face-to-face education, e-learning and helpdesk. More than 600 moderators have completed the education.

The education concept has been developed in close co-operation between Social networking providers and Save the Children Denmark. Viewing online moderators as a central resource to prevent online abuse of children is innovative and has a potential all over Europe where the number of providers of social networking sites for children is on the rise.

Start/duration:

The project started on 01 March 2008 and is still running but with no funding since 31 December 2013.

Background research:

Jon Kristian Lange at Save the Children (Master in psychology and communication, former schoolteacher and the creator of the education) interviewed more than 50 children and 20 moderators about good and bad things on being online. Furthermore, Save the Children followed and analysed communication between a moderator and the users on a particular site during 12 months. All this data lead to the three pillars in the education; conflict management, cyber bullying and grooming.

Budget:
The Egmont Foundation donated 525.000 DKK (approx. 70.000 EUR) in 2008 and 790.000 DKK (approx. 105.000 EUR) in 2010.

These amounts covered salary, travel expenses and development of e-learning modules.

Type of evaluation:
Save the Children use the feedback from companies and moderators as a way of evaluating the impact.

Following the education, we have conducted follow-up meetings with the educated moderators, to gauge whether they applied the education. The moderators we talked to were in fact using the skills gained in education in their daily practices.

Save the children meet every year with the certified companies to talk about new trends and explore new educational needs.

Embedded in the education is a policy plan that guides the SNS company in how to raise awareness within the company around illegal or offending behaviour.

As part of the education the companies/SNS have to commit and ensure the time of 1- 2 moderators to “maintain” the level of education in the company and keep contact with Save the Children.

Actor conducting evaluation/timing:
Internal: Red Barnet / Save the Children Denmark

Type of data collection method:
Process evaluation in the form of an anonymous evaluation questionnaire with plenty of room for comments.

Further information
General information on the project:
http://eucpn.org/document/moderator-education-digital-playground

Other related links: http://www.sikkerchat.dk/da-DK/Moderator.aspx
Most of the material is in Danish. However, the materials for printing and the grooming e-learning module are translated into English.

Digital Safety Game (DSG) (EE)

Short description:

Game is designed for people who want to renew or enhance their digital safety knowledge with the help of a fun seductive game.

This game is for 1-6 people you can as individual or in teams. Recommended target audience is 16 years and up. Best suitable for vocational, professional higher and university education programs. Takes about 20...25 minutes to play a single game. ICT skills are needed. During playing real life examples, storytelling and case importance description are encouraged besides the actual fact knowledge.

The goal is to answer as many questions as possible and win after accumulating a required number (e.g. 3 if agreed so) of cards. The game is designed so the inquirer has to formulate a question and evaluate whether the answer is correct or not. Discussions and real life examples why this knowledge is important are encouraged.

There are six different categories - social engineering, privacy, network, internet, hacking, malware and 54 cards in the game.

Start/duration:

The project ran from 01 March 2013 untill 20 June 2015.

Background research:

The context was analysed by Digital Safety Lab with purpose to develop study and research and learning direction of digital safety at Tallinn University, Institute of Informatics. Research has been made during 2011-2015 as described in section II.1 by 6 researchers (2 scientists and 4 doctoral students). There were these 14 schools and youth centers involved as mentioned in section II.1. There were around 10 000 students involved into testing group in different schools.

The purpose of research group is to investigate digital safety area and use accomplished competence in both academic and business projects. The lab is managed by Kaido Kikkas, PhD and Andro Kull, PhD and is still active.

Budget:
The overal project cost was 5980 € and 2000 copies printing cost were 3700 € of that. One pack cost 2,99 €.

As there were so many iterations then game got ready around a year later than preliminary expected. Almost whole game was revamped during improvements. There were around 300 working hours spent during development process.

Type of evaluation:
Impact evaluation.

Actor conducting evaluation/timing:
Internal: Tallinn University Digital Safety Lab.

Type of data collection method:
Feedback from users of the game orally or by e-mail.

Further information
General information on the project: http://eucpn.org/document/digital-safety-game-dsg

The project's website: http://dsg.onu.ee/

Preventing and fighting the rise of online Sextortion and Gender Based Digital Violence (ES)

Short description:

To prevent the rise of Sextortion and Gender Based Digital Violence, PantallasAmigas has developed various awareness campaigns in conjunction of related educational tools. The goal of the project is to have all those resources available online freely, as many victims of these type of cybercrimes look for help online privately, rarely asking for help to others, or reporting to the police. Acting quickly and providing tools to ask for help is essential to prevent the problem from complicating, and to avoid the victim to feel trapped with no solution.

The tools and resources created to achieve the goal of this project are comprised of:

- Various awareness campaigns on YouTube about sexting and sextortion.
- Two interactive games to prevent and fight sextortion online.
- A booklet or guide for the teacher about gender based violence online.
- Various thematic websites with information, news, studies, and a form to report any crimes and/or ask for help

Start/duration:

The project started on 07 May 2009 and is still running and is comprised of several of the following elements: awareness campaigns, interactive games, booklets and guides for teachers and educators, intervention protocols for victims, blogs and complaint forms.

Background research:

Smartphone penetration in Spain in 2008 was still not very high, and few adolescents practiced sexting and cybersex back then, but it was a trend growing very rapidly in those countries where Internet and smartphone penetration was higher (Canada, UK, United States). This context would be replicated in Spain and in many other countries in a matter of one or two years, so PantallasAmigas decided to start working on the prevention work before the trend was common among Spanish youngsters.

Pantallas Amigas published a comprehensive study3 on a booklet about sexting and its risks on 2011, in collaboration with INCIBE (Ministry of Industry):
https://www.incibe.es/pressRoom/Prensa/Actualidad_INCIBE/Presentacion_Guia_Sexting/?year=2011

Budget:

- videos sexting (2009): 9000€
- 10 videos of sexting (2014): 30.000€
- Sexting.es: 4000€
- Sextorsion.com: 4000€
- Decalogovictimasextorsion.com: 20.000€
- Guide for the prevention of sexting (2011): 10.000€
- Animation: sexting awareness campaign (2009): 3000€
- Educational DVD, “Amy_16, a story of sextortion”: 12.000€
- Booklet for teachers, “Sexual Violence on the Internet.Know it! Fight it!”: 10.000€

Type of evaluation:

Impact evaluation measured trough Google Analytics (for websites) or with YouTube Analytics (for the awareness campaigns).

Actor conducting evaluation/timing:

External: governmental agencies that work on the promotion of equality in the society, and in the prevention of gender based violence

Type of data collection method:

/

Further information

General information on the project: http://eucpn.org/document/preventing-and-fighting-rise-online-sextortion-and-gender-based-digital-violence

For more information:
A chapter for Harvard and UNICEF’s Digitally Connected ebook was written to explain the work on this ongoing project. The chapter is titled “Sexting: Teens, Sex, Smartphones and the Rise of Sextortion and Gender Based Digital Violence” and is available in the following link: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2585686

The full project is at the moment available only in Spanish in the following links:
www.sexting.es

www.pantallasamigas.net/xunta/nonsexting

www.sextorsion.com

www.decalogovictimasextorsion.com

http://www.pantallasamigas.net/recursos-educativos-materiales-didacticos/Amy-16-una-historia-de-sextorsion-violencia-digital-sexual-genero-adolescente/

http://www.pantallasamigas.net/recursos-educativos-materiales-didacticos/guia-violencia-digital-sexual-genero-adolescente/

www.youtube.com/playlist?list=PL17350D2F33BC2602

www.youtube.com/playlist?list=PLUGAcyUkQe0qLW6UARPMKIU6SlX-l8t4L

The first awareness campaign for the prevention of risks associated to the practice of sexting is also available in English:
https://www.youtube.com/playlist?list=PLEA7DD2511065ADB7

Two animations related to sextortion awareness have been translated to other languages, but are not available yet publicly, as parts of the project are still not translated. They can be viewed in the following lnks:

- Sextortion (blackmail) awareness campaign in English:
  https://drive.google.com/a/pantallasamigas.net/file/d/0Bz7v-yb5YYS-aHNuaUtQWEFJbzg/view

- Sextortion (sexual violence) awareness campaign in French:
  https://drive.google.com/file/d/0B6rabuJpC6OFV2VCd1RneXA0Zzg/view?usp=sharing

Croga.fi - “I take the responsibility” online self-help material (FI)

Short description:
Otanvastuun.fi is a free and easily accessible online self-help material for people who are worried about their sexual interest and/or online behavior regarding children, or child sexual abuse images.

The material introduces a new and innovative approach to prevent online child sexual abuse by focusing on potential offenders and their motives, and by helping them to chance their own problematic thinking and behavior.

The project is (co-)funded by the Finnish Ministry of Justice and responds to the obligation of the European members states to take all actions to prevent child sexual abuse.

Several national and international partners and stakeholders have been involved in the project, of which convicted sexual offenders have had a significant role.

The media coverage around the project has been wide and the feedback has been very positive. The number of the unique visits paid to the web site since its publication Jan 2015 is 13 108.

Start/duration:
The project started on 13 May 2011 and is still running.

Background research:
Research in the area of online child sexual abuse is limited in Finland. The actors working in the field of child sexual abuse prevention were identified and contacted. Visits were paid to Criminal Sanctions Agency, Forensic Child and Adolescent Psychiatric Unit, Psychology Department at the Åbo Akademi University, Family federation of Finland, and Sexpo Foundation. This provided extensive information about the newest research on sex offenders and offender rehabilitation in Finland and internationally. The Riihimäki Prison was also contacted at an early phase and plans were made on how to engage sex offenders in the project. Project staff participated in two trainings focusing specifically on online child sexual abuse in UK and visited a preventative project “Dunkelfeld” in Germany.

Budget:
Funding of 14 000 euros enabled the translation, design and technical implementation of the material.

The adaption of the material into Finnish context required more time and resources than was initially planned, and the project activities were integrated into other child protection programme activities, and divided into several years. All and all, the estimated work time was thirteen person months. The project has evolved beyond the original funding and achieved more than was initially planned.

Type of evaluation:
An outcome / impact evaluation of the material has not (yet) been conducted. The material was published in January 2015 and it is too early for the impact evaluation.

Actor conducting evaluation/timing:
External: project partners.

Type of data collection method:
Sex offenders were interviewed at the onset, in the middle and in the end of the project, and their feedback was used as monitoring and evaluation tool to keep the project on the right track.

The project partners also assessed the material several times during the process and gave their views on the content. The web site structure was also assessed before the material was put online.

Further information
General information on the project:
http://eucpn.org/document/crogafi-i-take-responsibility-online-self-help-material

More information on: www.otanvastuun.fi

http://www.pelastakaalapset.fi/en/how-we-work/children-and-digital-media/finnish-hotline-nettivihje/
Save the Children internal news article attached (last page) .

"Face to Face - How to keep connected with yourself" ("Face to Face : Comment rester connecté-e avec toi-même ?") (FR)

Short description:
Carried out by the Seine-Saint-Denis department (local council), situated near Paris (France), the "Face to Face: How to Keep Connected with Yourself" project aims at giving young people practical tools to avoid being victim of cybercrime.

The originality of the project is that it is based on an interactive, user-friendly exhibition that includes a specifically designed social media called "Face to Face". By navigating through the exhibition and the Face to Face social media, youngsters learn how to protect their identity, data and contact lists and to avoid common cyber threats such as sexting and bullying.

The project also includes the organisation of special events and debate-meetings with local practitioners and relevant institutions (education, social and youth welfare, judicial system).
The exhibition is located in the youth centre Tête à Tête, situated in one of the largest commercial malls of the Île de France region, in Rosny 2.

Start/duration:
The project started in October 2014 and is still running.

Background research:
Project was mainly set up to ensure that reception centres had up-to-date materials, knowledge, practices, and ability to counter trafficking and labour exploitation of asylum seekers and to assist the victims.

Budget:
The total budget for one year is €252,000. The main expense items are the scenography, the sets of the exhibition and the specific tools designed for the project (total €78,000); the renting of the space (€57,300), and wages (€87,000).

Type of evaluation:
Because the project is still ongoing as of October 2014 so we haven't yet conducted a full evaluation.

Actor conducting evaluation/timing:
/

Type of data collection method:
Although the action is still ongoing (October 2015) so it has not yet been fully evaluated. However, we base our current assessment on:

- the number of requests for group visits
- the number of group visits carried out
- the analysis of the "evaluation sheets" given to each participant in collective visits
- the assessment reports prepared by each of the professionals who intervene in the scheme
- the "reception reports" prepared by speakers and moderators
- the total number of visitors

Further information
General information on the project:
http://eucpn.org/document/face-face-how-keep-connected-yourself

More information on:
http://efus.eu/fr/topics/risks-forms-of-crime/substance-abuse/public/2742/
https://www.seine-saint-denis.fr/Tete-a-Tete,206.html
https://www.seine-saint-denis.fr/Mission-metropolitaine-de-5256.html
http://www.dsden93.ac-creteil.fr/spip/IMG/pdf/DIVEL_-_Annexe2.pdf

Safety and Protection of Children on the Internet (HR)

Short description:

The aim of the project ”Safety and Protection of Children on the Internet“ is to increase the level of knowledge and awareness regarding the consequences of Internet and social networks abuse, as well as the ways of safer Internet use and protection while using the Internet. Also, its purpose is contribution to general safety of children as Internet users by educating target groups about responsible and conscientious Internet approach. The implementation of the project activities brings promotion of the knowledge regarding possibilities and consequences of abuse of contemporary technology such as computers, mobile phones, Internet and social networks with children, the young, parents and professional assistants. It also provides reduction of criminal activity that is harmful for the children, and which is a result of Internet abuse, as well as documented cases of bullying. Finally, it raises the level of knowledge and awareness regarding importance of safe Internet.

Start/duration:

Project activities implementation started on January 1, 2012 and the project is still conducted. The ending of the project implementation is planned for August 31, 2020. Given the positive outcomes and the interest of the target group, the project implementation is also conducted in coming years. However, every year adjustments of the project activities were made according to the recommendations and guidelines of the users and experts involved in the implementation of the activities. Namely, the aim of the project is to give high-quality and comprehensive support in the field of cybercrime prevention, with the special emphasis on cyberbullying amongst the most sensitive group – the children. That is why it is very important to adjust project activities continually to the needs and interests of the target group. Project activities implementation started on the regional level. However, bearing in mind the accomplished results and the impact of the project activities, the next phase is the implementation of the project activities on the national level, and inclusion of experts from different state and public institutions and organizations in the project, as well as the experts from civil society organizations that deal with the above mentioned issue across the Republic of Croatia.

Background research:

The data used in planning of the project activities were a result of the analysis of the available data taken from authorities, institutions and organizations of the civil society, local government

and recognized experts in a community. The research of the Polyclinic for Children Protection in Zagreb, in which 4000 students from 19 primary schools and 2 secondary schools participated, has shown the following: 73% of the children has some experience in using Internet, while 58% of children use it on a daily basis. The research has shown that almost 18% children aged 12-15 was a victim of some sort of cyberbullying. 62% of children, out of all the children that were exposed to cyberbullying, said that the bully was someone they knew, or even a classmate, and 27% of the children was exposed to messages with the sexual content (photographs of naked people, sexual activity..)

Budget:
Anticipated expenses are divided into the financial, i.e. material ones, and human resources expenses. Conducting project activities includes only the expenses for the work of a police officer, project manager and material expenses, whereas the expenses of the professional assistants from partner and cooperative organizations are a part of their pay checks.

Expenses of the police officer's engagement within their working hours (working hour) – 300 hours x 52 = 15,600.00 kn

Stationery expenses required for preparation of documents and education materials – 20 pieces x 10 = 200.00 kn

Expenses of using a business vehicle – 2000 km = 15,040.00 kn

Expenses of making the promotive materials (200 pieces of posters x 20 kn and 5000 pieces of flyers x 1 kn = 9,000.00 kn

Expenses of making a video = 6,000.00 kn
The above mentioned expenses apply to a period of one year.

Type of evaluation:
The external evaluation of the effects of the project activities is planned at the end of the project activities in 2020.

Actor conducting evaluation/timing:
Internal: Police Directorate and the Ministry of the Interior.
External: outside independent collaborator with the experience in conducting project evaluation.

Type of data collection method:
Quantitative and qualitative monitoring tools and techniques (monthly reports, feedback, …).

Further information
General information on the project: http://eucpn.org/document/safety-and-protection-children-internet

For more information:
http://osjecko-baranjska.policija.hr/MainPu.aspx?id=9831

http://osjecko-baranjska.policija.hr/MainPu.aspx?id=207929

http://osjecko-baranjska.policija.hr/MainPu.aspx?id=149349

http://policija.hr/MainPu.aspx?id=186709

http://os-ibslovak-jelisavac.skole.hr/

http://www.gimnazija-agmatosa-dj.skole.hr/upload/gimnazija-agmatosa-dj/newsattach/548/Popis_prev__projekata--_srednja_skola.pdf

http://klasje.hr/odrzano-predavanje-o-zastiti-djece-na-internetu/

http://klasje.hr/category/vijesti-2/page/2/

http://www.nasice.com/vijesti/54-nasice2013/puz2013/191-nasice1692011.html

http://www.nasice.com/vijesti/54-nasice2013/puz2013/3978-na%C5%A1ice-sigurnost-i-za%C5%A1tita-djece-na-internetu.html

http://www.osijek031.com/osijek.php?topic_id=43535

http://www.icm-osijek.info/index.php/obrazovanje/zanimljivo-korisno/1850-ucimo-o-zastiti-osobnih-podataka-na-internetu-u-avenue-mallu-osijek

http://www.azoo.hr/index.php?option=com_content&view=article&id=2751:struni-skupovi-sigurnost-i-zatita-djece-na-internetu&catid=277:informatika&Itemid=115

http://www.osijek.hr/index.php/cro/Novosti/POTPISAN-SPORAZUM-O-SURADNJI-IZMEDU-GRADA-OSIJEKA-I-PU-OSJECKO-BARANJSKE

https://pogledkrozprozor.wordpress.com/2011/08/31/strucni-skupovi-sigurnost-i-zatita-djece-na-internetu/

http://www.rkud-darda.org/nacionalni-projekt-imam-izbor-obiljezavanje-svjetskog-dana-roma-2015/

http://www.nasa-djeca-os.hr/o-nama/novosti/108-seminar-sigurnost-djece-na-internetu.html

http://www.cnzd.org/site2/index.php?searchword=internet&searchphrase=all&option=com_search

http://osijek.avenuemall.hr/ucimo-o-zastiti-osobnih-podataka-na-internetu

http://www.epicentar-slavonije.com/index.php/nagradezabava/35-os/23-sigurnost-i-zastita-djece-na-internetu

http://www.vukovar.hr/kultura-i-obrazovanje/obrazovanje/7094-vukovarski-gimnazijalci-obiljezili-dan-sigurnijeg-interneta-pod-sloganom-let-s-create-a-better-internet-together

http://download14.documents.tips/uploads/check_up14/322015/55bed34cbb61ebfd3c8b4604.pdf

http://www.ss-valpovo.hr/joomla/index.php?option=com_content&view=article&id=899:prevencija-ovisnosti-zdrav-za-pet&catid=37:posjete&Itemid=70

http://www.novilist.hr/Znanost-i-tehnologija/Tehnologija/Kako-sprijeciti-epidemiju-nasilja-na-drustvenim-mrezama

http://www.novilist.hr/Znanost-i-tehnologija/Tehnologija/Na-facebooku-30-posto-profila-lazno-koriste-ih-za-maltretiranje-i-igrice

http://www.vijesti.rtl.hr/novosti/645853/mali-web-detektivi-jedini-u-hrvatskoj-odsad-stite-vrsnjake/

http://www.lokalnahrvatska.hr/vijest.php?rss=196658

www.cnzd.org

www.csi.hr

http://www.skole.hr/veliki-odmor/tehnologija?news_id=9375

http://www.boljiinternet2015.com/

A TABBY (Threat Assessment of Bullying Behaviour in Youth) in Internet and TABBY Trip in EU (HU)

Short description:

The TABBY projects aim to increase knowledge, skills to protect young people when using internet, mobile communications, social networks, being in school but also off-campus from victimisation by peers or other youngsters or adults by setting up a system for school officials and students themselves for the identification of risk factors and assessment of cyberbullying, cyber threats and sexting, and take adequate preventive actions to protect themselves and victims from such noxious behaviours. The Tabby approach is an effective and efficient approach for risk assessment and management of cyberbullying incidents. The Tabby Trip approach is composed of an online self-assessment of risks tool, videos, booklet for teachers, but also of a so called “serious educational videogame” aiming at increasing awareness and eventually, hopefully change any risky behaviour.

Start/duration:

The project started on December 2011 and was finished on 20 January 2015.

Background research:

The Tabby project applied a longitudinal data collection. Before the introduction of the complex program (which included the teacher training, the peer mentor training, the program monitoring, and the online video game), the students’ level and forms of risk in the involvement in school- and cyberbullying was assessed. For the assessment different methods were used: (1) focus group sessions were held with teachers and students (separately) in order to find out the level of risk and the forms of school- and cyberbullying in Hungary; (2) The participating schools assessed their students’ risk by administering the Tabby toolkit – that is, the online questionnaire. The students of the participating schools were identified by the project code and the student ID included.

Budget:

website management (1500 EUR),
administrative costs were

- 2420 EUR in ‘TABBY in Internet’
- and 1989 EUR in ‘Tabby in trip EU’,

Travelling costs were
- 1214 EUR project 'TABBY in Internet'
- and in 'Tabby trip in EU' were 6536 EUR.

Material costs were the following:
- 420 EUR for 100 handbooks and 4 videos.

Human resources were
- 26 250 EUR in Tabby in 'Trip EU'
- and 27.500 EUR in 'Tabby in Internet'.

Type of evaluation:
impact assessment evaluation. Monthly monitoring of the needs assessment and the results assessment.

Actor conducting evaluation/timing:
Internal: CEO -ESZTER Foundation

Type of data collection method:
Monitoring.

Further information
General information on the project:
http://eucpn.org/document/tabby-threat-assessment-bullying-behaviour-youth-internet-and-tabby-trip-eu

The project's website: http://tabby.eu/

iGloss@1.0 – Online Deviant Behaviour Lexicon (IT)

Short description:
iGloss@ 1.0 is a useful consultation instrument created by Juvenile Justice Department, and by the IFOS, Master's Degree in Clinical Criminology.

The glossary is a compendium of specialist terms covering cybercrimes and abuse and at risk digital activities.

Each term defined within "iGloss@" provides a brief explanation of the main features of the behaviour and a brief note concerning the socio-legal elements.

One of the main aims of the project is child protection, because they can as easily become bad actors as well as victims. Because of this, some entries of the glossary concerning abusive behaviour and victimization risk provide a more comprehensive description.

This product, edited by Luca Pisano, Isabella Mastropasqua and Valeria Cadau was produced with the collaboration of several national\international experts, is endorsed by WiredSafety Inc., the American organisation founded by Dr. Parry Aftab, the worldwide-known expert of digital security.

Sponsored by Google Italy and by the Italian Association of Judges dedicated to Children and Family (www.iglossa.org/en).

Start/duration:
The project started in September 2014 and is still running.

Background research:
First the existing Hungarian prevention programmes were examined and HIA found that the available crime prevention programs focus on victimization in point of violent crimes and crimes against property (e.g. implemented by the Police) but do not handle child- prostitution and human trafficking in its depths.

Budget:
The program was realized by HIA from 12.813,12 EUR (4.000.000 HUF). Professional project management's costs were 3203,28 EUR, commission fees paid for experts amounted to 3843,93 EUR. In addition to these, training of experts required 640,65 EUR. 1921,97 EUR was spent on information flyers needed for sessions. A submenu is created on HIA's webpage which costs 2242,29 EUR and another 960,98 EUR was allocated for other administration costs.

Type of evaluation:
Project activities, implementation and impact evaluation.

Actor conducting evaluation/timing:
The evaluation process was two-fold:
PROCESS 1
1) the **internal evaluation *(ex ante)***, conducted by the team of international experts who also worked on the technical-legal aspects of the Lexicon (see Scientific Committee: http://www.iglossa.org/en/il-comitatoscientifico/)
2) the second **external evaluation** (ex ante), conducted by Google Italy and by the Italian Association of Judges dedicated to Children and Family (http://www.minoriefamiglia.it/categoria-www/id_51/), centred on the lexicon's various entries and legal aspects;
3) the **internal evaluation *(in itinere)*** constantly operated by the international supervisors (see: http://www.iglossa.org/en/i-supervisori/) with the purpose of:
   a) check and evaluate the updates the lexicon might require for the legal and psycho-social aspects;
   b) monitor the answers provided by the scientific committee to citizens who ask for information and support the National Observatory on Cybercrime;
   c) examine and evaluate the work of juvenile justice operators (psychologists, social assistants and educators from the Ministry of Justice) responsible for the wellbeing of children (and their parents) who have perpetrated online crimes;

PROCESS 2 *(in itinere internal evaluation)*
4) Juvenile Justice operators who currently help young people who have perpetrated online crime and their parents, are periodically interviewed by supervisors (through questionnaires and focus groups) in order to provide data on the effects that iGloss@ has produced for subjects in social care (results will be published during January 2016 in italian and english).

It is necessary to specify that, in order to reduce the project's economic impact, the ex-ante and the in itinere evaluations have been performed by the Scientific Committee team and the Supervisors who cooperated with the authors (Luca Pisano, Isabella Mastropasqua e Valeria Cadau) during the lexicon's writing phase (internal evaluation). Google Italy and the Italian Association of Judges dedicated to Children and Family have proofread the project in its final stage, highlighting the few necessary amendments (external evaluation).

Type of data collection method:
Questionnaires and focus groups with Juvenile Justice operators.

Further information
General information on the project:
http://eucpn.org/document/igloss10-online-deviant-behaviour-lexicon

For more information:
http://www.iglossa.org/en/
www.giustizia.it/giustizia/en/mg_2_5_12.wp

Child Line Campaign "Without Bullying" (LT)

Short description:

Campaign „WITHOUT BULLYING“

The fundamental goal of this campaign initiated by “Child Line” in 2004 is prevention of bullying and violence, main focus is paid to cyberbullying. The campaign is targeted at creating safer environment in schools and kindergartens, but not that only; it aims to secure safer life for adults by focusing on the significance of this problem and the need to raise public awareness.

One week in March “Child Line” initiates “Action Week WITHOUT BULLYING” aimed at changing the attitude of society towards bullying from favorable into unfavorable. More than 1137 educational institutions (schools, kindergartens, NGOs) took part in the anti-bullying week in 2015. These educational institutions from all of 60 municipalities participated in this week by organizing various activities. The website of the campaign is www.bepatyciu.lt.

Child Line has organized various trainings about effective bullying prevention for children, teachers, parents during all campaign‘s „WITHOUT BULLYING“ period. In these training seminars people were taught how to recognize bullying phenomenon, how to distinguish it from another deviant aggressive behaviour and how to react correctly in „here and now“ situations. In trainings for school‘s workers teachers and school staff were taught essential principles how the bullying prevention should be conducted in school, what the school‘s administration should do, how each one of the classes educator should work with his class and what should do each school worker if he notices or suspects bullying situation going on.

Also Child Line has published various methodological material for children, 10 parents, school workers about bullying and prevention - leaflets, flyers, methodological publications, visual methodological material.

Start/duration:

The Campaign “Without Bullying” (earlier called “Stop bullying”) was started in 2004, and is still going.

Background research:

According to the data of the International Study of Health Behaviour in School-aged Children (HBSC Study), the rates of experiencing bullying and bullying others among school children

in Lithuania where one of the highest among all the results of the Study conducted every four years starting from 1994. HBSC Study conducted in 2009-2010 showed that the rate of experience of bullying for girls in Lithuania was the highest (26 perc.) and for boys one of the highest (30 perc.) among all participated countries. The percentage of boys bullying others (32 perc.) and and girls bullying others (18 perc.) in Lithuania was among the highest prevalences in the study.

Budget:
The total budget of the project was 140 300 Eur including organising conferences, trainings, production and broadcasting of social advertisement.

Type of evaluation:
/

Actor conducting evaluation/timing:
/

Type of data collection method:
Research.

Further information
General information on the project:
http://eucpn.org/document/child-line-campaign-without-bullying

Project website:
http://www.bepatyciu.lt/;
http://www.vaikulinija.lt/en/campaign-without-bullying/?preview=1#sidebar

Bibi and friends ("De Bibi a seng Frënn") (LU)

Short description:

With "Bibi", the little bee, and his friends, children from the age range from 3 to 6 years learn how to safely take their first steps on the internet. They can listen to the stories online or have them read by their parents offline. Easily accessible for both parebts and kids, these stories are full of hints and ideas on how to successfully protect yourself or your children from potential online threats. Out of the first three stories, two deal with online crime prevention: false identity and online fraud. The website is complemented by printed booklets, and also by complementary handcraft activities.

Start/duration:

The project started on 01 October 2013 an is still running.

Background research:

The "Service National de la Jeunesse" has close contact to children, youth and parents, who share their thoughts and concerns about internet use with them during fairs, in schools and in workshops. Published once a year, the report "lessons learned" collects the feedback gained annually during over 700 school trainings.

This insight was backed up by data from EU surveys held in 2013. While the "Bibi and friends" project was evolving, specific data gathered in Luxembourg confirmed the following main trends: kids start using the internet at an increasingly younger age and mobile internet access is replacing the classical "fixed line" access (survey done by University of Luxembourg in 2014).

Finally, the yearly statistics from the law enforcement agency showed an increasing trend in cybercrime, by now also separately listed as a form of crime.

Budget:

For the first three editions of the "Bibi and friends" stories, the following costs occurred:

- 54000.- EUR, wherefrom:
  - I. 21600.- project concept and character design
  - II. 2700.- Story development
  - III. 10700.- Illustration
  - IV. 11500.- programming and sound
  - V. 7500.- layout and printing cost

In terms of material, about 4600 EUR have been spent on printing material (booklets, drawing games). These figures are already included in the above mentioned budget totals.

On the coordination level, a total of 0.10 FTE had been necessary (184h of work).

Type of evaluation:
The project is still on-going. As such, no structured impact evaluation has been conducted yet.

Actor conducting evaluation/timing:
Process evaluation was conducted internally.

Type of data collection method:
feedback tool and egular field tests.

Further information
General information on the project:
http://eucpn.org/document/de-bibi-seng-frenn-bibi-and-friends

Project website: http://www.bee.lu/; https://www.bee-secure.lu/

SME Cybersecure, Cybersecurity Business edition (NL)

Short description:

Subsidised by the Dutch Ministry of Security and Justice, MKB-Nederland (together with other partners) developed a project to make entrepreneurs more aware of the impact of cybercrime on their businesses. A lot of Small Medium Sized companies (SME's) do not realise that their websites and databases are potential targets. To make SME's more aware of their own cybersecurity, the project organises an awareness campaign based on a roadshow through the country. During this roadshow SME's are given the possibility to improve their cybersecurity by offering 300 free 'social' hacks, giving them a clear insight into their vulnerabilities and measurements they can take to improve their cybersecurity. The partnership with KPN (Telco) offers SME's a professional service with a discount, which means SME's can immediately take action to improve their cybersecurity. Moreover, the partnership with the Association of Insurers offers SME's a clear insight into insurances for cybercrime.

Start/duration:

The start date of the project was 18 August 2015 and it ran till 9 December 2015.

Background research:

Cyber-attacks, online fraud and digital theft accounts for 8,8 billion euros of economic loss in the Netherlands (Source: report 'Net Losses: Estimating the Global Cost of Cybercrime - Economic impact of cybercrime II', Center for Strategic and International Studies / McAfee, June 2014). Approximately 75% of this comes at the expense of entrepreneurs.

SME's are companies with up to 250 employees. 99% of all companies in the Netherlands belong to this group. Together they represent 58% of the gross revenue in the Netherland and offer employment to 60% of all employees (Source: 'MKB in beeld', 13 March 2015 by the Dutch Network Group). The vast majority of SME's have up to 10 employees, which means they lack the capacity to form a strategy and take effective measures against cybercrime. This is why the National Network for Safe Entrepreneurship has identified 'cyber' as one of its main themes.

Budget:
The costs of the project in term of finances, material and human resources are the following:
▷ € 491.900,00 (including project management, communications, roadshows and free hacks);
- €72.400 project preparation – Infrastructure, Communication, Service & Support;
- € 83.900,00 by region (5x): Roadshow, Recruitment, Organisation, Hack (€14.000), Support, Data collection, IT.

Type of evaluation:
Monitoring.

Actor conducting evaluation/timing:
Evaluation will take place between MKB-Nederland and the ministry of Security and Justice in December 2016.

Type of data collection method:
The project continuously monitors the amount of applications for the hacks, visitors of the roadshows, media attention and digital hits.

Further information
General information on the project:
http://eucpn.org/document/sme-cybersecure-cybersecurity-business-edition

Project information:
Campaign: www.veiligzakelijkinternetten.nl

Online Report Amsterdam - http://magazine.veiligzakelijkinternetten.nl/aa

Cyberbullying at schools" (PL)

Short description:
Cyberbullying is a new problem. Virtual violence of teenagers towards their peers or teachers was developed alongside the rapid growth of the ICT. The problem especially affects adolescent people. Most of the teachers is helpless in the face of the problem. They do not have the skills and qualifications that would allow counteracting. Moreover - they can become the victims as well.

Through a series of training sessions for a teachers our project equips people working with teenagers with necessary skills in order to be able to identify, prevent, and respond to cyberbullying. The training program focuses on the psycho-pedagogical, technological, and legal aspects of the phenomenon. During the implementation of the project we have extended its scope by other actions: activities carried out directly with students and parents, awareness publications and actions on Facebook and other media, as well as research aimed at assessing the incidence of the problem.

Start/duration:
The project started on 01 August 2014 and is still running.

Background research:
After developing the scope of the project we have conducted a series of interviews to help us better understand the scale and nature of the problem and to learn the expectations of our main partners. We have interview representatives from the following institutions: The Education Complex no 21 in Gdansk, Primary and Secondary Schools in Bolszewo, Secondary School no 9 in Gdansk, Catholic School Complex in Gdansk, Salesian High School in Rumia, and High School no 3 in Gdansk. It allowed us to get a representative group of respondents with various backgrounds, either in terms of the level of education, social realities (schools are located in big urban areas, smaller towns and urban/rural and municipalities), or nature of their administration (state and private). From the chosen institutions we have received reviews of our project. The conclusions from the interviews were homogeneous, similar to the initial analysis of the problem.

Budget:
Total expenditure of the 2014 edition amounted to 80,000 PLN, including approx. 10,000 PLN from the Association's budget. The budget of the ongoing 2015 edition equals to about 140,000 PLN, with 10,000 PLN from the financial resources of the Association, and the rest being public funds.

The biggest part of the project's budget (85%) are substantive expenses, especially coaches' salaries (approx. 45% of the budget). The rest of the substantive expenses are the costs of the preparations of our publications, materials for the training sessions and its organization.

The relatively low administrative costs (15%) are connected with the fact that a number of administrative tasks have been done voluntarily, e.g. all tasks connected to project management have been voluntary work from one of the members of our Association. Part of the substantive tasks of the projects (managing the Facebook page, conducting studies on cyberbullying among teachers) is implemented free of charge by our members.

Type of evaluation:
Effectiveness and results evaluation.

Actor conducting evaluation/timing:
In the 2014 edition the evaluation of the process was an element of the comprehensive project evaluation conducted by an external specialized consulting firm. There were three independent evaluation reports created during the 2014 edition.

Type of data collection method:
Survey combining quantitative (Yes/No questions, rating scale, etc.) and qualitative analysis (open questions).

Further information
General information on the project: http://eucpn.org/document/cyberbullying-schools

For more information:
Our main website: http://drogowskazy.com.pl/
Section dedicated to the project: http://drogowskazy.com.pl/docs/207
Our Facebook profile dedicated to the project:
https://www.facebook.com/cyberprzemocwszkolach

Internet Segura (Safer Internet) (PT)

Short description:
This project consists in several web 2.0 initiatives that promote sensitization and awareness on Cyberprevention directed to citizens, especially to youngsters, promoting Cybercrime prevention, strengthening the moral and ethical values from which cyberspace must be built.

Start/duration:
The project started in January 2014 and is still running.

Background research:
Through the databases that our Force uses to register crime incidents, the existing data was processed and compiled, in particular those crimes pertaining to internet use.

It was considered in the plan of the program principles and directives reflected in the European Digital Agenda, the recent European Security Agenda of 2015, the European Cyber Security Strategy and the new National Strategy Cyberspace Security of Portugal.

Budget:
The costs result from the salaries of the police officers that work in the “special community programs” department and the logistic resources used to conduct the various program actions (fuel, paper, printing, etc.).

Type of evaluation:
/

Actor conducting evaluation/timing:
The project will be evaluated at a national level by the Portuguese Board of Assessment and Accountability that assesses the performance in Public Administration and internally within the GNR Strategy 2020.

Type of data collection method:
Awareness-raising actions are subject to evaluation by filling out a specific document by youngsters and teachers.

Further information
General information on the project: http://eucpn.org/document/safer-internet

For more information:
https://sway.com/WI7_Ij0e-D7-ycIt

http://www.gnr.pt/default.asp?do=tnov0r6r_vz24r05n/016vpvn5/016vpvn5_qr5p4vpn1&fonte=noticias&id=2136

http://www.gnr.pt/default.asp?do=tnov0r6r_vz24r05n/016vpvn5/016vpvn5_qr5p4vpn1&fonte=noticias&id=1911

http://www.gnr.pt/default.asp?do=tnov0r6r_vz24r05n/016vpvn5/016vpvn5_qr5p4vpn1&fonte=noticias&id=1333

http://www.gnr.pt/default.asp?do=tnov0r6r_vz24r05n/016vpvn5/016vpvn5_qr5p4vpn1&fonte=noticias&id=1494

http://www.gnr.pt/default.asp?do=tnov0r6r_vz24r05n/016vpvn5/016vpvn5_qr5p4vpn1&fonte=noticias&id=2349

http://www.gnr.pt/default.asp?do=tnov0r6r_vz24r05n/016vpvn5/016vpvn5_qr5p4vpn1&fonte=noticias&id=2343

https://www.fct.pt/media/notas_imprensa/docs/NI_08052014.pdf

https://news.microsoft.com/pt-pt/2015/02/10/microsoft-e-gnr-sensibilizamalunos-e-encarregados-de-educacao-para-os-perigos-da-internet-e-desafiamescolas-a-criar-carta-magna-do-ciberespaco/

http://news.microsoft.com/pt-pt/2014/02/11/02-11microsoftegnrinternetsegurapr/

http://www.noticiasaominuto.com/pais/458685/gnr-pede-reforcos-a-disney-paraalertar-criancas-sobre-a-internet

http://www.publico.pt/sociedade/noticia/gnr-e-personagens-da-disney-lutampela-ciberseguranca-em-mais-de-cinco-mil-escolas-1708560

Theatre FestivalArsPraeventiva– The faces of technology (RO)

Short description:

The Crime Research and Prevention Institute within the Romanian General Inspectorate of Police (IGPR), with the support of BSA | The Software Alliance, organized, in the school year 2013-2014, a theatre festival for Bucharest high-schools students, called ArsPraeventiva, dedicated to addressing the threats that the use of new technologies raise for a vulnerable segment of the population – young people, namely preventing youth from becoming victims as well as perpetrators in cybercrime.

Participants (high-school students) creatively engaged in writing theatrical plays with preventive messages and stories inspired from the use of technology and, then, in a second phase, such plays were put on stage by the writers' peers, Bucharest high-school students activating in high-school amateur theatrical companies.

The organizers invited a large range of partners for this first edition – educational authorities, a Bucharest theatre, technology companies and association, the media, thus ensuring a successful project with minimum resources, as the efforts were mainly in-kind contribution and voluntary work from organizers and partners.

Start/duration:

ArsPraeventiva started in September 2013, once the school year started, and the first edition, focused on „safe use of computer and electronic communications by the young people" ended on May 30th, 2014, when the school year ended. It may run every school year, on different themes.

Background research:

The context was analysed before the project was initiated and the private co-organizer BSA and other partners from the public and private sectors were invited to participate.

The analysis was conducted by the Crime Research and Prevention Institute, by specific means, using both publicly available data and data from internal police sources, especially from cybercrime police department.

Budget:

There was no funding for the project, all the institutions, bodies and companies involved had in-kind contributions – working for creating the brief and talking to the target group, participating in events and rehearsals, judging and evaluating scripts, supervising the creative and

interpretative work, awarding the participants with their own means and products (hardware, theatrical books, free tickets for theatrical shows), making the venues available free of charge for the events, covering the events by media channels.

Type of evaluation:
Impact evaluation.

Actor conducting evaluation/timing:
Internal: The Crime Research and Prevention Institute within the Romanian General Inspectorate of Police (I.C.P.C.).

Type of data collection method:
/

Further information
General information on the project:
http://eucpn.org/document/theatre-festivalarspraeventiva-faces-technology

For more information:
While the edition on safe use of computer and electronic communications by the young people was running, all the campaign materials and info were posted on the then available website www.softwareculicenta.ro, a site built and run in partnership by the Romanian Police and BSA | The Software Alliance.

After the first edition was completed, the new updated version of the aforementioned website only includes the three press-releases published in the course of the contest:
http://download.softwareculicenta.ro/comunicat-de-presa-2013-10-01-ars-praeventiva.pdf

http://download.softwareculicenta.ro/comunicat-de-presa-2014-02-25-ars-praeventiva.pdf

http://download.softwareculicenta.ro/comunicat-de-presa-2014-05-30-ars-praeventiva.pdf

Please find below three online articles published by Hotnews, one of the media partners of the festival, on their online news platform, covering the three events of the festival in the school year 2013-2014:
http://www.hotnews.ro/stiri-prin_oras-15701726-liceeni-din-bucuresti-vor-scenaristi-actori-cadrul-festivalului-ars-praeventiva.htm

http://www.hotnews.ro/stiri-esential-16682962-inspectoratul-general-politiei-romane-bsa-the-software-alliance-anunta-castigatorii-primei-etape-festivalului-ars-praeventiva.htm

http://economie.hotnews.ro/stiri-companii-17386641-the-software-alliance-premiaza-trupa-teatru-colegiului-national-grigore-moisil-cadrul-festivalului-ars-praeventiva.htm

CORPORATE COMPASS – ETHICAL GUIDELINES AGAINST SEXUAL Financial Coalition against Commercial Sexual Exploitation of Children (SE)

Short description:

The Swedish Financial Coalition Against Child Pornography was started in 2008.
The child sex trade, or commercial sexual exploitation of children, means child sexual abuse material (called "child pornography" in the law), sexual exploitation of children sold in Sweden or in connection with travel, and trafficking in children for sexual purposes. New ways to sexually exploit children are generated at the same pace as the development of technology and access to the Internet. A great number of cases go unreported and individual seizures conducted by the police can contain millions of pictures and films documenting abuse. Buyers and sellers use different payment methods over the Internet to transfer money between them.

The Financial Coalition Against Child Pornography was started in order to prevent this trade through the financial system. It is a unique and successful collaboration between public authorities, the private sector, and the non-profit sector.

The activities are based, among other things, on active cooperation between payment services providers, technology providers and the police, for the purpose of tracking and stopping payments before a transfer is made. Among other things, the members use a method which focuses on finding points of sale in order to shut down the seller's ability to receive payments. One advantage of this method is that it is crime prevention work which does not invade the individual's privacy.

The work is carried out in close cooperation with ECPAT Sverige and relevant public authorities and has the stated goals of detecting new routes of payment and linking up with relevant parties who can contribute to impeding payments for illegal material. The police are ultimately responsible for combating criminality. However, the financial services industry is a key player in the work of detecting new behaviours and finding solutions to stop these transactions.

The Financial Coalition's work has been very successful. At present, we believe that the cooperation between the Financial Coalition and the police, together with other global parties, has had a significant effect. For example, it is now extremely difficult to use a payment card in these contexts and the number of websites expressly for the purpose of selling child sexual abuse material has decreased radically.

Start/duration:
The initiative for the Financial Coalition was taken in 2008, when ECPAT Sverige and Skandiabanken invited all Swedish banks to participate in a Swedish financial coalition to combat child pornography. Its activities are ongoing.

Background research:
The problems and the legal prerequisites for taking action were analysed in a report drafted by the law firm of Allen & Overy on instruction from the European Financial Coalition (which does not, however, conduct the same type of hands-on activities as the Swedish Financial Coalition). In addition, Setterwalls, a Swedish law firm, conducted a corresponding analysis based on Swedish circumstances.

Budget:
Initially, each member of the Coalition contributed only with its own working time. During the years in which the Coalition has been active, financing has been obtained in the form of voluntary financial contributions by allowing the members to pay to display their logos on marketing material in connection with different types of events. This has created a fund for different types of activities.

The Coalition has, in cooperation with universities, produced reports related to the Financial Coalition's work. The Financial Coalition has made a minor financial contribution to the students who wrote the reports.

Type of evaluation:
/

Actor conducting evaluation/timing:
/

Type of data collection method:
/

Further information
General information on the project:
http://eucpn.org/document/financial-coalition-against-commercial-sexual-exploitation-children

Project website: www.finanskoalitionen.se

Adam and Eve of the 21st century (SK)

Short description:
The project is designed for children 12-15 years of age, focuses on topics most interesting to adolescents. Discussions on topics such as adolescence, relationships, friends, internet, social networks, sex, pornography and others will be held with children openly. These topics are part of young Europeans everyday life. Children think that they already know everything and nothing can surprise them. They live online, “post” and “share” their thoughts, opinions, photographs, “like” contributions of their online friends, send friend requests to people they do not know, but they have a “mutual friend”. They visit adult websites without any problems with one click. They bet on who’s seen more forbidden things, who has tried them and who will try them. The project aims to ensure they can cope with these events and “problems”, enable them to learn the right information distortion-free, to be able to enjoy the benefits of today’s modern world.

Start/duration:
The project started on 10 September 2013 and is still running.

Background research:
The project was analyzed by the Chief of the Metropolitan Police, a child psychologist, teachers and educational counsellors and school directors. The project was launched on 10 September 2014 at schools in city Nove Zamky, Slovakia, in form of group and personal meetings, lectures, discussions, experimental learning and active cooperation with the pupils. Lectures led Klaudia Homolova, coordinator of youth crime prevention.

Budget:
/

Type of evaluation:
Content and information processing.

Actor conducting evaluation/timing:
Internal: municipality Dvory nad Zitavou.

Type of data collection method:
/

Further information

General information on the project:
http://eucpn.org/document/adam-and-eve-21st-century

For more information:
http://www.rtvs.sk/televizia/archiv/7600/57727

http://nasenovinky.sk/article/12579/tabor-pre-priatelov-policie

http://novezamky.sme.sk/c/7295008/maly-princ-vyrastol-na-adama-21-storocia.html

References and recommended further reading

CLOUGH, J., *Principles of cybercrime*, Cambridge, Cambride University Press, 2010.

CHAWKI, M., DARWISH, A., KHAN, M.A., TYAGA, S., '*Cybercrime, digital forensics and jurisdiction*', Springer, 2015.

DEBAETS, A., DEENE, J. and SENEL, N. '*Cybercriminaliteit*', in VERMEULEN, G., Aspecten van Europees materieel strafrecht, Antwerpen, Maklu-Apeldoorn, 2002, (381) 393.

EUCPN, '*Cybercrime - A theoretical overview of the growing digital threat*', Brussels, 2016.

European Union (2014), Cyber Security Strategy and Programs Handbook, Volume 1 Strategic Information and Regulations, p. 113

European Commission (1996). Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions. *Illegal and harmful content on the Internet, Brussels*: COM (1996)487, 16 October 1996. [http://publications.europa.eu/en/publication-detail/-/publication/1061a860-7528-4258-a132-cf468e5c22ac/language-en]

European Commission (2007). Communication from the Commission to the European Parliament, the Council and the Committee of the Regions. *Towards a general policy on the fight against cybercrime, Brussels*: Com(2007) 267 final, 22 May 2007. [http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52007DC0267]

European Commission (2013). Joint Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels: COM (2013) 01 final, 07 February 2013 [http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52013JC0001]

European Commission (2012), Communication from the Commission to the Council and the European Parliament. *Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre, Brussels*: COM (2012) 140 final, 28.3.2012. [http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/communication_european_cybercrime_centre_en.pdf]

European Union (2014), Cyber Security Strategy and Programs Handbook, Volume 1 Strategic Information and Regulations, p. 113.

Europol (2011), '*Internet Facilitated Organised Crime, iOcta 2011*', The Hague, 2011. [https:/www.europol.europa.eu/sites/default/files/publications/iocta_0.pdf]

Europol (2011), '*EU Organised Crime Threat Assessment, OCTA 2011*', The Hague, 2011. [https://www.europol.europa.eu/sites/default/files/publications/octa_2011_1.pdf]

Europol (2014), '*The Internet Organised Threat Assessment, iOCTA 2014*', The Hague, 2014.

GORDON, S., RICHARD, F. (2006), '*On the definition and classification of Cybercrime*,' Journal in Computer Virology 2006, Volume 2, Issue 1, pp. 13-20.

JEWKES, Y., YAR, M., '*Handbook of internet crime'*, Devon, Willan Publishing, 2010, 401.

LUNA, R. and FINKELHOR, D., (1998). '*School based prevention programs: Lessons for child victimization prevention*'. Retrieved October 21, 2014 [http://www.unh.edu/ccrc/pdf/CV30.pdf]

MASTERS, G., '*Global cybercrime treaty rejected at U.N.'*, SC Magazine 23 April 2010. [www.scmagazine.com]

OECD, '*Computer viruses and Other Malicious Software: A Threat to the Internet Economy*', 2009, 244p.

Robinson, N., Disley, E, Dimitris, P., Reding, A., Culley, D., Penny, M., Botterman, M., Carpenter, G., Blackman, C. and Millard, J., '*Feasibility study for a European Cybercrime Centre*', Final Report, UK, February 2012. [http://ec.europa.eu/dgs/home-affairs/e-library/docs/pdf/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre_en.pdf]

SCHILDER, J.D, BRUSSELAERS, M.B. and BOGAERTS, S. (2015), '*The Effectiveness of an Intervention to Promote Awareness and Reduce Online Risk Behavior in Early Adolescence*'. Journal of Youth and Adolescence, 1-15.

United Nations Office on Drugs and Crime, '*United Nations convention against transnational organized crime and the protocols thereto*', New York, 2004.

United Nations, '*Working paper of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice*', Salvador, Brasil, 22 January 2010: UN Doc. A/CONF.213/9 (2009) [https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf]

United Nations Office on Drugs and Crime (2013), Comprehensive Study on Cybercrime, Vienna, February 2013. [https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf]

Yar, M., (2006) '*Cybercrime and society*'. Sage Publications Inc., London, p. 9

Contact details:

EUCPN Secretariat
Phone: +32 2 557 33 30
Fax: +32 2 557 35 23
Email: eucpn@ibz.eu
Website: www.eucpn.org

D.P. Jean-Marie Wagner - Route de Trèves Complexe A - L-2632 Findel - Luxembourg

D.P : Philip Willekens – Boulevard de Waterloo 76 – 1000 Brussels