



**EU2017.EE**



**EUROPEAN CRIME PREVENTION NETWORK**

# **EUCPN Toolbox Series**

No. 12

## ***Cybersecurity and Safety Policy and best practices***

In the framework of the project 'The implementation of the Multiannual strategy plan of the EUCPN and the Informal Network on the Administrative Approach' - EUCPN Secretariat, March 2018, Brussels



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



# Cybersecurity and Safety: policy and best practices

## Preface

The 12th toolbox in the series published by the EUCPN Secretariat focuses on the main theme of the Estonian Presidency and the 2017 Best Practice Conference (BPC), which was 'Cyber Safety'. This practical toolbox is to be read in tandem with the theoretical paper on this topic.

First, the cybersecurity policy is situated between two driving forces: the economic and security forces. Creating trust in the digital market and protecting citizens from online harm are the main goals. Recently, the renewed EU policy on cyber-related issues is taking form. This first part presents an overview for policymakers and tries to guide the reader through the myriad of legislative proposals and policy documents.

The second and third part focus on the good and promising practices which were submitted to compete in the 2017 European Crime Prevention Award (ECPA) and some additional projects that were sent to the Secretariat by the Member States. Being safe online is not a reflex for everyone and the projects that were gathered aim to achieve just that. We have a look at the orientation of the projects, which partners are present and some of the methods that were applied. These lessons learned provide practical information for the practitioners in their effort to prevent cybercrime and promote cyber safe behaviour.

## Citation

EUCPN (2018). *EUCPN Toolbox Series No. 12 Cybersecurity and Safety. Policies and practices.* Brussels

## Legal notice

The contents of this publication do not necessarily reflect the official opinion of any EU Member State or any agency or institution of the European Union or European Communities.

## Authors/editors

Jorne Vanhee, Research Officer, EUCPN Secretariat, Brussels, Belgium

Cindy Verleysen, Senior Research Officer, EUCPN Secretariat, Brussels, Belgium

---

**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](mailto:eucpn@ibz.eu) – [www.eucpn.org](http://www.eucpn.org)

## Acknowledgement

This toolbox has been developed in close collaboration between the EUCPN Secretariat and the Estonian Presidency, who organized the 2017 Best Practice Conference (BPC) and the European Crime Prevention Award (ECPA). The award celebrated its 20th birthday in 2017 and has evolved into a quality mark for crime prevention in Europe.

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 particularly would like to thank the three experts who were willing to follow the various sessions during the BPC and to contribute to the content and conclusions of this toolbox: Manuela Mus (EC3, Europol), Raoul Notté (The Hague University of Applied Sciences) and Michael McGuire (University of Surrey).

Also, we are very grateful towards all the participants of the workshop we organized in relation to this toolbox: Manuela Mus (European Cybercrime Centre (EC3), Europol), María Sanchez (EC3, Europol), Nathalie Van Raemdonck (Cybersecurity Centre Belgium), Raoul Notté (The Hague University of Applied Sciences), Paul Caruana (University of Malta), Georgi Apostolov (Bulgarian Safer Internet Center) and Michael Levi (University of Cardiff).

Finally, we would like to thank all the participants of the ECPA 2017. Like in the previous editions of the BPC and ECPA competition, we were inspired 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.

Thank you all!

The EUCPN Secretariat

# Table of contents

Introduction .....	7
--------------------	---

## **PART 1:**

### **Recent developments in European cyber policy .....**

1. Introduction .....	9
2. The Budapest Convention and the Council of Europe .....	10
3. The EU's cyber policy .....	13
3.1. Cybersecurity Strategy of the European Union (2013) and the NIS directive .....	13
3.2. Digital Single Market .....	16
3.3. The European Agenda on Security .....	19
3.4. Cybersecurity Package .....	19
3.5. The EU Policy Cycle and EC3 .....	22
4. Member States Policies .....	24
5. Conclusion .....	26

## **PART 2:**

### **Good and promising practices on cyber safety .....**

1. Introduction .....	28
2. The three winning projects .....	29
3. Lessons learned .....	35
3.1. Introduction .....	35
3.2. Orientation and target group .....	36
3.3. Partners .....	40
3.4. Methods .....	42
4. Conclusion and recommendations .....	44

## **PART 3:**

### **Overview ECPA 2017 projects and additional projects .....**

Austria: The Watchlist Internet .....	48
Belgium: Cybersimple .....	49
Bulgaria: Cyberscout program .....	50
Croatia: Who's Joking with my Data .....	51
Czech Republic: Regions for Safe Internet .....	52
Denmark: The Danes' digital self-defense .....	53
Estonia: The cyber defence field of study at Põltsamaa Coeducational Gymnasium .....	54
Finland: Finnish Hotline Nettivihje .....	55
Germany: Don't Offend .....	56
Greece: Raise Awareness for Cyber Crime through Innovative Processes and Applications .....	57
Hungary: Fables of Crime Prevention – Tales of Forest-town .....	58
Ireland: Cyber-UP – CyberYouth Diversion Project .....	59
Lithuania: Safe Behaviour on the Internet .....	60

The Netherlands: Boefproof .....	61
Poland: Cyber Jungle .....	62
Portugal: Project PROTEUS: supporting victims of identity theft and identity fraud .....	63
Romania: The Internet Class .....	64
Sweden: Safe Surfing .....	65
Additional projects .....	66
Germany: Cybercrime: The criminal investigation department explains .....	67
Hungary: Save Gordon! .....	68
Poland: Cyberprzemocowy Falochron .....	69
Poland: Served on the Tray .....	70
Portugal: Safer Internet - CyberGNRation .....	71
<b>References</b> .....	<b>72</b>

## Introduction

*You just received an email from your boss asking for your banking credentials. Apparently it is your lucky day because you are getting a bonus! He thanks you for the hard work you have been doing lately. The only thing you have to do is to fill in your account number followed by your pin on a website. As a trustful employee, you of course follow the orders and thankfully accept the bonus. When you check your account the morning after, instead of having got a bonus, you seem to have bought something nice in the Bahamas...*

The Internet offers a wide range of benefits. Online payments give us the possibility of paying everywhere and whenever we want. Location services can give you up to date information on traffic jams or delays in public transport. Instead of typing a text, you could send a picture instead. The only problem is that you leave behind breadcrumbs in the form of data. This data can easily be turned into an object of interest for the cybercriminal. Your banking credentials can be extracted if the link in the email for example contains a key logger. And if you think that the picture you sent to your friend is completely safe, think again. Being safe online is not a reflex for everyone. Moving through cyberspace is typically perceived as safe. The vastness of cyberspace creates a kind of 'safety by numbers' feeling combined with a sense of anonymity. After all, who knows "the Dread Pirate Roberts"?

In fact, "the Dread Pirate Roberts" figure is the founder of Silk Road, an online market where illicit goods were sold in a way based on eBay and Amazon features. Completely anonymous people can also buy cybercrime-enabling tools such as key loggers on these Dark Net marketplaces. No skills are needed to commit the crime later on, except accessing the market and buying the service.

This Crime-as-a-Service model drives law enforcement to engage in a cat-and-mouse game with cybercriminals to keep up with the newest and latest types of ransomware, phishing campaigns, card fraud,... These efforts are however very costly. Preventing victimization could be more cost-effective. Having as little breadcrumbs as possible could avoid victimization. Being aware of social engineering tactics could leave criminals with empty hands.

In this toolbox, we combine efforts in regard to the prevention of cybercrime in order to disseminate best practices and guiding frameworks. The **first part** will concentrate on the **policy level**, including legislative measures in the European Union and Member States. The **second part** will focus on the lessons learned from the 2017 **Best Practice Conference (BPC) and European Crime Prevention Award (ECPA)** on the theme Cyber Safety. This event was held in Tallinn at the end of 2017 as the conclusion of the Estonian Presidency of the EUCPN. The **third part** shows all **ECPA entries and additional projects** in order to stimulate the exchange of good practices between Member States and practitioners.

# Part 1

## Recent developments in European cyber policy

---

### Recent developments in European cyber policy

## 1. Introduction

In this first part of the toolbox we provide an overview of the policy on cyber-related issues. The focus is put on the policy within the European Union. We will discuss the agenda setting within this context and the most relevant instruments and organisations. Next, we also look into the different policies on the national level<sup>1 2</sup>.

Together with this toolbox, a theoretical paper on the topic is available. The interested reader is advised to go over this paper as it explains important aspects of ‘cyber safety’.

Following the presidency of Luxembourg from 2015 the EUCPN Secretariat published a toolbox and theoretical paper on cybercrime in general, encompassing all subtopics. A very thorough overview was given on the history of legislation in Europe. It is not necessary to repeat this here. Instead we will focus on the newest developments in European policy. These developments are to be situated within the presidency of the Council of the European Union by Estonia and their drive to renew the cyber policy of the EU.

Estonia has its historical reasons for prioritizing cyber policy. In 2007 the country experienced a nation-wide Distributed Denial of Service (DDoS) attack on its public and private infrastructure. These events drove the European Union to up their game within this policy area and elevated cyber security up the political agenda<sup>3</sup>. During their presidency of the Council in the second part of 2017, one of their priorities was to renew the EU Cyber Security Strategy (2013)<sup>4</sup> in order for the EU to be able to better respond to the constantly evolving challenges<sup>5</sup>. On the 13th of September the European Commission proposed the Cyber Security Act together with a range of proposals<sup>6</sup>, known as the ‘Cybersecurity Package’.

In order to fully comprehend current developments, we will briefly go through the recent history in regard to cyber security policy and the main policy documents. Within the European context, there is however a predefined starting point: the Budapest Convention established within the Council of Europe (2001)<sup>7</sup>.

<sup>1</sup> ENISA (2016). *NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies*. Heraklion

<sup>2</sup> ENISA (2017). *National Cyber Security Strategies*.

Retrieved from <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map>

<sup>3</sup> Christou, G.(2017). The EU's Approach to Cybersecurity. *EU-Japan Security Cooperation: Challenges and Opportunities, 2017* (Spring/Summer), 1-13

<sup>4</sup> 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

<sup>5</sup> Council of the European Union. (2017). *Discussion paper on the EU's fight against cybercrime. (10829/17)*. Brussels

<sup>6</sup> European Commission. (2017). *Factsheet Resilience, Deterrence and Defence: Building strong cybersecurity in Europe*. Brussels

<sup>7</sup> 23/11/2001 - Council of Europe Convention on Cybercrime (CETS No 185)

## 2. The Budapest Convention and the Council of Europe

‘Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks’, the Council of Europe accepted the Budapest Convention in 2001 in order to ‘deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct [...] and the adaption of powers sufficient for effectively combating such criminal offences’<sup>8</sup>. The Convention entered into force on the first of June 2004 and was the first international treaty seeking to harmonize national laws, improve investigative techniques and increase international cooperation within this subject<sup>9</sup>. As of January 2018, 56 states have ratified the Convention<sup>10</sup>. Ireland and Sweden are the only EU Member States who have not ratified the Convention yet.

One of the main goals of the Convention was to harmonize domestic criminal law and to categorize offences that need to be criminalized:

- offences against the confidentiality, integrity and availability of computer data and systems, encompassing illegal access, illegal interception, data interference, system interference and misuse of devices;
- computer-related offences such as forgery and fraud;
- content-related offences related to child pornography;
- offences related to infringements of copyright and related rights.

In 2003, the Additional Protocol (AP)<sup>11</sup> to the Convention was signed and came into force in 2006. This protocol broadens the scope of the original Convention and adds the criminalisation of acts of a racist and xenophobic nature committed through computer systems. As of January 2018, 29 countries ratified the AP<sup>12</sup>.

<sup>8</sup> Preamble Convention on Cybercrime

<sup>9</sup> EUCPN. (2016). EUCPN Toolbox Series No.8: Preventing cybercrime. Policies and practices. Brussels

<sup>10</sup> Council of Europe (11/01/2018). Chart of signatures and ratifications of treaty 185.

Retrieved from [https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p\\_auth=g7X0pLMm](https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=g7X0pLMm)

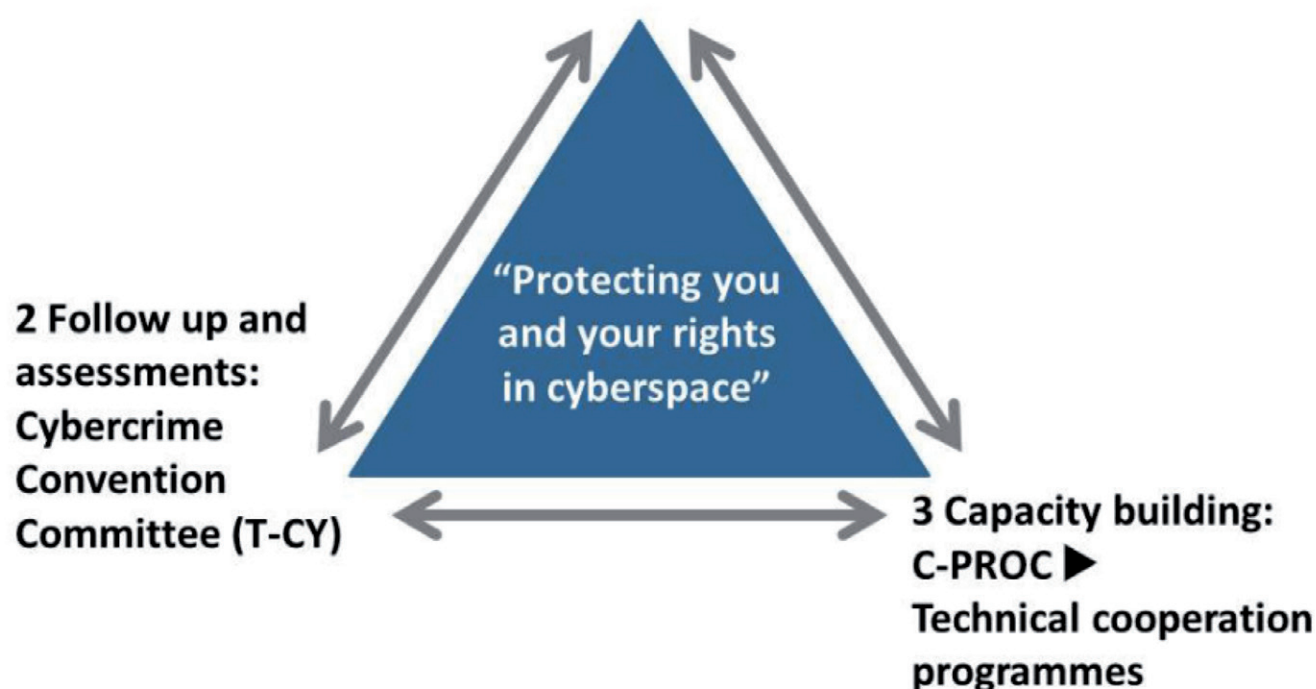
<sup>11</sup> 28/01/2003 - Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS No 189)

<sup>12</sup> Council of Europe (11/01/2018). Chart of signatures and ratifications of treaty 189.

Retrieved from [https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p\\_auth=g7X0pLMm](https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=g7X0pLMm)

In June 2017, the Council of Europe decided to launch the preparation of a second protocol to help law enforcement secure evidence on servers in foreign, multiple or unknown jurisdictions<sup>13</sup>. This followed as a recommendation from a report from the Cybercrime Convention Committee (T-CY) stemming from the recognition that additional solutions are required to permit criminal justice authorities to obtain specified electronic evidence<sup>14</sup>. The rationale behind all of this is that if there is no evidence, there will be no justice. According to the Terms of Reference for the preparation of a draft Second AP the following aspects will have to be considered: provisions for more effective mutual legal assistance, provisions allowing for direct cooperation with service providers in other jurisdictions, a clearer framework and stronger safeguards for existing practices of trans border access to data and safeguards including data protection requirements. It is expected to have a draft version by December 2019<sup>15</sup>.

## 1 Common standards: Budapest Convention on Cybercrime and relates standards



**Source:** Council of Europe. (2017). *Action against Cybercrime*. Retrieved from <https://www.coe.int/en/web/cybercrime/home>

<sup>13</sup> Council of Europe (08/06/2017). *Cybercrime: Towards a Protocol on evidence in the Cloud*.

Retrieved from <https://www.coe.int/en/web/human-rights-rule-of-law/-/cybercrime-towards-a-protocol-on-evidence-in-the-clo-1>

<sup>14</sup> T-CY Cloud Evidence Group. (2016). *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY*. Strasbourg

<sup>15</sup> T-CY. (2017). *(DRAFT) Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime*. Strasbourg

Originating from the Convention (art.46), the T-CY assesses the implementation by the Parties of the Convention and facilitates the sharing of good practices and experience and helps addressing problems encountered with implementation. Another task is to consider possible supplementation to the Convention, such as the currently under discussion AP<sup>16</sup>. C-PROC or the **Cybercrime Programme Office** is located in Bucharest, Romania and is responsible for assisting countries in strengthening their legal systems capacity to respond to the challenges posed by cybercrime and electronic evidence. This includes training, promoting public-private cooperation, enhancing the effectiveness of international cooperation,... through the work of projects<sup>17</sup>.

## Council of Europe:

- *Legislation*
  - *Budapest Convention (2001)*
  - *Additional Protocol on the criminalization of acts of a racist and xenophobic nature committed through computer systems (2003)*
  - *Additional Protocol on e-evidence (under discussion)*
- *Organizations*
  - *C-PROC: capacity building body*
  - *T-CY: monitoring body*

<sup>16</sup> T-CY. (2014). T-CY Rules of Procedure. Strasbourg

<sup>17</sup> Council of Europe (30/10/2017). About C-PROC. Retrieved from <https://rm.coe.int/cproc-about/1680762b41>

### 3. The EU's cyber policy

Following the aforementioned cyber-attacks in Estonia in 2007 and the rapid increase in cybercrime, the European Commission prepared the grounds for a policy framework to tackle the problem. As we can see in the previous toolbox, before this turning point, there were some initiatives but they were not specifically coordinated in a broader policy perspective<sup>18</sup>.

In the Commission's communication 'Towards a general strategy on the fight against cybercrime'<sup>19</sup>, it was sought to achieve just this in order to better coordinate the fight against cybercrime. The main achievements were a Directive on combating the sexual exploitation of children online and child pornography<sup>20</sup>, a Directive on attacks against Information Systems<sup>21</sup>, the establishment of the **European Cybercrime Centre (EC3)** within Europol (cf. infra) and the EU's Cybersecurity Strategy (2013).

#### 3.1. Cybersecurity Strategy of the European Union (2013) and the NIS directive

This strategy was the first attempt ever by the EU to set out clear priorities for the protection of cyberspace<sup>22</sup>. The 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace' aimed at an overall harmonisation and coordination and had five objectives<sup>23</sup>.

1. Achieving cyber resilience;
2. Drastically reducing cybercrime;
3. Developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP);
4. Develop the industrial and technological resources for cybersecurity;
5. Establish a coherent international cyberspace policy for the European Union and promote core EU values.

One of the harmonisation aspects was defining cybersecurity in this Strategy. It states: "Cybersecurity commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein"<sup>24</sup>.

<sup>18</sup> EUCPN. (2016). *EUCPN Toolbox Series No.8: Preventing cybercrime. Policies and practices*. Brussels

<sup>19</sup> 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

<sup>20</sup> 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, and replacing Council Framework Decision 2004/68/JHA

<sup>21</sup> 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

<sup>22</sup> Christou, G.(2017). The EU's Approach to Cybersecurity. *EU-Japan Security Cooperation: Challenges and Opportunities, 2017* (Spring/Summer), 1-13

<sup>23</sup> van der Meulen, Nicole, Eun Jo and Stefan Soesanto (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. European Parliament [https://www.rand.org/pubs/research\\_reports/RR1354.html](https://www.rand.org/pubs/research_reports/RR1354.html)

<sup>24</sup> 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

Another aspect had a more formal nature. In order to achieve both cyber resilience and reduce cybercrime, the Commission proposed legislation on Network and Information Security (NIS)<sup>25</sup>. In 2016 the NIS Directive came into effect and concerned measures for a high common level of security of network and information systems across the Union by putting minimum standards in place covering at least the following sectors: energy, transport, banking, financial market infrastructures, health sector, drinking water supply and distribution, digital infrastructure and also digital services such as online marketplaces, online search engines and cloud computing services. The Commission does however stress that other sectors should be considered but are not obliged under this directive.

As such, Member States are obliged to adopt a national strategy on NIS, to have one or more competent authorities that monitor the Directive and to have a Computer Security Incident Response Team (**CSIRT**). In regard to cooperation, **Cooperation Group** was established to support and facilitate strategic cooperation and information sharing. Additionally, the **CSIRTs Network** contributes to the development of confidence and trust between Member States and promotes swift and effective operational cooperation between national CSIRTs.

Key actor in the implementation of the NIS directive is the **European Agency for Network and Information Security (ENISA)**. This agency was established in 2004 for the purpose of contributing to a high level of NIS within the Union. It does so by raising awareness of NIS and promoting a culture of network and information security for the benefit of citizens, consumers, enterprises and public sector organizations in the Union<sup>26</sup>. It supports the development of Union policy and law, capability building, voluntary cooperation among public bodies and stakeholders and research and development. It also cooperates with other Union bodies dealing with the subject and contributes to the EU's external cooperation efforts<sup>27</sup>.

ENISA for example helps Member States in developing national strategies on NIS or national CSIRTs and provides the secretariat for the CSIRTs Network. The agency is also a crucial actor in the European Cyber Security Month, an EU advocacy campaign set up every year in October<sup>28</sup>. Since 2013, ENISA, together with different partners in the Member States, the Commission and EC3, coordinates this pan-European campaign promoting cybersecurity awareness and a sense of shared responsibility for citizens to behave safely and informed on the Internet.

<sup>25</sup> Directive (EU) 2016/1148 of the European parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

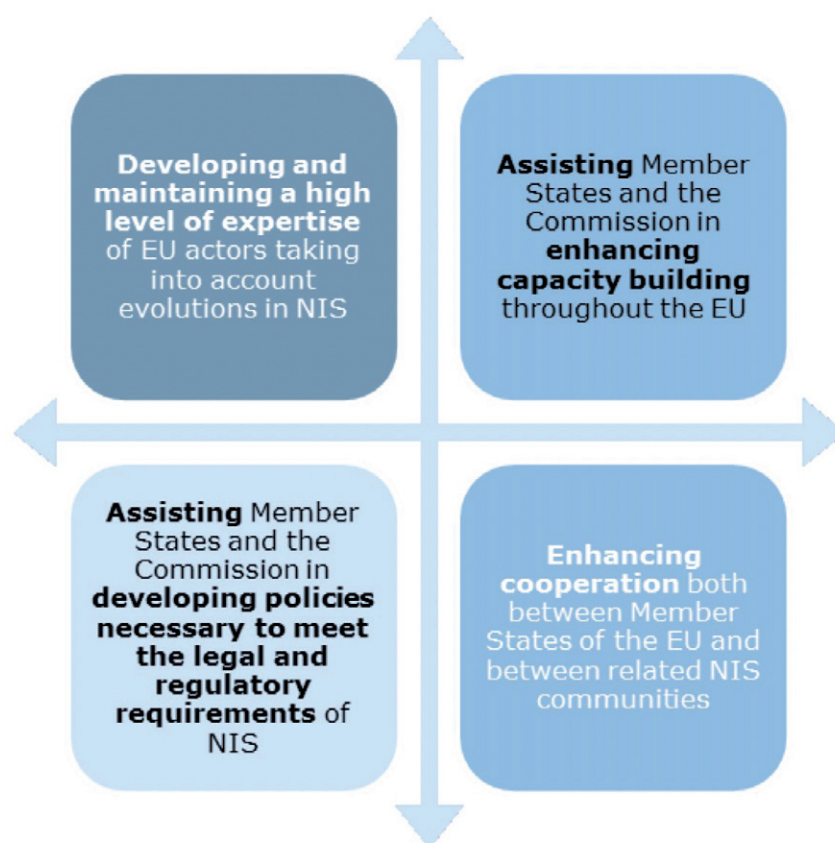
<sup>26</sup> ENISA. (2016). ENISA Strategy 2016-2020. Heraklion

<sup>27</sup> Regulation (EU) no 526/2013 of the European parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004

<sup>28</sup> EUCPN. (2016). EUCPN Toolbox Series No.8: Preventing cybercrime. Policies and practices. Brussels

In its assessment<sup>29</sup> of the 2013 Cybersecurity Strategy, the Commission is quite critical on the campaign and on raising awareness in general. The progress of the campaign is noteworthy: an increase of almost 300% in campaign activities since 2013. Member States confirmed the added-value of this campaign in a survey that was done by the Council and even felt that more has to be done on a pan-European level, and that the coordination role of ENISA and also EC3 should be strengthened.

Nevertheless European citizens and companies still seem to have limited awareness and knowledge of cybersecurity issues. The 2017 Special Eurobarometer on Cybersecurity<sup>30</sup> illustrates these findings as it does not show an increase in cybersecurity awareness since the last three years. In fact, 51% of the respondents do not feel well informed about cybercrime. The Barometer concludes by mentioning that the overall findings highlight the importance of greater public education on different types of cybercrime, their consequences and ways in which their impact can be avoided or mitigated. Another interesting number here is that 87% of the respondents perceive cybercrime as a major challenge to the security of the European Union.



**Source:** European Commission (2017). Evaluation of ENISA. Luxembourg. Publications Office of the European Union. (p.9)

<sup>29</sup> European Commission (2017). *Commission staff working document Assessment of the EU 2013 Cybersecurity strategy*. Brussels

<sup>30</sup> Special Eurobarometer 464, 2017

Aside from achieving cyber resilience and reducing cybercrime, there also is the objective of developing the industrial and technological resources for cybersecurity. The other two objectives, focusing on defence and international policy, would take us too far out of the scope of this toolbox. The industrial and technological resources are however at the centre in cybersecurity policy. In 2016 the Commission signed an agreement with the cybersecurity industry to establish a **Cyber Public-Private Partnership (cPPP)** with the **European Cyber Security Organisation (ECSO)**<sup>31</sup>. ECSO is a fully self-financed non-profit organisation which represents the industry with stakeholders as large companies, SMEs, research centres, universities, end users,... The cPPP is expected to trigger 1.8 billion euros of investment by 2020 in order to better equip Europe against cyber-attacks and strengthen the competitiveness of its cybersecurity sector. €450 million will come from the EU and its Horizon 2020 program, the market players are expected to invest three times more<sup>32</sup>.

### 3.2. Digital Single Market

This economic rationale is a very active input to the European cybersecurity policy. The reason is quite simple and put forward in the *Digital Agenda for Europe* (2010)<sup>33</sup>: users will not embrace technology they do not trust. One of the main outcomes of this document is the creation of a **Computer Emergency Response Team for the EU institutions (CERT-EU)** which supports European institutions to protect themselves. However, in order to maximise the potential of the digital economy, other obstacles need to be removed. One of the main obstacles is the national fragmentation of the European economy<sup>34</sup>.

The goal of a Digital Single Market (DSM) aims to break down these barriers. In 2015 the Commission put forth a new *Digital Single Market Strategy*<sup>35</sup> restating its objective to create a single market 'in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection'. This should ensure that the EU will maintain its position as a world leader in the digital economy.

The Strategy recognises that the growing number of cybercrime offences is leading to significant economic losses. The adoption of the NIS directive is important in combatting this. The development of the industrial and technological resources for cybersecurity as a priority in the Cybersecurity Strategy and the birth of the cPPP are noteworthy here. But more had to be done. The DSM Strategy links itself to the European Agenda for Security (cf. infra) and proposes the General Data Protection Regulation (GDPR). This regulation was voted in 2016 and will be in force as of May 2018 and replaces the previous one from 1995<sup>36</sup>.

<sup>31</sup> European Commission. (2016). *Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats*. Brussels

<sup>32</sup> ECSO. (2017). About ECSO. Retrieved from <http://ecs-org.eu/about>

<sup>33</sup> European Commission. (2010). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe*. Brussels

<sup>34</sup> European Commission. (2014). *The EU explained: Digital Agenda for Europe*. Brussels

<sup>35</sup> European Commission. (2015). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A digital Single Market Strategy for Europe*. Brussels

<sup>36</sup> Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

The previous legislation did not live up to its expectations due to differences in implementation in the Member States.<sup>37</sup> The GDPR will increase trust in digital services, as it should protect individuals with respect to the processing of personal data by all companies that are active in the European market<sup>38</sup>. The new legislation is praised for its intentions and for creating a new mindset on privacy and personal data. Questions can however be raised on the legally capable age of consent, which is set on 16 years old. There is the discretionary possibility for Member States to lower this to 13. Current reality however does not reflect this as children go online from a very young age. As the Bulgarian example shows, the average age of the first use is 8. 90% of the children in Bulgaria became Internet users before the age of 11<sup>39</sup>. Enforcement will be a second major issue. After all, who will stop a parent from posting a picture from their child on their Facebook wall?

Together with GDPR, the **ePrivacy Directive**<sup>40</sup> is currently under debate as a newly proposed directive is put on the table<sup>41</sup>. This will further increase legal certainty and protection of users' privacy online<sup>42</sup>.

<sup>37</sup> Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer.

<sup>38</sup> European Commission. (2015). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A digital Single Market Strategy for Europe*. Brussels

<sup>39</sup> Hajdinak, M., Kanchev, P., Georgiev, E., Apostolov, G. (2016) *Children in Bulgaria: risks and safety*.

<sup>40</sup> 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 (Directive on privacy and electronic communications)

<sup>41</sup> Proposal for a Regulation of the European parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

<sup>42</sup> European Commission. (2017). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy A Connected Digital Single Market for All*. Brussels

## General Data Protection Regulation (GDPR)

Application date: 25<sup>th</sup> of May 2018

Rationale: contribute to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons

Scope: any processing of personal data, except in the areas of security policy, criminal prosecution, in the course of purely personal or household activity and activities that are outside of Union law

Important in regards to prevention:

- Processor and controller of the personal data have to keep records of their processing activities in order to be able to prove compliance;
- Data protection officer: obliged if the core activities consist of regular and systematic monitoring of data subjects or of processing special categories of personal data on a large scale or if the processing is carried out by a public authority or body. This officer has to monitor compliance;
- Data protection impact assessment: if an intended processing activity, can result in a high risk to the rights and freedoms of the data subject, there has to be a preventive data protection impact assessment in order to be able to identify appropriate protective measures;
- Data protection by design: the conditions for processing are fundamentally set by the soft- and hardware used for the task. These have to be minimally invasive;
- Data protection by default: only personal data that are necessary for the specific purpose of the data processing can be obtained. This restricts the amount of data that is allowed to be collected;
- Data subject rights: data processing entities have to proactively fulfil numerous obligations towards the data subject, such as granting information on processing, 'the right to be forgotten', ...;
- Data breach notification: in case of a breach, the controller has to report within 72 hours of being aware of the breach.
- Consent: in order for data processing to be lawful, the data subject has to give its consent. Children can give this consent starting from 16 year. If younger, parents have to give or authorize the consent. Member States can lower this, but not lower than 13 years is allowed.

### 3.3. The European Agenda on Security

The DSM Strategy directly links itself with its ‘security counterpart’: the European Agenda on Security (2015)<sup>43</sup>. This five-year plan sets the priorities in regard to crime phenomena within the EU policy. The three priorities in the Agenda are terrorism, organised crime and cybercrime. Cybercrime is seen as an ever-growing threat to the fundamental rights of the European citizens and to the economy and the Digital Single Market, completing the two-fold policy nexus.

The Agenda puts further emphasis on the Cybersecurity Strategy (2013) as a key policy document. It reiterates the most important aspects of the Strategy. Additionally, the Agenda stresses the need to fully implement all existent EU legislation, such as the Directive on attacks against Information Systems (2013)<sup>44</sup> and the Directive on combating the sexual exploitation of children online and child pornography (2011)<sup>45</sup>. Building on the legislation, the Agenda proposed to update the Framework Decision combatting fraud and counterfeiting of non-cash means of payments (2001)<sup>46</sup>, as this was no longer up to date in light of current realities (e.g. virtual currencies).

Acknowledging the need for renewal, the Commission stated in its Mid-Term Review of the Implementation of the Digital Single Market Strategy in May 2017 to review the Cybersecurity Strategy. By September, it promised to do so and added to this the review of the mandate for ENISA and to develop measures on cyber security standards, certification and labelling<sup>47</sup>.

### 3.4. Cybersecurity Package

The Commission delivered on its promise and together with the State of the Union of Jean-Claude Juncker<sup>48</sup>, it published what is called the ‘Cybersecurity Package’. Explaining the two-fold security/economy logic within the cybersecurity policy, Juncker stated:

*“Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. [...] Cyber-attacks know no borders and no one is immune. This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks”*

<sup>43</sup> European Commission. (2015). *Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security*. Brussels

<sup>44</sup> 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

<sup>45</sup> 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, and replacing Council Framework Decision 2004/68/JHA

<sup>46</sup> Council framework decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment (2001/413/JHA)

<sup>47</sup> European Commission. (2017). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy A Connected Digital Single Market for All*. Brussels

<sup>48</sup> European Commission President Jean-Claude Juncker, State of the Union Address, 13 September 2017

*“We need to better protect Europeans in the digital age. In the past three years, we have made progress in keeping Europeans safe online.*

*New rules, put forward by the Commission will protect our intellectual property, our cultural diversity and our personal data. Today, the Commission is proposing new tools”*

The overall guiding framework was given in a joint communication called ‘*Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*<sup>49</sup>. The focus is shifted from a more reactive to a proactive approach in order to protect European prosperity, society and values through responding to both existing and future threats. As the title of the document says, the renewed policy builds on three pillars:

- Resilience: building EU resilience to cyber-attacks and stepping up the EU’s cybersecurity capacity;
- Deterrence: creating an effective criminal law response;
- Defence: strengthening global stability through international cooperation.

The policy document has several proposals in order to achieve this strong cybersecurity for Europe. As Juncker stated in his State of the Union, a new European Cybersecurity Agency will be proposed. This new agency will be built on the existing framework of **ENISA**. The proposed *Cybersecurity Act*<sup>50</sup> will be the main basis for this. ENISA would be given a strong and permanent mandate as well as the adequate resources it needs to fulfil the proposed tasks:

- Policy development and implementation: to strengthen support to the Commission and Member States in the development, implementation and review of general cybersecurity policy and in key strategic sectors identified by the NIS directive, such as energy, transport and finance;
- Operational cooperation: to contribute to cooperation in the CSIRTs Network at EU level and provide assistance on request to Member States to handle incidents;
- Knowledge and information: to provide analyses and advice and to raise awareness, to become the one-stop shop for cybersecurity information from the EU institutions and bodies;
- Capacity building: to reinforce support to Member States in order to improve capabilities and expertise, for instance on the prevention of and response to incidents;
- Market-related tasks: within the Cybersecurity Certification Framework prepare candidate European cybersecurity certification schemes, with the expert assistance and close cooperation of national certification authorities. Schemes would be adopted by the Commission. ENISA will also support policy development in ICT standardization.

This last task has an important preventive aspect. This voluntary framework is aimed at ensuring trust from consumers in new technology in a way that the CE label does as this indicates

<sup>49</sup> European Commission. (2017). *Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*. Brussels

<sup>50</sup> Proposal for a Regulation of the European Parliament and of the Council on ENISA, the “EU Cybersecurity Agency”, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (“Cybersecurity Act”)

conformity with health, safety and environmental standards for products that are sold in the EU. The Certification framework would indicate safety and security standards. The security-by-design approach that follows protects the user better as this will provide a competitive arena within the industry, forcing the industry to produce safe and secure products in order to remain competitive. The security logic serves the economic logic and vice versa.

Other proposals are the Blueprint<sup>51 52</sup> which maps how to respond quickly, operationally and in unison when a large scale cyber-attack hits the EU; the *Cyber Diplomacy Toolbox*<sup>53</sup> which sets out the framework for a joint EU diplomatic response to malicious cyber activities; the establishment of a **European Cybersecurity Research and Competence Centre** that will help to develop and roll out the tools and technology needed to keep up with the constantly evolving threat landscape. Another important proposal is a new *directive on non-cash payment fraud*<sup>54</sup>. The EU Agenda on Security already acknowledged this need to renew the directive from 2001 as it no longer reflects current realities. Moreover, this embodies the security-economic logic as it poses a threat to both. The goal of the new directive will be to boost deterrence by ensuring a technology neutral framework, enhancing prevention, and eliminate operational obstacles that hamper investigation and prosecution. Building on this last objective, the Commission promises to put forward proposals to facilitate cross-border access to electronic evidence or e-evidence<sup>55</sup>.

In the *Joint Communication* there are three important advises directed to the Member States in regard to cyber hygiene and awareness which are of specific interest to the topic of this toolbox.

*“With some 95% of incidents said to be enabled by ‘some type of human error – intentional or not’, there is a strong human factor at play. So cybersecurity is everyone’s responsibility. This means personal, corporate and public administration behaviour must change to ensure everybody understands the threat, and is equipped with the tools and skills necessary to quickly detect and actively protect themselves against attacks. People need to develop cyber hygiene habits and businesses and organizations must adopt appropriate risk-based cybersecurity programmes and update them regularly to reflect the evolving risk landscape”<sup>56</sup>*

The three advises start off by stating that Member States should maximize the availability of cybersecurity tools for businesses and individuals. In this regard, more should be done to prevent and mitigate the impact of cybercrime on end-users. As an example they use the ‘NoMoreRansom!’ campaign<sup>57</sup> where close cooperation between law enforcement – EC3 (cf. infra) in specific – and cybersecurity companies helps to prevent ransomware infections and decrypt data when users are victim of an attack. Schemes like the ‘NoMoreRansom’ campaign should act as a start to develop a single portal to bring together all advice to users on prevention and detection on malware and links to reporting mechanisms.

<sup>51</sup> Commission recommendation of 13.9.2017 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises

<sup>52</sup> Annex to the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises

<sup>53</sup> Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities («Cyber Diplomacy Toolbox»), 19 June 2017. The Toolbox was presented earlier but is stated to be part of the package.

<sup>54</sup> Proposal for a Directive of the European Parliament and Of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA

<sup>55</sup> European Commission. (2017). *Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*. Brussels

<sup>56</sup> Ibid., p.11

<sup>57</sup> No more Ransom! (2017). *About the project*. Retrieved from <https://www.nomoreransom.org/en/about-the-project.html>

Next, Member States should accelerate the use of more cyber-secure tools in the development of e-government. Lastly, Member States should make cyber-awareness a priority in awareness campaigns, including those targeting schools, universities, the business community and research bodies. We hope the best practices that are gathered in this toolbox are a step in this direction.

### 3.5. The EU Policy Cycle and EC3

Parallel with these developments, the EU has a four-year policy cycle for the fight against serious international and organized crime<sup>58</sup>. As it is not within the objective of this toolbox to go too much into detail, we refer to the paper from the EUCPN Secretariat on how the Policy Cycle works<sup>59</sup>.

An important input to the prioritization in this cycle, is the Serious and organized crime threat assessment (SOCTA) drawn by Europol on the basis of input from the Member States. In this report, Europol identifies several criminal phenomena in which serious and organized criminal groups are the key actors. Prevention is a horizontal goal in the Policy Cycle, meaning that preventive measures and actions should be done for all priorities. Cybercrime is one of them and will as such be a priority in the four-year cycle of 2018-2021<sup>61</sup>. The phenomenon is further divided into three subcategories: Cyber-dependent crimes, online child sexual exploitation and payment card fraud. The EUCPN has an active involvement in the prevention of cybercrime in this context and more specifically in the subtopic of online child sexual exploitation.

Within Europol, the **European Cybercrime Centre (EC3)** was established in 2013 within the European Cybersecurity Strategy<sup>62</sup>. The strategy called for support to EC3 as a focal point in the fight against cybercrime and targets three cybercriminal priorities:

- cybercrimes committed by organized crime groups, especially those generating large profits (e.g. online fraud);
- cybercrimes causing serious harm to its victims (e.g. online sexual exploitation);
- cybercrimes affecting critical infrastructure and information systems in the EU (including cyber-attacks).

EC3 has the following functions:

- European cybercrime information focal point;
- Pooling expertise to support EU countries in capacity building;
- Operational support to member countries;
- The collective voice of European cybercrime investigators across law enforcement and the judiciary.

<sup>58</sup> Europol. (2017). *EU Policy Cycle- EMPACT*. Retrieved from <https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact>

<sup>59</sup> EUCPN Secretariat. (2017). *EU Policy Cycle: what is it, how does it work and what is the role of prevention?!*. Brussels

<sup>60</sup> Europol. (2017). *Serious and Organised Crime threat Assessment*. The Hague

<sup>61</sup> Council conclusions on setting the EU's priorities for the fight against organised and serious international crime between 2018 and 2021

<sup>62</sup> Communication from the Commission to the Council and the European Parliament: Tackling crime in our digital age: establishing a European Cybercrime Centre (COM(2012) 140 final of 28 March 2012).

The EC3 presents its own Internet Organized Crime Threat Assessment (IOCTA) to further elaborate on the picture of the cyber threat landscape. Here it gives recommendations to address the phenomenon and goes deeper into the cybercrime-related SOCTA priorities<sup>63</sup>.

Located within the EC3, the **Joint Cybercrime Action Taskforce (J-CAT)** is the operational facility. The taskforce's objective is to drive intelligence-led, coordinated action in the cybercrime priorities in the European Union.

## European Union:

- *Policy documents*
  - o *Towards a general strategy on the fight against cybercrime (2007)*
  - o *EU Cybersecurity Strategy (2013)*
  - o *Digital Single Market Strategy (2015)*
  - o *European Agenda on Security (2015)*
  - o *Resilience, Deterrence & Defence: Building strong cybersecurity for the EU (2017)*
  - o *EU Policy Cycle (2018-2021)*
- *Legislation*
  - o *Directive on combatting the sexual exploitation of children online and child pornography (2011)*
  - o *Directive on attacks against Information Systems (2013)*
  - o *Directive on Security and Information Systems (NIS) (2016)*
  - o *General Data Protection Regulation (2018)*
  - o *ePrivacy Directive*
  - o *Cybersecurity Package (2017)*
- *Organizations*
  - o *CSIRT/CERT: National NIS monitoring bodies*
  - o *Cooperation Group: Strategic cooperation NIS*
  - o *CSIRTs Network: operational cooperation NIS*
  - o *ENISA: NIS implementation and overall NIS expertise centre, new mandate under proposal*
  - o *ECISO: Private cybersecurity industry association*
  - o *CERT-EU: Computer Emergency Response Team for the EU institutions*
  - o *EC3: Europol's cybercrime centre*
  - o *J-CAT: operational taskforce within EC3*

<sup>63</sup> Europol. (2017). *Internet Organised Crime Threat Assessment (IOCTA) 2017*. The Hague

## 4. Member States Policies

The NIS directive requires Member States to develop and adopt national cyber security strategies in at least the sectors that were mentioned earlier. In this regard, Member States can ask ENISA to assist them. This had led ENISA to come up with a good practice guide in order to support MS in their efforts<sup>64</sup>. This guide from 2016 presents an overview of the objectives of national cyber security strategies of 16 MS. All other countries are currently under study by ENISA and the assessments are not public yet. Many Member States are also working on the next version of their strategy so ENISA waits on publishing for these specific countries. All countries in the European Union do however have a national cyber security strategy.

In addition to the valuable work from ENISA, the Working Party on General Matters including Evaluations (GENVAL) situated within the Council of the European Union, decided in 2013 to evaluate the cybercrime policies of the Member States and in October 2014 the first evaluation mission started. Two years later, the Working Party ended the visitation round in September 2016. For each country, specific reports were written and adopted by GENVAL. It has to be noted however that due to the long-lasting character of the evaluation, the country reports do not always reflect the current state of play<sup>65</sup>. It is for this reason that we will not go into the details of these reports.

We can however make a general comment on this ‘Seventh round of mutual evaluations on “The practical implementation and operation of the European policies on prevention and combating cybercrime”’. In contrast to what the title suggests and even to the country specific reports, the final report has only a slightly marginal focus on the prevention of cybercrime. This only further supports the need for a toolbox on the prevention of cybercrime and on cyber safety.

<sup>64</sup> ENISA (2016). NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies. Heraklion

Objectives	A T	B E	B G	H R	D K	E E	F I	F R	G R	H U	I E	L U	M T	S I	E S	S E
1. Develop national cyber contingency plans	x				x	x	x	x		x	x	x			x	x
2. Protect critical information infrastructure	x	x	x		x	x	x	x		x		x		x	x	x
3. Organise cyber security exercises	x	x			x	x	x	x	x	x	x	x		x	x	x
4. Establish baseline security measures	x			x	x	x	x	x		x		x			x	
5. Establish incident reporting mechanisms	x	x		x	x	x	x	x	x	x	x	x	x	x	x	
6. Raise user awareness		x	x		x	x	x	x	x			x	x	x	x	
7. Strengthen training and educational programmes	x	x			x	x	x	x		x		x	x	x	x	
8. Establish an incident response capability	x	x		x	x	x	x	x	x	x	x		x	x	x	
9. Address cyber crime	x	x		x	x	x	x	x	x			x	x	x	x	x
10. Engage in international cooperation	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x
11. Establish a public-private partnership	x	x	x				x					x			x	x
12. Balance security with privacy				x		x	x	x						x	x	x
13. Institutionalise cooperation between public agencies	x	x				x		x		x		x		x	x	x
14. Foster R&D	x	x		x	x	x	x	x							x	x
15. Provide incentives for the private sector to invest in security measures							x									

<sup>65</sup> Working Party on General Matters including Evaluations (GENVAL). (2017). *Final Report on the seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime"*. Brussels

## 5. Conclusion

As with cyberspace itself, policy is constantly evolving. The last three decades show an unseen evolution in technology. In this first part of the toolbox, we have tried to give a brief overview of the current state of the European policy. Very recently, the European Commission proposed a 'cybersecurity package' which sets the agenda for the upcoming years. Our toolbox comes at a crucial period in time and we can only hope that prevention will be one of the key issues for the future.

In the next part of the toolbox, we will present the best practices that exist within the European Crime Prevention Network regarding the topic of cyber safety. First of all, we present the winners of the 2017 European Crime Prevention Award. Second, together with information we gathered from experts, we will provide an analysis of these best practices that were gathered by the Secretariat.

## Part 2 Good and promising practices on cyber safety

---

### Good and promising practices on cyber safety

## 1. Introduction

The highlight of the year for the EUCPN is the Best Practice Conference (BPC) which brings together practitioners and policy makers from all over the European Union to share their experiences. Here they present their country's best project regarding the topic that is chosen by the presidency. Since 2004, the BPC is linked to the competition of the European Crime Prevention Award (ECPA). This competition, which celebrated its 20th anniversary in 2017, aims to publicly award good or promising practices in the field of crime prevention through an assessment by a jury made up by the National Representatives or their substitutes of the current presidency, the former presidency and the two incoming. In 2017 this was respectively Estonia, Malta, Bulgaria and Austria.

As already mentioned, the topic of Estonia for the 2017 BPC-ECPA was 'cyber safety'. In the call for projects the presidency explained this choice as follows:

*Cybercrime is a real and growing threat that impacts the EU's internal security as digitalising society unavoidably becomes more vulnerable to new cyber threats. The Estonian Presidency is committed to make the fight against cybercrime even more effective as foreseen in the renewed Internal Security Strategy and in the EU Policy Cycle for both the 2014-2017 period and the 2018-2021 period. The Estonian Presidency will continue these discussions on strengthening the EU's response to cyber threats in Council preparatory bodies. Related to this, the literacy of the people and communities of the EU must be better in order to respond to malicious cyber activities. Overall one of the priorities of the Estonian Presidency of the Council of the EU is a digital Europe and the free movement of data.*

*Under the EUCPN, the Presidency will focus on the reduction and prevention of cybercrimes in the communities as a priority. This means, that projects submitted to the ECPA 2017 should be in line with EU Policy Cycle priorities to combat cybercrimes committed by organized crime groups and generating large criminal profits and related to the EU crime priority 'Cybercrime (card fraud)' or EU crime priority 'Cyber Attacks'. For example, the projects could raise issues around cyber hygiene such as combating organised forms of cybercrimes and raising awareness, including threats caused by the use of internet and smart devices.*

Every EU Member States announced the national call for ideas related to this topic. The aim was to find ideas to enhance the cyber safety of the persons, enterprises, state and local authorities and after evaluation of all the ECPA entries to award the three best projects on the EU level. This evaluation of the 18 projects was done according to the rules of procedure on the 15th and 16th of November 2017 by the Jury in Tallinn. In part 3 of this toolbox, fact sheets of all these entries are included. When a project, entered by the MS where a jury member originates from, was discussed he/she withheld him/herself in the discussion. The Jury explained its decision on the winning projects as follows:

*[...] The winner of the ECPA is the project “Cyber Defence field of study at Põltsamaa Coeducational Gymnasium” of Estonia. This project was chosen because of its uniqueness and innovativeness. This school is the first known school in Europe to implement this field of study. With this course the Estonian project tries to fill the knowledge gap and to make its students carriers of cyber defence awareness. The goal of the project is for students to become the next cyber safety experts.*

*The runner-up project ‘The Danes’ digital self-defense’ of Denmark was particularly liked because of the promising method. Through the interactive application, users are given practical tips and information on the cyber threat landscape. The users themselves can also tip the project by offering their experiences, effectively contributing to the overall knowledge.*

*The second runner-up project is the Belgian project ‘Cybersimple’. Having Google as a partner was seen as a major asset and the high replication possibility, due to it already being developed in three languages, was much appreciated by the jury. Additionally, the project encompasses a wide range of topics within cyber safety.*

## 2. The three winning projects

### **First prize: the Estonian project ‘The cyber defence field of study at Põltsamaa Coeducational Gymnasium’**



Põltsamaa Coeducational Gymnasium has opened a cyber defence field of study (3-year upper secondary school programme). The project, which is ongoing, started with the initiative from Põltsamaa Coeducational Gymnasium and has evolved with the help of several key partners who supported it.

On November 9, 2015, the key partners signed a cooperation agreement at the school. Thus, it became probably the first high school in the world to open this specific field of study at the upper secondary school level.

The cyber defence curriculum of Põltsamaa Coeducational Gymnasium has 4 cyber defence courses (35h each):

1. Information society. Key topics: defence strategy; data and social media; gathering and use of data; the EU digital market; e-Estonia and its components; the culture of a digital society; device security; the legal basis of (cyber)security; contemporary threats (including cyber warfare, hybrid warfare).
2. Information technology: the basics of safe networking. Key topics: the basic principles of physical and IT-related network security; common mistakes in creating safe networks: detection and prevention; overview of critical IT infrastructure (at a service provider in the field in Estonia).
3. Digital security and cryptography. Key topics: the principles of a digital lifestyle in Estonia; the history of cryptography; modern cryptographic solutions; institutions that ensure the operation of a digital lifestyle; e-Estonia: structure and operation; responsible and informed use of social media.
4. Introduction to mechatronics. Key topics: the history, trends and scope of use of mechatronics; the functioning of various sensors, microprocessors, controllers, actuators and software; tools and materials in mechatronics; safety and safety equipment; UAV types; UAVs (DJI F550) – construction and operation/flying (FrSky Taranis X9D); the theoretical methods of deploying UAVs in warfare

The 3-year programme has the following structure:

During the first trimester of Year 1, students learn national defence (3h a week, 35-hour course). In the second and third trimester, the focus is on Information technology (35 h) and mechatronics (35h) (robotics and UAVs). Both theoretical and practical learning is used. A technical drawing course (35h) supports these courses. During Year 1, students usually have training visits at the NATO Cooperative Cyber Defence Centre of Excellence, e-Estonia Showroom and Estonian Information System Authority.

During Year 2, students learn via an integrated syllabus (2h a week, 70 h in total) of safe networking, cyber security, cryptography and mechatronics (UAVs). The additional courses are 3D modelling (35h) and programming (35h). During Year 2, students have training visits at Santa Monica Networks and The Estonian Foreign Ministry.

In Year 3, the course Basics of safe networking continues based on the Mikrotik programme (35h) and students take an exam to obtain an MTCNA certificate.

In total, students pass 10 courses (350h) in the cyber defence field of study, which are complemented by three training visits and practical programming at the University of Tartu Computer Science Institute. All added together, this makes 400h of study.

Various learning methods are used: seminars; Skype-lectures; watching relevant film (for example, CyberWar Threat by PBS NOVA); practical projects; training visits, etc. Lectors include specialists from the Estonian Information System Authority, the National Cyber Defence League, and the Center for Communication and Information Security Research and Development. These are some examples of practical assignments:

- 1) analysing a case study of information manipulation – the sides, root and motivation in the conflict
- 2) virus detection with virustotal.com
- 3) compiling network schematics
- 4) IP address detection and operations
- 5) security audit on a device; scanning a file for threats; setting up firewalls
- 6) analysis of standard contracts
- 7) case study with the emphasis of finding the applicable law.

### ***Second prize: The Danish project ‘the Danes’ digital self-defense’***



According to surveys done in 2014, an estimated 150.000 Danish citizens had been the victim of IT-crime in the form of identity theft, fraud, harassment and/or ransomware within the last 12 months. About half of which was concerned with credit card fraud estimated to a cost of 200 million DKK (approx. 25 million EUR) in 2014.

This proves that the Danish consumers meet many new kinds of crime online, e.g. phishing, smishing, ransomware or fake websites. In 2016 the Danish Consumer Council, and the Danish foundation 'Tryg Fonden', therefore agreed to collaborate with the purpose to investigate 'the consumers' experience of digital safety – and the most significant challenges'. A report was published in December 2016 stating that the majority of the Danes basically feel safe online, but unsafe when confronted with a number of everyday online scenarios:

- 78 % feel unsecure about the risk of having their credit card information abused online.
- 74 % feel unsecure about the risk of their social security number (CPR) being abused online.
- 70 % do not trust the public sector to keep their personal information safe
- 66 % feels unsecure about the fact that private services sell their data to third party services

The report also stated, that the more knowledge the consumer has on Internet-security and possibilities to protect themselves online, the more they do protect themselves. Also the experience of digital safety turned out to rely strongly on the consumer's amount of knowledge. That context fostered the idea of an app with the purpose of alerting and guiding the consumers with the help from private and public organizations whose brands are subjects to misuse online. The Danish Crime Prevention Council (DKR), the foundation 'TrygFonden', and the Danish

Consumer Council took a common interest to collaborate with a twofold objective:

1. To develop and run the app 'My digital self-defense' with the Danish public as target group.
2. To research the field of citizens' self-protection against digital threats in order to describe a long term effort to support the consumers digital education, safety and security.

The project management was placed with the Danish Consumer Council.

The first version of the free app 'My digital self-defense' was launched on April 7th 2017 on the AppStore and GooglePlay and has had more than 50.000 downloads within the first 6 months. The app alerts its app-users of current threats and waves of ongoing cyber-attacks. Messages are pushed by a large group of associated partners, counting both private and public organizations as well as NGO's. More than 80 alerts have been sent out in the first 6 months, more than half by the associated partners.

Through the app the app-users can also tip the project team on the threats and/or scams they experience and thereby contribute to the knowledge sharing. 1700 tips on digital threats have been received from the app-users since April 7th 2017.

The project team researches the incoming tips, spot waves of attacks and trends, and when patterns arise, new alerts are published to the users through the app and the relevant company, whose brand is being misused, is alerted.

The app also holds sections with information on

1. What to do, if the damage is done.  
(Block credit card, reboot system, notify police etc.)
2. General characteristics of how to distinguish fraud from trustworthy messages  
(Analyse links sent by unknown distributors, look for physical addresses of web shops, look for the Danish e-mark on web shops etc.)
3. How to improve your personal, digital protection (Secure use of passwords, backup data, keep security software updated, browser settings, and use of VPN etc.)

### *Third prize: the Belgian project 'Cybersimple'*



The Cybersimple campaign aims to educate and empower consumers in Belgium to protect themselves for a safer online experience. The Internet changes how we live and work and it's changing all the time too. Keeping up is vital to be able to benefit fully from the new opportunities it offers. The campaign wants all Belgians to seize those opportunities while remaining safe and secure. Building on local research, Google and Test Achats (Belgian consumer association) joined forces to develop an online educational platform – cybersimple.be – where consumers can learn from a series of 90 web-safety tips ranging from account and device protection to child safety and online transactions.

The website is available in French, Dutch and English. The website content is split into categories helping consumers to protect their online accounts, devices, online transactions, and more. It also includes tips on how to keep your children safe online. Everything is easy to find, with tips from various categories featured on a tiled wall on the homepage. A tile on the homepage also invites users to participate in online quizzes covering each category of the site and offering citizens a playful way to test their knowledge and fill in the gaps at the same time. The Cybersimple campaign was launched with the announcement of Google's partnership with the Belgian consumer association Test-Achats with a press event in Brussels on March 15th – World Consumer Rights Day. Google and Test-Achats were joined by local partners Digital Belgium, Child Focus, Centre for Cyber Security Belgium, the Belgian Police and European Consumer Centre Belgium. A joint press release was distributed to the national press on that day. "This partnership between Google and Test-Achats is a great initiative giving people the ability to test their knowledge and have a clear overview of the basic protective measures they need to take to ensure their safety online" said Alexander De Croo, Belgian Deputy Prime Minister. The event, attended by over 20 journalists, resulted in 47 pieces of media coverage - including prime time on TV news and front page of some newspapers, helping to spread the message to the population. The development of a simple, engaging online safety quiz that journalists could embed on their own website helped to scale the campaign content across many news sites.

Mid-April a paid media campaign helped to raise the campaign awareness amongst consumers in Belgium. This 8 weeks long campaign included Video pre-rolls on YouTube, Online banners, Out-of-home placements in Brussels, and Social media. Test Achats also promoted the initiative on their website and in an e-mail newsletter to their subscribers. The creative executions of the newsletter featured three easy-to-do web safety tips, mirroring some of the Cybersimple.be website categories: Online transactions, Child safety & Account safety. These executions showed each one web safety tip, so even by only seeing the advertisement a citizen could just follow the tip and be a bit safer online without even visiting the Cybersimple Website. Pragmatic tips included for example: Always check the green padlock in your URL - making consumers aware that they should always ensure they buy on websites that transmit their transaction data securely.

---

xxx

## 3. Lessons learned

### 3.1. Introduction

In total 18 different projects entered the ECPA competition and were presented at the BPC in Tallinn, Estonia, on the 14th and 15th of December 2017. In addition 5 more projects were sent to the Secretariat of the EUCPN and will also be part of the following overview. All of them can be found in part 3 of this toolbox. References will be made to these 23 projects throughout these 'lessons learned'.

Here we will present some lessons learned from these projects and useful recommendations and guidelines regarding cybercrime prevention and the promotion of cyber safe behaviour. As a result, this toolbox is of course not exhaustive and does not cover all possible prevention activities in this field. The lessons learned are based on the gathered projects from the Member States.

In addition, the EUCPN Secretariat invited three rapporteurs to the BPC to further assess the projects. These rapporteurs were asked to write a critical report on the 18 ECPA projects. The reports were used as a valuable input to this toolbox and provided key insights regarding best practices. These experts were:

- Manuela Mus, EC3 Europol
- Raoul Notté, The Hague University of Applied Sciences
- Michael McGuire, University of Surrey

Building on these reports, a workshop was organized in January 2018 by the Secretariat. The first part of this toolbox (policy) was discussed in this workshop, but also crime prevention activities. Not all projects were discussed in depth, the discussion was held on a more general and abstract level. Key elements and issues regarding cybercrime prevention were taken into consideration here. Seven international experts attended this workshop:

- Manuela Mus, EC3 Europol
- María Sanchez, EC3 Europol
- Nathalie Van Raemdonck, Cybersecurity Centre Belgium
- Michael Levi, Cardiff University
- Paul Caruana, University of Malta
- Raoul Notté, The Hague University of Applied Sciences
- Georgi Apostolov, Bulgarian Safer Internet Centre

This section combines the three 'streams' of information: projects, reports and workshop.

### 3.2. Orientation and target group

Of all 23 projects that are taken into consideration, only two of them focused directly on the **offender** side of the spectrum. The reason for this could be attributed to the huge dark number regarding cybercrime and hence the lack of understanding thereof. Data gathering methods and by consequence our evidence base are only partial<sup>66</sup>. Trying to prevent possible offenders becomes even more difficult when the majority of the offenders do not live in the same country as the victim. The German *Don't Offend* project is one of the two which does focus on the offender side. This project offers a free and confidential treatment option designed for those who have a sexual preference towards children. The goal is to prevent sexual offending and the consumption or production of child sexual abuse material online. The project works in a network like fashion, trying to reach as many patients throughout the 'Dunkelfeld' (dark field) and reaching as many possible (re)offenders in the country.

This outreach method is very active in the second offender oriented project as well. The Irish project *Cyber-UP CyberYouth Diversion Project* actively seeks youth that have the propensity to use their skills for malicious intent. Rather than adopting a punitive approach, the Irish police try to redirect their skills towards the good side of the spectrum. The police go online and meet the youth in their own habitat. When they are identified, the teens are then made aware of the negative consequences their online behaviour can have and are given the opportunity to educate themselves to redirect, share and improve their skills. The EC3 has an interesting webpage on this subject<sup>67</sup> which offers useful tips for parents and teachers and also shows positive alternatives at EU level. On the webpage, there is a link to the research 'Youth Pathways into Cybercrime' which tries to fill the knowledge gap on the youth offender side.

<sup>66</sup> Williams, M. L., & Levi, M. (2017). Cybercrime prevention. Handbook of Crime Prevention and Community Safety, 454.

<sup>67</sup> <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/cyber-crime-vs-cyber-security-what-will-you-choose#alternatives>

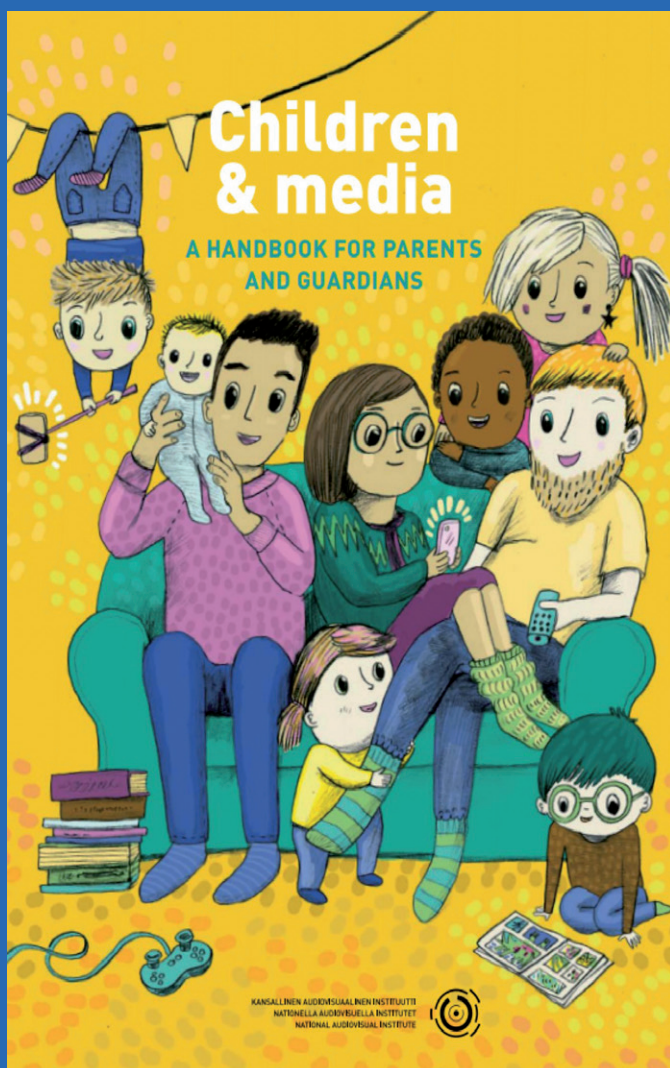


All other projects are oriented towards the prevention of **victimization**. This was perhaps the truest for the Portuguese project *PROTEUS* which aimed at raising awareness on a population level, but more specifically tried to capacitate professionals to support victims of identity theft and identity fraud. The German project *Cybercrime: the criminal investigation department explains* tries to educate the public in general on the typical tricks online fraudsters use. Although these projects focus on a more specific topic, it is more common for projects to cover a wide range of topics. For example, the Belgian project *Cybersimple* which offers easy information about the most common online threats and also shows practical tips on how to protect yourself against them.

Some projects target **different groups** at once. For example, the Czech project *Regions for Safe Internet* aims at children and students, parents, police, social workers, teachers, senior citizens and the public in general. It does so in tailored e-learning lessons and seminars. *Who's Joking with my Data* from Croatia, has a similar towards targeting different groups with a variety of actions. Another example is the Greek *Raise awareness for Cyber Crime through Innovative processes and applications*. Here the Hellenic police try to raise awareness within the police with workshops, lectures, but also uses mobile applications to target the youth.

In other projects, there is a more **targeted** focus. The Austrian *The Watchlist Internet* targets the online shopper for example and lists the fake sites and shops in order to warn users to not buy their products on these fraudulent sites. Also the *Danes' digital self-defense* aims more towards online consumers. The two offender oriented projects obviously also have this more targeted approach.

More often than not, **children** are the target group. As they are more and more online, they do have the highest risk of becoming a victim and learning the skills on how to deal with threats, how to prevent them,... at a young age is essential. The Bulgarian *Cyberscout program*, both Hungarian projects *Save Gordon and Fables of Crime Prevention- tales of Forest-town* are but a few examples here. Projects also target parents in their effort to reach the children. The Polish *Cyberjungle* and the Swedish *Safe Surfing* both try to activate parental interest and control over their children's online behaviour.



*This Children & Media Handbook is a concise review of media as a part of family life, exploring the media content used by children and their meaning in everyday life. The handbook provides links for accessing further information. In addition, the various chapters include useful tips on how to discuss media use in your family and seek the best ways your family can enjoy media from day to day.*

*The handbook is targeted for parents and guardians with children under 12-year old. The handbook has been very popular for example in media and internet related parental events in schools and kindergartens.*

Source: [https://kavi.fi/sites/default/files/documents/children\\_and\\_media.pdf](https://kavi.fi/sites/default/files/documents/children_and_media.pdf)

Aside from the obvious paternalistic reasons, a more pragmatic reason also leads to a more youthful focus. Most communication strategies regarding cybercrime prevention are made around exactly the cyber environment. *Boefproof* for example, the Dutch project, had a nationwide scope, but was found to be more successful in reaching the youth due to their social media campaign and the use of influencers to spread the message. Elderly people tend not to 'like and share' a GIF or watch a vlog on YouTube. Most likely, the best prevention strategy is avoidance according to the elderly. It is a very difficult exercise to not fall into the trap of scaring people instead of making them aware and use the Internet in an informed and safe manner. This does not only count for elderly people but is equally true for adults and children alike.

### 3.3. Partners

The Internet itself is organized in a **partnership approach**, consequently this seems true for cybercrime prevention activities as well. An important aspect here is that creating a strong cyber ecosystem involves all partners and not only the government and police. Every partner has a piece of the puzzle. The Romanian Internet Class is a good example of this multi-partnership approach as it combines relevant actors in telecommunication activities (mobile operators, Internet Service Providers, Ministry of communication,...), education (Ministry of Education, Ministry of Family, Microsoft, Google Romania, researchers, national police,...) and safety (Kaspersky Lab, Bitdefender, the Cybercrime Department,...).

Civil society is a very active partner throughout all the projects. This is especially true for the projects that are organised in the Insafe-INHOPE Network and the respective country's Safer Internet Centre. For example the Finnish Hotline Nettivihje is maintained by Safe the Children Finland (a part of the Safer Internet Centre) and tries to prevent re-victimisation of children that are depicted in child sexual abuse material by quickly removing it. Through a hotline people can anonymously report these materials. The Romanian, Bulgarian, Croatian and Portuguese project (*CyberGNRation*) also work with these centres as a partner and/or coordinator.



**Safer Internet Day 2018** | Tuesday 6 February

Create, connect and share respect:  
A better internet starts with you

[www.saferinternetday.org](http://www.saferinternetday.org)

European Commission

INHOPE

insafe

*Safer Internet Centres or SICs raise awareness regarding online risks amongst children, parents, teachers and caretakers. Every year in February, the European network combining all SICs, Insafe, but also global Safer Internet Committees, organize the Safer Internet Day. On this day, approximately 130 countries try to raise awareness on emerging online issues. In 2018, the theme was: "Create, connect and share respect: A better internet starts with you".*

Source: <https://www.betterinternetforkids.eu/> | <https://www.saferinternetday.org/web/sid/about>

Most projects also involve the **government** in their activities in either a coordinating way or supportive role. For example, the Hungarian project *Fables of Crime Prevention – tales of Forest-Town*, published interactive children’s books on a variety of topics, including cyber safety and security. The National Crime Prevention Council is the organizing actor here and made this crime preventing stories for schools to use. Another example where the government is a very visible partner is the *Regions for Safe Internet* from the Czech Republic. Here the Association of Regions of the Czech Republic is the coordinating actor. All 14 regions of the Czech Republic participate and are involved in the implementation. The government can also have a supportive role, as for example the ministry of education in school related projects.

Followed by the government, the **police** are common actors within cybercrime prevention. The Portuguese *CyberGNRation* makes sure that the police is capable of responding to the new environment but also sets up sensitization and awareness actions. The Vilnius City Police in the Lithuanian project *Safe behaviour* on the Internet goes to educational institutions in their territory to teach children the dangers of the Internet, but also the appropriate behaviour. Questions can be raised however on the position of the police in cybercrime prevention activities. Not in every country the police are seen as the best actor in this field. Educating the police is of equal importance as educating the public, not at least to prevent secondary victimization .<sup>68</sup>

*The European Cybercrime Training and Education Group (ECTEG) provides experience and knowledge to further enhance the coordination of cybercrime training for law enforcement agencies in the MS. As a project they are currently working on e-learning packages called ‘First Responders’. By the end of summer 2018 a first English version will be ready and will later on be translated in 7 EU languages. The project offers information to:*

- *identify and seize potential electronic evidence, including “live data” forensics;*
- *get awareness on cybercrime, internet, encryption, dark web and cryptocurrencies;*
- *assist victims of crimes facilitated by use of new technologies when taking complaint and starting criminal case.*

*This last part was very much welcomed during the workshop that was held in relation to this toolbox. Having a better informed and capable police will help close the gap with the public and lower the threshold to file complaints regarding cybercrime.*

**Source:** <https://www.ecteg.eu/running/first-responders/>

<sup>68</sup> EUCPN. (2016). EUCPN Toolbox Series No.7: Preventing Secondary Victimization. Policies and practices. Brussels

The actors that are most likely to be in the perfect position are situated in the private sector. As we can see in the projects, the **private sector** has an active involvement in 16 projects. It seems as if the sector takes – at least a part of the – responsibility for the governing or structuring of cyberspace and its users. ICT companies, Internet Service Providers, telecom sector, ... are the ones controlling the means and tools to access cyberspace and therefore have an important role to play. Google is the starting partner in *Cybersimple*, Microsoft provides content to the Danish app, Telenor as a major telecom player has an active involvement in the Bulgarian project, *Boefproof* involved Samsung, ...

*Did you know you can enable a SafeSearch preference on Google? By adjusting your settings, you can filter out adult content and explicit material in your search results. Just follow this link and switch it on: <https://www.google.com/preferences>. You can do the same for Bing on <https://www.bing.com/account>.*

*Don't want to tweak it yourself? Use Qwant instead! This European search engine never records your searches and never uses your personal data for advertising or other purposes. There even is a Qwant Junior which filters out inappropriate content and puts forward results that have recognized educational value. Go to <https://www.qwant.com> and install the extension.*

When it comes to children **schools** are of course the ideal setting for prevention activities. The Polish *Cyberprzemocowy Falochron* aims to establish online safety rules for the students on topics as cyberbullying, sexting, hate speech,... Similarly, the Lithuanian *Safe Behaviour on the Internet* lets the children sign a Code of Honourable Behaviour on the Internet. However no project goes as far as the Estonian *Cyber defence field of study at Põltsamaa Coeducational gymnasium*; an entire field of study on cyber-related issues is available in the upper secondary school curriculum and offers a program of 400 hours of study in three years.

Other interesting partners are **influencers** who can help to spread the message. The Romanian example uses a popular singer to further strengthen their campaign reach. *Boefproof* also targeted the public through social media influencers. There are some dangers however. Influencers do have their own agenda. Of course, they can help to spread the message but might adjust the message to their persona. It is important to acknowledge this and to have some clear rules on how to stick to the original message.

### 3.4. Methods

Almost all projects focus on target hardening techniques. They try to raise awareness and establish barriers to prevent victimization. The user is made aware of certain dangers, learns

how to recognize them and prevent them from happening. There are exceptions however: the two offender oriented projects of course focus on redirecting the skills (*Cyber-UP CyberYouth Diversion Project*) or offering therapy to people with perverse sexual desires (*Don't Offend*). The Finnish example tries to prevent revictimization by removing child sexual abuse material that is reported to them through a hotline.

Furthermore, the methods to raise awareness differ among the projects. Classical, top-down awareness campaigns are used, either in the form of a website or video (e.g. *Cybersimple*, *The Watchlist Internet*, *Cybercrime: the criminal investigation department explains* or *Who's Joking with my Data*), classes that are taught (*Cyberjungle*, *The Internet Class*) or applications (*Raise Awareness for Cyber Crime through Innovative Processes and Applications*). Some additions are however made in these campaigns to make them more appealing and interactive. **Gamification** is an important factor and is used in numerous activities. The *Cybersimple* website for example uses simple quizzes to spark the interest and hopes to activate the visitor of the website and let him or her engage with the tips and tricks that are provided. *Save Gordon* is perhaps the most showing gamified project. Children need to solve quizzes, puzzles, logical tasks,... related to cyber safety in order to free Gordon, a handcuffed bear.

The difficult part for prevention strategies here is on which user level they should focus. There is a huge knowledge gap between users. Some users are lightyears ahead of others when it comes to online skills. Not losing the interest of both sides is a very hard exercise. Peer-to-peer methods and empowerment more generally are a way out of this stalemate. A much known maxim is that the human factor is the weakest link in the defence line. Empowering some and giving them the means to share their knowledge could reverse this.

The *Danes' digital self-defense* application provides consumers with an overview and notifications of the latest alerts as well as advice on digital self-protection. An interesting aspect in this regard is that the app has the possibility to receive tips from the users themselves. The users are thus enhancing the knowledge pool and are able to share their own skills and experiences. The Estonian school program has the same objective, learning interested teens the right skills and let them share this with their family and peers. In the Bulgarian *Cyberscout program* this peer-to-peer model is used as the main method. Children are trained to be a cyberscout and get two-day training on online safety. At the same time, they are trained to be peer-to-peer trainers. The cyberscout is then expected to be a leading example, advise his or her peers and organize public activities aimed at their peers.

*Giving people a sense of responsibility helps to empower them in their online behaviour and skills. The Centre for Cybersecurity Belgium (CCB) offers a tool for citizens where they can send their detected phishing emails so the experts can further analyse it. Combined with a campaign explaining what phishing is and how to recognize it, people feel they are contributing to the solution.*

Source: <https://www.safeonweb.be/nl/wat-verdachtsafeonwebbe>

## 4. Conclusion and recommendations

When we looked at all the gathered projects we see that almost all of them were oriented towards victims. Only two projects focused directly on offenders. More research into the motivations of online **offenders** is advisable here. The difficulty of course stems from the anonymity that comes with the Internet. The outreach method from both offender oriented projects can serve as an example here. Challenging the skilful youths and giving them incentives to use their skills for a good cause is a good method here. In some cases, showing the consequences from their negative online behaviour could also have an inhibiting effect.

As stated, most of the projects focused on preventing online **victimization**. This was done either in a general scope (population level) or in a more targeted manner. As a recommendation here, it could be said that in order for a project to be as effective as possible, they should consider the online behaviour patterns of the targeted group when setting up their communication strategies. Differentiating among these groups is of crucial importance due to the different levels of knowledge throughout age and population groups. A nationwide campaign using social media or influencers would only partially reach adults or elderly people. For the same reason, it could be a suggestion to not make the distinction between offline and online behaviour when it comes to targeting children. Often, children do not make the distinction themselves as the online world becomes more and more a new reality. Overall critical thinking and social and responsible behaviour apply as much in the physical world as they do in the online world. Just as parental control is equally important.

When it comes to **partners** within the different projects, we can definitely see a multi-partnership approach. Nearly all actors of society take responsibility in the gathered projects. Private partners have an interesting role to play here and also offer some interesting possibilities in regard to transferability. Having international partners broadens the scope of implementation. Not only do they have the means, but they also have a wide reach. The private sector might have commercial interests, but as with the policy nexus (see part 1), this is beneficial for the user as well. Influencers might also have their own interests, so involving them in spreading the campaign message needs delicate deliberation. They can alter the message to their own agenda. Having a good and firm agreement here is absolutely a must as influencers do have great potential to reach certain target groups. This could be in some form of a non-disclosure agreement where there are some leeway possibilities within well-established boundaries. To lay down some rules of engagement is another recommendation directed towards the police. In order to prevent secondary victimization and for the police to be seen as an even better partner, officers should be made aware of the online threats and how to deal with cyber victims, training the officers is an important step here. Some projects already have made a good start in this regard.

Aside from three projects, all others are focused on **target hardening**, trying to raise awareness so citizens will better protect themselves and behave more safely. Activating parental control, as was explained for the Polish *Cyberjungle* for example, is another way of protecting children. Overall, **gamification and empowerment** are beneficial to all projects. Actively engaging with

the public keeps them interested and more open towards learning. Moreover, installing a peer-to-peer relationship bypasses the difficulties of the existing knowledge gap between users. This method offers the unique opportunity to not lose the interest of both sides of the spectrum.

Thorough impact **evaluation** proved to be lacking in the gathered projects. Most of them focus on outcome parameters such as the amount of clicks, amount of participants, ... These figures do not provide sufficient evidence to prove their effectiveness. Even these outcome parameters can be dubious and this does not always exclude 'preaching to the choir' statistics. Moreover, comparing crime records before and after the project is difficult due to the huge dark number and sometimes even irrelevant in light of the scope and target of the project. Rather than proving the strength of the project and its efficiency, more effort should be put into impact evaluations and the assessment of its effectiveness. Admittedly, more research has to be done on how to adequately evaluate cybercrime prevention activities<sup>69</sup>. There are exceptions – such as the *Cybersimple* campaign – using pre-post questionnaires, but these are scarce. The Bulgarian *Cyberscout program* keeps track of the received reports and calls regarding certain problems or issues from the cyberscouts. However this could filter out the benefits the peers had from the scout as only negative issues will be reported.

Overall, the prevention activities that were gathered here show great potential. One of the remarkable side-effects of cyberspace is that the encountered phenomena are universal. Citizens from Sweden can fall victim to fraudulent websites as easily as citizens from Poland. Safe online behaviour is the same in Germany as it is in Malta. In this regard, the content of the gathered projects are easily transferable to other countries. Looking for the green padlock right next to the URL will show you the security level of the website in Luxembourg and in Greece all the same. But although the content will be the same, the methods to spread the message must be different. What works in Sweden, might not work in Poland. Impact evaluations are a key shortcoming, but local embeddedness cannot be underestimated as well. Some partners will not be fit to be the leading actor in all countries. Some methods will work to a lesser extent when implemented in a different country. The games that are played, the books or the videos that are shown, are culturally sensitive. The national or local context should be thoroughly analysed before implementing or transposing another European project. *Think global, act local.*

<sup>69</sup> Williams, M. L., & Levi, M. (2017). Cybercrime prevention. Handbook of Crime Prevention and Community Safety, 454

## Lessons learned

### Orientation and target group

- ✓ *Prevention of offender:*
- ✓ *More research is needed on the motivations of online offenders*
- ✓ *Reach out to possible offenders*
- ✓ *Challenge skillful users and give positive alternatives and incentives*
- ✓ *Prevention of online victimization: Differentiate communication strategy based on the targeted group both in*
- ✓ *Means: use of influencers, sharing images, online or offline,...*
- ✓ *Content: beware of the knowledge gap*

### Partners

- ✓ *Multi-partnership approach: cyber safety is a shared responsibility*
- ✓ *Private sector partners can offer a wide reach and broad transferability possibilities*
- ✓ *Influencers have a great potential reach*  
*! Caution: stick to the original message!*
- ✓ *Police: watch out for secondary victimization*

### Methods

- ✓ *Gamification: actively engage your public*
- ✓ *Empowerment: installing peer-to-peer relations can bypass the knowledge gap problem*

### Evaluation

- ✓ *Impact evaluations are lacking*
- ✓ *More research is needed on how to evaluate cybercrime prevention activities*

## **Part 3** Overview ECPA 2017 projects and additional projects

---

### **Overview ECPA 2017 projects and additional projects**

## Austria: The Watchlist Internet



### Short Description

The Watchlist Internet is a project to prevent and to fight against online crime such as fraud and other online traps. Since 2013 the project team researches into fake sites and online fraud cases, with the objective to seriously inform the public at large with news articles on its website. Its unique selling points are continuity and effective search engine optimization. The project also contributes to fighting online crime at large by the network it has established between e-commerce platforms, private banks, governmental bodies and law enforcement agencies in Austria. Essential to the success of the project is also the close cooperation with the online dispute settlement body “Internet Ombudsmann” and with the stakeholders and users of the website, which contribute to reporting cases.

### Start/ Duration

The project started on the 3rd of July in 2013 and is still running.

### Background Research

There was an analysis of the context by the team of the Internet Ombudsmann. The noticed rise of Internet fraud cases, stressed the need to raise the efforts in awareness raising. The amount of cases raised by 18 percent in 2012 to the year before. Based on this data, the Watchlist Internet was founded by the Austrian Institute of Applied Telecommunication.

### Budget

The Watchlist Internet is funded by the Austrian Federal Ministry of Labour, Social Affairs and Consumer Protection, the Austrian Chamber of Labour, the largest Austrian online market place willhaben.at and the Bank Austria. The yearly costs of the project amount to approximately 65 000 euro/year.

### Type of evaluation

There has been an internal process evaluation in August 2014 in the form of an online survey among readers of the Watchlist Internet website. Based on these findings, the project was further shaped, for example using a more easy language with the regard to the older public. No external outcome or impact evaluation has been conducted, but an internal impact evaluation is done on a yearly basis.

### Actor conducting evaluation/ timing

Internal: by the project team and an advisory board with public and private stakeholders

### Type of data collection method

The annual evaluation is based on Google Analytics, such as user statistics, website visitors, visit duration,..., the feedback from users and funding partners, as well as constantly with checks on whether news about Internet fraud lead to the disappearance of a fake-site.

### Links to further information

<http://eucpn.org/document/watchlist-internet>

## Belgium: Cybersimple



### Short Description

Governments, NGOs and companies work towards making the Internet a safer place. Google and Test Achats recognize that everybody in society should play their part in helping citizens to enjoy the benefits of the Internet safe and secure. Therefore they have joined forces to develop Cybersimple, an initiative to raise awareness and to educate Belgian citizen about online security. On the cybersimple.be website citizens can get consumer-friendly information about the most common online threats and short practical tips how that they can easily implement to protect themselves and their families.

### Start/ Duration

The project started in April 2017 and is still running.

### Background Research

Before the project was initiated, Google and Test Achats commissioned a research to be conducted by GfK to give a clear understanding of users' perceptions towards online security, to uncover use cases where security and privacy are barriers for online behaviour and to reveal inner truths regarding the lack of safe and advanced web usage. This informed the topics that were chosen to showcase in the awareness campaign.

### Budget

The project is financed by Google and Test Achats. The cost of the campaign and its assets is 2 million Euros.

### Type of evaluation

There has been a process evaluation by monitoring the website usage with Google Analytics. The media company that was responsible for the delivery of the campaign adjusted its process according to its own monitoring tool. Additionally, there was an outcome evaluation by the same company, an additional company and Google Analytics.

### Actor conducting evaluation/ timing

External: Essence, OMD and Google Analytics

### Type of data collection method

The outcome of the campaign was evaluated in three ways. First, an online pre-post campaign survey was conducted on general awareness level, campaign awareness and campaign appreciation. Second, they have measured traffic and behaviour on the Cybersimple website. Lastly, it was measured if the media campaign increased awareness by 5 percent as was the goal.

### Links to further information

<http://eucpn.org/document/cybersimple>

## Bulgaria: Cyberscout program



### Short Description

Cyberscout program is two-day training on online safety for children in fifth grade (aged 11-12). The training uses an interactive methodology developed by experts of Bulgarian SIC, which has been upgraded regularly. The children are also trained for peer trainers using the peer-to-peer method, so that the knowledge can reach as many children as possible.

The mission of the Cyberscout program is to create a community of children and young people all over Bulgaria who demonstrate responsible and safe online behaviour and promote it among their peers. Certified Cyberscout is a trained student who:

- 1) Provides an example of safe and responsible online behaviour to their peers.
- 2) Advise their peers to a problem on the Internet.
- 3) Organizes and conducts public activities aimed at their peers.

### Start/ Duration

The project has started in 2015 and is still running.

### Background Research

The context was analysed before the project was initiated in 2015 by Bulgarian national representative research conducted by ARC Fund and partners as of a European-wide survey conducted by the research network EU kids online. They did this again before initiating the third year of the project.

### Budget

By the end of the 'third season' of the program (2018), a total of 22 trainings will be provided. The total cost will be 24 184 euro.

### Type of evaluation

The performance is evaluated via input and output questionnaires which children are asked to fill in in the beginning and end of their training. As such, these provide internal process evaluation since the team reflects on these findings after each training. These findings also present the team with an outcome evaluation after each training.

### Actor conducting evaluation/ timing

Before and after each training, the participating children are presented with questions on online safety issues and questions about attitudes to safe and responsible Internet use.

### Type of data collection method

See above

### Links to further information

<http://eucpn.org/document/cyberscout-program>

## Croatia: Who's Joking with my Data



REPUBLIC OF CROATIA  
MINISTRY OF THE INTERIOR  
GENERAL POLICE DIRECTORATE



NATIONAL PREVENTION PROJECT

### WHO'S JOKING WITH MY DATA

### Short Description

The purpose of the project is to provide knowledge and raise awareness of the public on the importance of the protection of personal data and the protection of privacy in the context of the use of Internet and social networks aiming at preventing Cyber Crime and levelling up Cyber Safety. The target groups of the project are: pupils of elementary and secondary schools, their parents and teachers, police officers, public authorities, state officials, personal data protection officers, citizens' associations, professional organizations and academic circles. A number of interrelated interactive activities, specially designed to appeal to each target group while using contemporary multimedia and newest technologies, train and inform citizens and raise their awareness on the protection of personal data with special emphasis on their protection in the digital environment, that is while using Internet and social networks.

### Start/ Duration

The project has started in February 2016 and is still ongoing.

### Background Research

Crime prevention police officers of the General Police Directorate conducted an analysis of indicators and trends related to crime and employees of the Personal Data Protection Agency analysed cases of abuse of personal data within their competence. The analyses were based on indicators of the police and the Personal Data Protection Agency, along with expert and scientific papers that were published

in the Republic of Croatia and other available materials published in the European Union and available online.

### Budget

The police and other partners used available human resources and resources for organization and implementation of activities, transportation and other material costs within their own budgets so that such costs were not monitored. An extra 18 000 euro was however spent on the project.

### Type of evaluation

There were two types of evaluation. An internal process evaluation looked inter alia into the participation rate and number of views of the film. An internal impact evaluation revealed the increase in reported offences, showing a public that is better informed and capable of recognizing risks.

### Actor conducting evaluation /timing

Both evaluations were internal and made by prevention police officers of the General Police Directorate, in cooperation with officers of the Personal Data Protection Agency.

### Type of data collection method

The performance of the project was measured by the following methods:

Qualitative methods: monthly reports on conducted activities, feedback from target groups regarding satisfaction with the conducted activity, feedback from partner and associate organizations regarding satisfaction with the conducted activity.

Quantitative methods: a number of educated students from primary and secondary schools, a number of educated police officers and other experts, a number of conducted workshops, a number of published and distributed didactic and informative materials, data about project monitoring in the media, a number of seminars, training and workshops for experts

### Links to further information

<http://eucpn.org/document/whos-joking-my-data>

## Czech Republic: Regions for Safe Internet



### Short Description

The aim of the project is to minimize the risks associated with the use of Internet and communication technologies, to raise awareness of these risks and to provide information about the possibilities of prevention in the area of electronic security.

The target groups of this project are children and students, parents and the public, police officers, social workers, teachers and senior citizens. E-learning lessons available on the project website were prepared for each target group. Lessons for children and students are complemented by a contest quiz. For senior citizens, short video footages focused on electronic security were prepared last year and awarded as the best crime prevention project in the Czech Republic. In addition to e-learning lessons and video footages, regular seminars for students, teachers and IT informatics take place each year.

### Start/ Duration

The project started on the 13th of September in 2013 and is still running.

### Background Research

The project utilized the already existing analyses of Seznam.cz and the Centre for the prevention of risky virtual communication at the Pedagogical Faculty of the Palacký University Olomouc – Research on Behaviour of Czech Children in the Internet Environment in 2013, and similar research

of the e-Safety project (research of teachers' bullying, etc.).

### Budget

In 2017, the project has a budget of approximately 70.000 euros.

### Type of evaluation

The project undergoes an annual process evaluation. An outcome evaluation is also carried out internally on an annual basis. It usually includes information on the regions which joined the project and project partners in the given year. In addition, it lists outcomes and results, such as number of video footages, number of e-learning lessons and regular seminars for specific target groups, information on contest quiz and statistics which allow for the comparison with previous years.

### Actor conducting evaluation/ timing

The process evaluation is done by the Council of the Association of Regions of the Czech Republic. The outcome evaluation is conducted by the head of the Regions for Safer Internet project.

### Type of data collection method

The evaluation criteria include the number of participants in individual activities or the number of project outputs.

### Links to further information

<http://eucpn.org/document/regions-safe-internet>

## Denmark: The Danes' digital self-defense



### Short Description

Crowdsourcing among consumers and co-creation with various societal actors has turned out to be a viable and relevant approach when it comes to raising awareness and stimulating online behavioural change among the Danes.

In April 2017 the Danish Consumer Council, the foundation TrygFonden and The Danish Crime Prevention Council launched the free app 'My digital self-defense' that has been downloaded by more than 50,000 Danes to their Smartphones.

The app pushes current alerts to the consumers, provided by a wide array of societal actors from public organizations, private companies and NGO's, when waves of cyber-attacks hit Danish mail-accounts. Also, the app provides guidance and advice on digital self-protection. Last, but not least interesting the app also provides the consumers with a channel to tipping the project on current threats, which the app users have done 1700 times since the launch of the app.

### Start/ Duration

The project started on 01/04/2017 and is still running.

### Background Research

In 2016, an extensive study on 'Digital Safety' was carried out by The Danish Consumer Council and the foundation TrygFonden with the aim to investigate if the experience of insecurity among the Danes was increasing due to newer uses of data

(Data brooking, and trading) the complexity of digital technologies and the regulatory requirements on Danish citizens to interact digitally with public institutions. A report was published in December 2016 stating a series of challenges in the matter: Inadequate legislation, digital business models not transparent to the consumers, and last but not least to what extent the average Dane experience a lack of digital competences.

### Budget

The operation and ongoing development of the app has a yearly budget of approx. 403.000 Euros.

### Type of evaluation

The project is subjected to weekly internal evaluation in the project team and monthly evaluations by the steering group to assess the process. During the first 6 months an outcome evaluation was conducted.

### Actor conducting evaluation/ timing

The process evaluation is done internally. The impact evaluation is measured by Google Analytics and Push woosh statistics. In the 4th quarter of 2017 a larger qualitative evaluation was planned.

### Type of data collection method

The following goals are measured continuously: effect of the launch campaign, received publicity, progressive amount of app downloads, rate of active app users and the progressive amount of tips received from the app users and the quality hereof.

### Links to further information

<http://eucpn.org/document/danes-digital-self-defense>

## Estonia: The cyber defence field of study at Põltsamaa Coeducational Gymnasium



### Short Description

In 2015, Põltsamaa Coeducational Gymnasium, a general education school in Põltsamaa, Estonia, became the first known school in Europe to implement a cyber defence field of studies in the upper secondary school curriculum. The school sees this as a vital innovation in the field of cybersecurity, which has been increasing in importance at an unstoppable rate in the past decades. Estonia and Europe will need both an informed digital society and more and more cybersecurity experts in the future. The aim of the project is to provide students with a more in depth education in cyber hygiene, ethics, relevant hardware and software, national defence and personal protection. In the Estonian cyber security expert career path, the programme is a new stepping stone - one that comes early rather than late. The first stages of the project have shown that the students are ready to take up this challenge. Are the policy-makers?

### Start/ Duration

The project has started in January 2015 and is currently still ongoing.

### Background Research

No real background research was done. However, everyday experiences were enough to show that students spend more and more time in cyber space, but do not understand the possible consequences or impact of their activities.

### Budget

For the three year-period (2015-2018): approx. 21.000 euros.

### Type of evaluation

There has been both a process evaluation and an impact evaluation.

### Actor conducting evaluation/ timing

Both evaluation types are conducted internally.

### Type of data collection method

The evaluations happened at the end of each course and also discussions, student feedback questionnaires and lesson observations were taken into consideration. Student's online behaviour was also informally monitored.

### Links to further information

<http://eucpn.org/document/cyber-defence-field-study-poltsamaa-coeducational-gymnasium>

## Finland: Finnish Hotline Nettivihje



### Short Description

The Finnish Hotline Nettivihje, maintained by Save the Children Finland, has been in operation since 2002. Nettivihje offers the public a way to anonymously report online child sexual abuse material (CSAM). The work of Nettivihje consists of daily assessment and classification of reports received by using ICCAM-solution.

The fast removal of CSAM prevents re-victimization of the children depicted in the material. By quickly passing on the information to both national and international law enforcement agencies both helps with the victim identification and saves children from ongoing abuse, also in Scandinavia.

National and international cooperation is key part of the hotline work. Nettivihje is a part of the International Association of Internet Hotlines (INHOPE) and closely cooperates with both national and international law enforcement agencies. Combating online child sexual exploitation requires diversified measures ranging from the activity of individual citizens to wider international cooperation.

### Start/ Duration

Finnish Hotline Nettivihje started in 2002 and is still ongoing.

### Background Research

No real research was conducted, but by 1995 it was already clear that the Internet was being used by persons with sexual

interest in children for the publication and exchange of Child Sexual Abuse Images. The Hotline was set up in 2002 to eradicate illegal material on the web.

### Budget

The annual costs of the operation are approximately €300.000

### Type of evaluation

The effectiveness of the process is evaluated internally on an ongoing basis. In regard to impact, it is important that the material passed on to the police has been properly assessed as illegal. This is the most important outcome factor.

### Actor conducting evaluation/ timing

Both are internal evaluations and based on law enforcement assessment.

### Type of data collection method

The evaluation is based on the number of received reports and the number of illegal content forwarded to the police.

### Links to further information

<http://eucpn.org/document/finnish-hotline-nettivihje>

## Germany: Don't Offend



**kein täter  
werden**  
PRÄVENTIONSNETZWERK

### Short Description

The German Prevention Network “Kein Täter Werden” (“Don’t offend!”) offers a free and confidential treatment option at all of its sites, designed for people who have a sexual preference for children and are seeking therapeutic help. In the context of the therapy, the affected persons receive support so as to prevent sexual offending in the form of both direct contact (hands-on CSA) and indirectly via the consumption or production of child sexual abuse images on the Internet. The goal of the therapy is to prevent sexual offending against minors as well as to prevent the consumption of child sexual abuse images. The project began at the Institute for Sexology and Sexual Medicine at the Charité University Clinic Berlin in 2005 and now encompasses 11 different sites across Germany, with common quality standards guaranteed by the Prevention Network “Kein Täter werden”. The goal is the establishment of a comprehensive, nationwide therapeutic offering.

### Start/ Duration

The project started on 01/06/2005 after a successful pilot study in July 2004. The project is still running.

### Background Research

From clinical experience with patients in a university clinic and from an epidemiological study, the sexologists knew that many men have sexual fantasies involving children. They sought help even though they were not (yet) under pressure from law enforcement. A pilot study was conducted before the enrolment of the actual project.

### Budget

In the last reporting year of 2016, the costs for personnel were approximately €555 000 and the non-personnel costs were approximately €71 000.

### Type of evaluation

Both process and outcome evaluations are carried out via regular interim and final reports to the respective funders.

### Actor conducting evaluation/ timing

These evaluations happen internally under the responsibility of the project manager. In its initial phase that was an external evaluation of the project website by academics.

### Type of data collection method

The reports contain information on the number of patient contacts, as well as on the progress and results of diagnostic assessments, therapy and aftercare. There is also regular supervision of the therapists, frequent case meetings and the sharing of ideas/experiences with colleagues and cooperation partners.

### Links to further information

<http://eucpn.org/document/dont-offend>

## Greece: Raise Awareness for Cyber Crime through Innovative Processes and Applications



### Short Description

The Cyber Crime Division of the Hellenic Police, in order to efficiently and effectively raise awareness about Internet safety, established in 2015 a specialized department named “Innovative Actions and Strategy Department”. It is focused on the innovative actions and design strategy for the raise awareness campaigns and cooperation with other stakeholders.

The campaigns include:

- Informative lectures and workshops all over the country
- Teleconferences with schools at national level
- Study visits at the Cyber Crime Division Headquarters
- 5 international conferences on Internet Safety
- Informative leaflets for different types of cybercrimes and dangers
- 3 TV and 3 radio spots
- The website [www.cyberkid.gr](http://www.cyberkid.gr), relevant application for mobile devices and Facebook page in order to inform parents and children about the Internet safety
- The website [cyberalert.gr](http://cyberalert.gr), relevant application for mobile devices, Facebook page and Twitter account in order to inform professionals for safe electronic transactions

### Start/ Duration

The project started in 2011 and it is still running.

### Background Research

Cyber Crime Division of Hellenic Police except from combating and prosecuting Cyber Crime pays particular attention to prevention and raise awareness. In this scope a unique department named “Innovative Actions and Strategy Department” was developed, which is responsible for planning and implementation of awareness activities and communication with public and private sector. The department collects data about new threats and trends from the operational departments of the Division and designs concrete raise awareness actions in order to efficiently and effectively inform citizens.

### Budget

All costs for the implementation of the project are covered by donations without burdening the budget of the Public Sector. Sponsors of the actions are mainly companies of the ICT sector which are concerned about Internet security issues and safe Internet usage.

### Type of evaluation

There has been no process or impact evaluation so far.

### Actor conducting evaluation/ timing

/

### Type of data collection method

/

### Links to further information

<http://eucpn.org/document/raise-awareness-cyber-crime-through-innovative-processes-and-applications>

## Hungary: Fables of Crime Prevention – Tales of Forest-town



### Short Description

The National Crime Prevention Council has published interactive children's books called Tales of Forest-town 1-2 and Life boat. The tales have different topics in the field of crime prevention, including computer security risks and the dangers of Internet. We believe that starting to draw the children's attention to safe Internet use at the earliest age is important.

In almost every family there are one or more smart phones or computers and it is important for the children to learn how to use them and what the dangers are.

The text of the tales can help children to learn assertive communication and conflict management and the charming, brave and helpful animal characters bring police officers and teachers closer to the children.

Besides the stories there are also exercises and picture puzzles in the storybooks which can be solved after reading the stories.

### Start/ Duration

The project started on 24/04/2015 and is still running.

### Background Research

An international comparative study, in which Hungary was active, showed that almost all of the answering experts predict that the number of Internet related crimes will increase in the future. The National Crime Prevention Council of Hungary also conducted a research with the participation of 10 000 students, in which children's Internet usage behaviour was studied.

### Budget

The writer of the tales works for the National Crime Prevention Council, so there are no extra human resources needed. The material costs were approx. €64.000.

### Type of evaluation

A process evaluation has been conducted. There has not been an impact evaluation yet.

### Actor conducting evaluation/ timing

Internal: The National Crime Prevention Council did interviews with the heads of the crime prevention units of the County Police Headquarters where the books were disseminated.

### Type of data collection method

Questions were asked about the available projects, interprofessional cooperation, needs and questions related to the work with the tales.

### Links to further information

<http://eucpn.org/document/fables-crime-prevention-forest-town>

## Ireland: Cyber-UP – CyberYouth Diversion Project

### Short Description

The world of the youth of Europe is migrating online as more and more communication, socialisation and education is carried out over computers and electronic networks. At the same time this online world provides a private global forum where e-skills can open access to significant illicit benefits and questionable peer recognition. The Cyber-Up youth diversion project of An Garda Síochána aims to help identified young people redirect those cyber skills to the benefit of their peers in a positive way by giving opportunities to learn, educate and share those skills with friends and benefactors.

### Start/ Duration

The project started on the 10th of September 2017 and is still running.

### Background Research

The context was analysed by investigators within the Garda Cyber Crime Bureau from its current and past caseload in which offenders under 18 were identified. These youths could have used those skills in a different manner if they were guided on the potential their knowledge presented, the benefits it could bring and the consequences of abusing those skills and the forums they used.

### Budget

The budget is still being identified but expected to be kept to a minimum with the primary investment being in terms of personnel.

### Type of evaluation

Due to its recent state, no type of evaluation has yet been conducted. However, both process and impact evaluation will form an

essential part of the project.

### Actor conducting evaluation/ timing

The foreseen evaluations will be carried out independently by one of the academic partner agencies.

### Type of data collection method

/

### Links to further information

<http://eucpn.org/document/cyber-cyberyouth-diversion-project>

## Lithuania: Safe Behaviour on the Internet



### Short Description

Vilnius City Third Police Unit of Vilnius County Police Headquarters decided to take action and to prevent the negative phenomena within the designated territory at the earliest

stage possible. During the implementation of the project a series of lectures were held at the 18 educational institutions in the area with the aim to have at least two project-related events at each institution. In addition, discussions with children were held, experience was shared and situational analysis was carried out by means of visual aids and situational modelling. Upon the completion of the full cycle of lectures within the framework of the project children signed the Code of Honourable Behaviour on the Internet, which was framed and hung in the classroom. Educators and parents were also provided with recommendations about actions, which need to be taken in order to identify the problems as soon as possible and to encourage the safe behaviour on the Internet. The initiative within the aforementioned project titled Protect Your Identity was held in the shopping centres of Vilnius, which encouraged the participants in the activities to treat their personal data more responsible. Finally, the participants in the initiative shared their experience about possible ways to lose or give away personal login data while being careless; the consequences of such carelessness are usually devastating, and resulting not only in financial trouble, but also in psychological burden.

### Start/ Duration

The project was launched on the first of March 2016 and continued till February 2017.

### Background Research

The project made use of the Eurobarometer on cyber security in 2013 and complemented this with findings from a national public opinion and identity theft survey in 2014. This information was collected and summarized in cooperation with educational institutions, as well as performing the analysis of numbers of received police reports regarding violation of rights in cyberspace.

### Budget

Only human resources of the Vilnius City Third Police Unit of Vilnius County Police Headquarters were used to implement the project, and lectures, presentations and situation-modelling activities were there main tools.

### Type of evaluation

Both a process and an impact evaluation have been performed.

### Actor conducting evaluation/ timing

The process evaluation was first carried out internally. As this turned out positive, the project entered a national crime prevention competition by the Ministry of Interior. Here there was an extra process evaluation. The impact evaluation was done only internally.

### Type of data collection method

Surveys/interviews of the employees of the educational institutions and also children and youth were carried out at the beginning and in the end of the project.

### Links to further information

<http://eucpn.org/document/safe-behaviour-internet>

## The Netherlands: Boefproof



### Short Description

Boefproof is part of a national awareness campaign for prevention, called “Do not make it too easy”. The name of this national campaign refers to making it less interesting for criminals to commit an actual crime. In Dutch “Boef” means criminal. The Boefproof campaign focuses on making mobile devices “criminal Proof” since mobile phones and portable computers were overrepresented when it comes to the loot of mugging and pick pocketing.

The Boefproof campaign started off in September 2014. It stimulates citizens to activate or install an anti-theft feature on a mobile device, thus making the device non-accessible by remote control in case it gets stolen. As a result, the stolen device becomes worthless for thieves and impossible to sell. Also, thieves cannot access e-mail, photos, and confidential documents. This ensures that files, including photos, are secured.

### Start/ Duration

The project started in September 2014 and is repeated annually. It is still running.

### Background Research

Through data from the national police in 2013 they identified the large amount of portable computers and smartphones that were stolen. Recent research commissioned by the Ministry of Security and Justice showed that 43% of the Dutch citizens surveyed still not know that they can change settings on their mobile phones and laptops in order to render them worthless for thieves.

### Budget

The costs are around 415.000 euro.

Type of evaluation

In 2016 an impact evaluation has been conducting marking the decrease of portable computers and smartphones that are stolen compared to 2013.

### Actor conducting evaluation/ timing

Internally.

### Type of data collection method

The evaluation is conducted on the basis of police data, looking at the effect on the number of mobile and portable devices that were stolen.

### Links to further information

<http://eucpn.org/document/boefproof>

## Poland: Cyber Jungle



### Short Description

“Cyberjungle” is an initiative aimed at children and young people and their caretakers. A program designed to enhance the level of safety is carried out in the form of meetings and workshops with children, youth and their parents, carers, teachers. A simple, accessible language and conversation about difficult issues is one of the advantages of Cyber Jungle.

The project consists of the various components:

- improve awareness of the perils connected with Internet use by children and youthful people and improving the safety of its users.
- activate parental control over children who employ the Internet and develop mechanisms for joint usage of it by children and their primary care providers.
- improve relations in the family and establishing the authority of the parent who is conversant with the specifics of virtual environments, youth becomes a collaborator for the adolescent in a conversation around the troubles

### Start/ Duration

The project started April 2008 and is still ongoing.

### Background Research

An analysis was conducted by the Department of Prevention of Police Headquarters based on questions posed by parents, educators, teachers during the meetings with the Police officers, and the letters addressed to the Headquarter, which all had been asking that the police should indulge into meetings with the youth and tell them about the risks of the Internet and share the statistical data on juvenile delinquency. This analysis has been elaborated with data from surveys conducted with a randomly selected group of parents participating in school meetings.

### Budget

In the first phase, the costs were 1000 euro. Regarding human resources, i.e. project preparation and the training of tutors, it is not possible to calculate the exact costs due to the fact that the charge of the project performed it as part of their duties.

### Type of evaluation

Both a process and impact evaluation have been conducted.

### Actor conducting evaluation/timing

Both types of evaluations have been conducted internally.

### Type of data collection method

The bases of the evaluations are the perceived interest of different entities and an analysis of statistical on criminal acts by minors.

### Links to further information

<http://eucpn.org/document/cyberjungle>

## Portugal: Project PROTEUS: supporting victims of identity theft and identity fraud



### Short Description

The project PROTEUS addressed the problems of cybercrime, namely identity theft and identity fraud. This 2-years-project was promoted by the Associação Portuguesa de Apoio à Vítima and had entities of other Member States as partners. The project's objectives were to raise awareness, protect victims of cybercrimes, and capacitate professionals to provide information and support to its victims. PROTEUS is targeted to the general public, law enforcement agents, judicial practitioners and victim support workers. It was based on the stakeholders' engagement for the development of the project's activities and outcomes, as they are key organisations linked to preventing and fighting cybercrime and providing information and support to its victims. To achieve the project's goals, training courses and workshops were held, best practice guides were developed, with a final conference having taken place in Lisbon. A campaign was also developed to raise awareness on adopting safe procedures when using the Internet.

### Start/ Duration

The project ran between 02/12/2013 and 01/12/2015.

### Background Research

Before starting the project, a contextual analysis was conducted by the Portuguese Association for Victim Support. They used the data from the 2012 Eurobarometer.

### Budget

The budget was €236.246, 80.

### Type of evaluation

There has been both a process and an impact evaluation.

### Actor conducting evaluation/ timing

The evaluations were done by the project management team every three months to readjust if necessary. The pilot training course and final conference was also evaluated by its participants.

### Type of data collection method

The project used the number of participants in the pilot training courses and in the workshops as indicators, the number of professionals who received the best practice guide, the number of organizations who received the best practice guide, the number of campaign materials developed and disseminated, the number of participants in the final conference, and the number of means used to disseminate the pilot training course, the best practice guide and the campaign materials.

### Links to further information

<http://eucpn.org/document/project-proteus-supporting-victims-identity-theft-and-identity-fraud>

## Romania: The Internet Class



### Short Description

The Internet Class or Ora de Net is a unique European project in Romania that promotes Internet safety for children and adolescents.

To reach the goal, they:

- organize training sessions and workshops on online safety issues for children, parents, teachers and specialists (National Police – prevention department representatives, school counsellors and social workers)
- offer advice - at ctrl\_Ajutor - one can ask any question about the Internet or using the technology
- offer a reporting line - at esc\_ABUZ - one can report the illegal content found on the Romanian webpages and help build a safer Internet.

The project collaborated with more than 2600 schools in over 430 cities and reached more than 360,000 children. 95,000 parents and teachers received information or counselling and more than 8,000 complaints were made on the specialized phone lines.

### Start/ Duration

The project started in 2008 and has been awarded funding until 2018.

### Background Research

The context was analysed by the project team, using national and international statistics and research. There was an identified need at European level to address the topic of Internet safety, reason why, in 2012, the European Commission elaborated the European Strategy for a Better Internet for Children and agreed to fund the setting up of a Safer Internet Center in each Member State.

### Budget

From January 2015 until July 2017, the project had a budget of 480.665 euros.

### Type of evaluation

The project has been regularly evaluated according to the project calendar.

### Actor conducting evaluation/ timing

The evaluations were performed by the project manager from the European Commission, as well as representatives of the Ministry of Informational Society.

### Type of data collection method

The main criteria for evaluation were: number and category of persons informed and included in the activities; number of calls on the Hotline; number of calls on the Helpline; materials and resources developed and disseminated nationwide; trained specialists.

### Links to further information

<http://eucpn.org/document/internet-class>

## Sweden: Safe Surfing

# Surfa Lugnt

### Short Description

Surfa Lugnt (Safe Surfing) is running a Swedish national initiative to raise school and adult knowledge about children's and young people's everyday lives on the Internet. The aim is to capture the benefits of young people's online life, such as commitment, communication and knowledge exchange, while giving parents and other adults more knowledge of managing pitfalls on the Internet, such as e-bullying and privacy issues.

On the website you will find tips about youth online habits and links to research on young people and the Internet. You can also ask questions and receive responses from their experts on Internet security and their teenage panel. There are tips and advice on twelve languages on the website.

Surfa Lugnt unites Swedish authorities, companies and non-profit organizations who are working together to improve adults' knowledge of youngsters' everyday activities on the internet and who inspire adults to take an active interest in youngsters' everyday Internet activities.

### Start/ Duration

The project started in April 2009 and is still ongoing.

### Background Research

The Post and Telecom Agency, the Government and Microsoft took the initiative and asked Kristina Axén Olin to start the New Surfa Lugnt because they were concerned

about the digital divide as well as saw the need for an organization that works for a safe Internet.

### Budget

The total cost of the project is approximately 103.000 euro annually.

### Type of evaluation

There has been no real process or impact evaluation. They do however measure visits to the website, Facebook, ordered folders, download of lesson pdf,...

### Actor conducting evaluation/ timing

/

### Type of data collection method

/

### Links to further information

<http://eucpn.org/document/safe-surfing>

## Additional projects

## Germany: Cybercrime: The criminal investigation department explains



### Short Description

A huge number of criminal offences could be prevented if the victims had been informed in advance of how criminals operate.

With this in mind, a Bavarian “cyber cop” reveals the typical tricks played by fraudsters in short video clips. He provides insights into his daily work and describes how offenders work to achieve their goals. In addition, he provides useful hints and tips on how to prevent such crimes from happening in the first place. By distributing such videos via official police social-media channels, the truly hair-raising stories of modern fraudsters are revealed and potential victims are protected from suffering serious damage.

More than 250,000 users in less than three months have already benefitted from this completely new channel of communication between citizens and public authorities.

### Start/Duration

The project started on the 10th of June 2017 and is still running.

### Background Research

Common data based on the Northern Upper Bavaria’s police headquarters’ statistical

yearbook were analysed by the social media team in cooperation with the cybercrime department of Ingolstadt’s criminal police service. Since 2010 they registered an increase of 46.2%.

### Budget

The project is embedded within the day-to-day work of the social media team, so no detailed specifications of costs can be made.

### Type of evaluation

There is a process evaluation in the form of figures showing the number of times the content is accessed.

### Actor conducting evaluation/ timing

The process evaluation is done externally.

### Type of data collection method

Ongoing assessment and analysis of the program’s user numbers.

### Links to further information

<http://eucpn.org/document/cybercrime-criminal-investigation-department-explains>

## Hungary: Save Gordon!



### Short Description

“Save Gordon!” is a crime prevention program based on experiential education developed by the Crime Prevention Subdivision of Zala County Police Headquarters in the framework of a project financed by the National Crime Prevention Council called “Network for safety”. The idea of the program is based on the experience that in a world full of information and stimulus it is hard to achieve objectives with preventive trainings in schools. With transforming the prevention topics into a playful form: “escape games”, the project tries to regain the attention of the children (10-14 years).

Gordon is a bear who is handcuffed and waiting for somebody to rescue him in 90 minutes. In that period of time students have to solve different exercises, logical tasks, quizzes to get small information packages related to crimes. To get the last code that finally frees Gordon they have to share the accumulated knowledge with the other teams. The last task is a survey that contains questions for each team. The whole class has to work together and discuss the questions.

### Start/Duration

The project started in 2016 and is still running.

### Background Research

/

### Budget

The total cost of the program is 29 820 euros. One ‘package’ of equipment costs 1 296 euros.

### Type of evaluation

No real evaluation has been conducted so far. They do ask feedback of the teachers and students.

### Actor conducting evaluation/timing

/

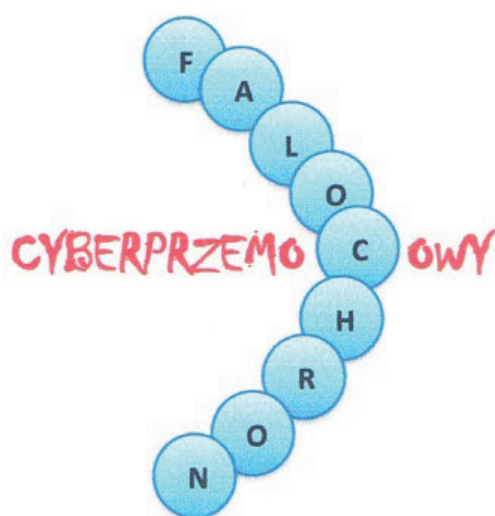
### Type of data collection method

/

### Links to further information

<http://eucpn.org/document/save-gordon>

## Poland: Cyberprzemocowy Falochron



### Short Description

The supervisors of the project disclosed a set of classroom scripts concerning online safety to other teachers, who then conducted a number of classes on topics like: cyberbullying, sexting, copyright laws, exposure to fake or disturbing content, sexual and financial abuse, hate speech etc. During the following classes a set of rules concerning online safety was established together with the students; it was then approved by the headmaster and propagated among other pupils. Additionally, policemen and an IT specialist were invited to meet the secondary school students both in the school building and in the local police headquarters to further their knowledge of the threat they can encounter online. The students' representatives who took part in the workshops were instructed to share their experience and newly gained knowledge with their peers during a form period. Furthermore, a number of contests were launched to further stimulate the students.

### Start/Duration

The project started on the first of September

2016 and ended the 20th of September 2017.

### Background Research

The issue was analysed by the ICT teachers, form teachers, parents, the school pedagogue and psychologist, Safety and Addiction Team and the student's council. Surveys were made among the students and teachers at the school. The matter was also discussed with the police. The school psychologist's notes were analysed.

### Budget

The project was realized as a result of volunteering work of the teachers and their own resources.

### Type of evaluation

Both a process and impact evaluation were conducted. Students were continuously checked on their interest in the proposed activities and also the parents were asked to evaluate the project. At the end of the project, an impact assessment was made.

### Actor conducting evaluation/timing

The impact assessment was conducted by the project coordinators. Process evaluation was done both internally and by the Center of Education and Digital Creation.

### Type of data collection method

The coordinators marked attendance in the competitions and activities and used interviews and questionnaires with parents and students as well.

### Links to further information

<http://eucpn.org/document/cyberprzemocowy-falochron>

## Poland: Served on the Tray



### Short Description

Maria Zientara Malewska's Primary School no 30 in Olsztyn has realized this all-Polish initiative. On the basis of the experiences from 2013/2014 from a different prevention project, the Primary School together with the Municipal Police Headquarters worked out the project "Served on the Tray". The objective of the project is extension of the student's knowledge of the human rights respect especially the right to the privacy and consciousness of the personal data prevention. This project is also addressed to the teachers to spread knowledge and competence about sufficient educational methods, and cooperation with parents and realization of their initiatives. The project is based on different initiatives like: educational meetings, debates and conferences, teachers workshops, art, literature, photographic competitions, or knowledge contests. It finishes with the City Game every year. The participants of the project are supplied with the didactic materials and lesson scenarios. The prevention materials are also published in local media.

### Start/Duration

The project is still running since the school year 2013/2014.

### Background Research

Before policemen from the Municipal Police Headquarter joined the Project, the cyber violence events, prevention of the personal data and privacy, were analysed. Especially the

police statistics according to the Internet crimes against the youngest children: swindles, identity thefts, cyber violence, encroach of the privacy rights. The information was taken from the Main Headquarter of the Police in Olsztyn and the region, as well as the Warmia and Mazury Provincial Police and from the Headquarter of the Police in Warsaw. The information from General Inspector of the Personal Data Prevention was also analysed. The information about different problems in Internet given from the students to the teachers was also taken into consideration. It was important to initiate the project because a lot of educational institutions were interested in this subject.

### Budget

The project is based on the work of the primary school teachers and staff and the prevention department of the municipal police in Olsztyn. All costs are covered in their daily activities.

### Type of evaluation

Both process and impact evaluations are conducted.

### Actor conducting evaluation/ timing

Both types of evaluation are conducted internally. There is an additional assessment each year where they present annual reports to the General Inspector of Personal Data Protection. The initiative got the 'Golden Pen' Award two times from this General Inspector.

### Type of data collection method

The evaluations are done by monitoring the interest rate of schools, educational institutions and cooperating institutions and quantity and quality of the initiatives.

### Links to further information

<http://eucpn.org/document/served-tray>

## Portugal: Safer Internet - CyberGNRation



### Short Description

The Safer Internet project that the GNR is conducting is developed at a national level and is based on police community principles. It includes eight lines of action:

- Analysis and investigation of the cybercrime in order to identify the foremost crimes related to the use of the Internet and assess their evolution.
- Training and Exercise provide the GNR military staff with the proper training that will allow them to respond within this new “space”.
- Impact assessment through the adoption of several assessment measures, the aim is to ensure that the objectives defined are achieved.
- Sensitization and awareness actions in the cyber prevention area engaging the overall school community and the society.
- Warnings through on-going publication of advice on social networks, with the aim to warn citizens and avoid their exposure to negative situations.
- Protocols to guarantee the cooperation of several institutions to build a joint crime

prevention policy.

- Develop resources to face the current social demands and to meet the challenges created by cyberspace.
- Partnerships to engage several social actors, with the aim of enlarging their communication channels.

### Start/Duration

The project began in January 2014 and is still running.

### Background Research

The context was analysed by the intelligence office, through databases that the security force uses to register crime incidents.

### Budget

The costs of the project result from the salaries of the police officers that work in the ‘special community programmes’ department and their logistic resources.

### Type of evaluation

Both a process and an impact evaluation have been conducted.

Actor conducting evaluation/ timing

Evaluation is conducted by the GNR themselves and externally by the Portuguese Board of Assessment and Accountability.

### Type of data collection method

The project is evaluated by assessing if the previously proposed goals are achieved and through evidence pertaining to an increase in security and a reduction in crime.

### Links to further information

<http://eucpn.org/document/safer-internet-cybergnrnation>

## References

**ENISA (2016).** *NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies*. Heraklion

**ENISA (2017).** *National Cyber Security Strategies*.

Retrieved from <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map>

**Christou, G. (2017).** The EU's Approach to Cybersecurity. *EU-Japan Security Cooperation: Challenges and Opportunities, 2017* (Spring/Summer), 1-13

**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

**Council of the European Union.** (2017). *Discussion paper on the EU's fight against cybercrime*. (10829/17). Brussels

**European Commission.** (2017). *Factsheet Resilience, Deterrence and Defence: Building strong cybersecurity in Europe*. Brussels

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

**EUCPN.** (2016). *EUCPN Toolbox Series No.8: Preventing cybercrime. Policies and practices*. Brussels

**Council of Europe (11/01/2018).** *Chart of signatures and ratifications of treaty 185*.

Retrieved from [https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p\\_auth=g7X0pLMm](https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=g7X0pLMm)

**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)

**Council of Europe (11/01/2018).** *Chart of signatures and ratifications of treaty 189*.

Retrieved from [https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p\\_auth=g7X0pLMm](https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=g7X0pLMm)

**Council of Europe (08/06/2017).** *Cybercrime: Towards a Protocol on evidence in the Cloud*.

Retrieved from <https://www.coe.int/en/web/human-rights-rule-of-law/-/cybercrime-towards-a-protocol-on-evidence-in-the-clo-1>

**T-CY Cloud Evidence Group.** (2016). *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY.* Strasbourg

**T-CY.** (2017). (DRAFT) *Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime.* Strasbourg

**T-CY.** (2014). *T-CY Rules of Procedure.* Strasbourg

**Council of Europe (30/10/2017).** *About C-PROC.*  
Retrieved from <https://rm.coe.int/cproc-about/1680762b41>

**EUCPN.** (2016). *EUCPN Toolbox Series No.8: Preventing cybercrime. Policies and practices.* Brussels

**EUCPN (2017).** *Cyber Safety: A theoretical Insight.* In: EUCPN Secretariat (eds.), *EUCPN Theoretical Paper Series*, European Crime Prevention Network: Brussels.

**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

**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, and replacing Council Framework Decision 2004/68/JHA

**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

**Christou, G.(2017).** *The EU's Approach to Cybersecurity. EU-Japan Security Cooperation: Challenges and Opportunities, 2017* (Spring/Summer), 1-13

**van der Meulen, Nicole, Eun Jo and Stefan Soesanto (2015).** *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses.* European Parliament [https://www.rand.org/pubs/research\\_reports/RR1354.html](https://www.rand.org/pubs/research_reports/RR1354.html)

**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

**Directive (EU) 2016/1148** of the European parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

**ENISA.** (2016). *ENISA Strategy 2016-2020*. Heraklion

**Regulation (EU) no 526/2013** of the European parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004

**EUCPN.** (2016). *EUCPN Toolbox Series No.7: Preventing Secondary Victimization. Policies and practices*. Brussels

**EUCPN.** (2016). *EUCPN Toolbox Series No.8: Preventing cybercrime. Policies and practices*. Brussels

**European Commission (2017).** *Commission staff working document Assessment of the EU 2013 Cybersecurity strategy*. Brussels

**Special Eurobarometer** 464, 2017

**European Commission.** (2016). *Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats*. Brussels

**ECISO.** (2017). *About ECISO*. Retrieved from <http://ecs-org.eu/about>

**European Commission.** (2010). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe*. Brussels

**European Commission.** (2014). *The EU explained: Digital Agenda for Europe*. Brussels

**European Commission.** (2015). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A digital Single Market Strategy for Europe*. Brussels

**Regulation (EU) 2016/679** of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

**Voigt, P., & von dem Bussche, A.** (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer.

**European Commission.** (2015). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A digital Single Market Strategy for Europe.* Brussels

**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 (Directive on privacy and electronic communications)

**Proposal for a Regulation** of the European parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

**European Commission.** (2017). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy A Connected Digital Single Market for All.* Brussels

**European Commission.** (2015). *Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security.* Brussels

**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 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, and replacing Council Framework Decision 2004/68/JHA

**Council framework decision** of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment (2001/413/JHA)

**European Commission.** (2017). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy A Connected Digital Single Market for All.* Brussels

**European Commission** President Jean-Claude Juncker, State of the Union Address, 13 September 2017

**European Commission.** (2017). *Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*. Brussels

**Proposal for a Regulation** of the European Parliament and of the Council on ENISA, the “EU Cybersecurity Agency”, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (“Cybersecurity Act”)

**Commission recommendation** of 13.9.2017 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises

**Annex to the Commission Recommendation** on Coordinated Response to Large Scale Cybersecurity Incidents and Crises

**Council Conclusions** on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (“Cyber Diplomacy Toolbox”), 19 June 2017. The Toolbox was presented earlier but is stated to be part of the package.

**Proposal for a Directive** of the European Parliament and Of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA

**European Commission.** (2017). *Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*. Brussels

**No more Ransom! (2017).** *About the project.*

Retrieved from <https://www.nomoreransom.org/en/about-the-project.html>

**Europol.** (2017). *EU Policy Cycle- EMPACT.*

Retrieved from <https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact>

**EUCPN Secretariat.** (2017). *EU Policy Cycle: what is it, how does it work and what is the role of prevention?!*. Brussels

**Europol.** (2017). *Serious and Organised Crime threat Assessment.* The Hague

**Council conclusions** on setting the EU’s priorities for the fight against organised and serious international crime between 2018 and 2021

**Communication from the Commission** to the Council and the European Parliament: Tackling crime in our digital age: establishing a European Cybercrime Centre (COM(2012) 140 final of 28 March 2012).

**Europol.** (2017). *Internet Organised Crime Threat Assessment (IOCTA) 2017*. The Hague

**ENISA (2016).** *NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies*. Heraklion

**Working Party** on General Matters including Evaluations (GENVAL). (2017). *Final Report on the seventh round of mutual evaluations on “The practical implementation and operation of the European policies on prevention and combating cybercrime”*. Brussels

**Williams, M. L., & Levi, M.** (2017). Cybercrime prevention. *Handbook of Crime Prevention and Community Safety*, 454.

## Contact details:

**EUCPN Secretariat**  
**Phone: +32 2 557 33 30**  
**Fax: +32 2 557 35 23**  
**Email: [eucpn@ibz.eu](mailto:eucpn@ibz.eu)**  
**Website: [www.eucpn.org](http://www.eucpn.org)**

