European Crime Prevention Award (ECPA)

Annex I

Approved by the EUCPN Management Board in 2017

Please complete the template in English in compliance with the ECPA criteria contained in the Rules and procedures for awarding and presenting the European Crime Prevention Award (Par.2 §3).

General information

1. Please specify your country.

Portugal

2. Is this your country's ECPA entry or an additional project?

3. What is the title of the project?

Safer Internet - CyberGNRation

4. Who is responsible for the project? Contact details.

Lieutenant Colonel João Carlos Marques Fonseca, Head of the Strategic Planning and International Affairs Division of the *Guarda Nacional Republicana* (GNR)

5. Start date of the project (dd/mm/yyyy)? Is the project still running (Yes/No)? If not, please provide the end date of the project.

The project began in January 2014 and is still running.

6. Where can we find more information about the project? Please provide links to the project's website or online reports or publications (preferably in English).

https://sway.com/Wl7_Ij0e-D7-ycIt http://www.gnr.pt/default.asp?do=tnov0r6r_vz24r05n/016vpvn5/016vpvn5_qr5p4vpn1&fonte=noticias&id=2136

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

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

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

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

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

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

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

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

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

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

http://www.portugal.gov.pt/pt/pm/documentos/20170331-pm-rasi-2016.aspx

http://www.gnr.pt/estrategia.aspx

http://www.gnr.pt/IG_Principal.aspx

https://goo.gl/ZMvhWN

https://goo.gl/6B4uuJ

https://goo.gl/3GcgwT

https://goo.gl/MDTjfY

https://goo.gl/hFTi8d

https://goo.gl/TJB7qj

https://goo.gl/bcHnx1

https://goo.gl/v18uwE

https://goo.gl/G2WU3T

https://goo.gl/3GYSGK

https://goo.gl/45pTFh

https://goo.gl/5aKV7b

https://goo.gl/bTehjE

https://goo.gl/agnrE4

https://goo.gl/FBwk3Z

https://goo.gl/4z327o

https://goo.gl/4HFDAX
https://goo.gl/qsSRaB

https://goo.gl/9eyUba

https://goo.gl/ub33L7

https://goo.gl/ZMvhWN

7. Please give a **one page** description of the project (**Max. 600 words)**

GNR intervention in protecting the population it serves begins with suiting the policing model, which is vital so that the GNR can respond to its current challenges. It is through Community Safety that the GNR ensures an adequate and proper intervention, fitting within a citizen of safety conception, not only because it sets the defence of the citizens' rights as first priority, but also because it should be the citizens themselves the stakeholders of their own fate.

For cyberspace to remain open and free, citizens should uphold the same norms, principles and values online that they do offline. Fundamental rights and the rule of law need to be protected in cyberspace.

The Safer Internet project includes several innovative initiatives, based on police community principles. The project that the GNR is conducting is developed at a national level. It includes eight lines of action followed over time within the scope of the overall GNR Strategy 2020 on cybersecurity.

In this context the project is based on lines of action that intend to contribute to the development of a generation that safely uses Internet - CyberGNRation:

- Analysis and investigation of the cybercrime phenomenon – this action aims to carry out a criminal analysis of the phenomenon in order to identify the foremost crimes related to the use of the Internet and assess their evolution with the development and implementation of the project.

- Training and Exercise – in order for the preventive actions to be effective it is necessary to provide the GNR military staff with the proper training that will allow them to respond within this new "space" (cyberspace). Another objective is to carry out exercises in conjunction with other institutions with different skills and responsibilities in cybersecurity, allowing to simulate risk situations and to identify measures for common problem resolution.

- Impact assessment – Measuring and demonstrating the social impact are crucial to validate the choices made and align the next step of the project. Through the adoption of several assessment measures, the aim is to ensure that the objectives defined are achieved in general and that these result in crime reduction and security increase.

- Sensitization and awareness actions on Cyber prevention directed to citizens, especially to youngsters, promoting Cybercrime prevention, strengthening the moral and ethical values from which cyberspace must be built; On-going awareness actions in the cyberprevention area engaging the overall school community, having a Safer Internet Day already been defined;
  Promotion of youth awareness of cognitive development, initiative and spirit of innovation and critical sense on issues of cybersecurity and cybercrime and inherently offenses concerning Internet.

- Warnings – through on-going publication of advice on social networks, namely Facebook and other social networks, the aim to warn citizens and avoid their exposure to negative situations. Particularly, to warn those that are most vulnerable, namely children, youngsters, elderly and businesses, against the actual dangers of Internet use.

- Protocols – The overall project implies continuous cooperation of several institutions of social, school and police areas so it is possible to build a joint crime prevention policy. Nationally and internationally promoting collaboration and cooperation between institutions and organizations in the field of Cybersecurity has enabled to enhance the GNR capacity through the exchange of knowledge and expertise that strengthens the institutional response capacity. In this process, security forces should collaborate and exchange information with other regulatory bodies, particularly personal data protection authorities, and actively involve these groups in defining crime prevention strategies.

- Resources – aware of the rapid and constant technological evolution and of the inherent risks, it is necessary to develop resources to face the current social demands and to meet the challenges created by cyberspace.

- Partnerships – to enhance the capacity to convey the GNR message in order to reach as many citizens as possible, the GNR has engaged several social actors in partnerships, with the aim of enlarging their communication channels given the great number of persons exposed daily to the threats of cyberspace.
  In this process, industry and organizations will be involved, in a cooperative perspective, in order that they themselves may identify their own concerns in terms of cybercrime with the objective to transmit these concerns to the security forces. Security forces can thus better determine and address crime prevention initiatives and define awareness initiatives to groups of risk (e.g.: youngsters and elders).

I. The project shall focus on prevention and/or reduction of everyday crime and fear of crime within the theme.

8. How does the project contribute to crime prevention and/or to the reduction of crime or the fear of crime? (**Max. 150 words**)

The key objective of the project is to create and instill a spirit of cybersecurity in most citizens so that the new generations of cyberspace users will be more aware of the risks inherent to Internet use.

The project consists essentially of different forms of communication networking and joint participation initiatives (awareness campaigns, training sessions, competitions, seminars, webcasts, etc.) to build and consolidate ethical and moral values among all cyberspace users, especially youngsters, prevent and reduce cybercrime, and increase the feeling of security among citizens.

This will be carried out by way of mobilization initiatives at a national level. The focus will be citizens that will be involved in prevention programmes concerning cybercrime, especially related to criminal activities that are conducted, more and more, on Internet. The ultimate goal is to reduce crime, reinforcing the "digital citizenship".

9. How is the project contributing to raising citizens' awareness of crime prevention? (**Max. 150 words**)

The integrated development of the actions that this project foresees will contribute to citizens being better informed about various cybercrimes and will take a more direct and active role, through the different project initiatives, in defining a national criminal cyberprevention programme.

In this project, industry and organizations will be involved (e.g.: training, workshops provided by security forces) in a cooperative perspective, in order that they themselves may identify their own concerns in terms of cybercrime with the objective to transmit these concerns to the security forces. Security forces can thus better determine and address crime prevention initiatives and define awareness initiatives to groups of risk.

Various types of competitions are carried out, for example, the consolidation of a "Charter of Cybersecurity Principles" written by youngsters in 2015 under the Safer Internet project, through initiatives.

Promoting a contest, first at a national level then at an international level, called "CyberChallenge" based on the disputes of challenges between teams constituted by students that can be challenged by organizations/companies.

II. The project shall have been evaluated and have achieved most or all of its objectives.[1]

10. What was the reason for setting up the project? What problem(s) did it aim to tackle?

The accelerated globalization process that we have witnessed in recent decades brought known advantages: millions of people worldwide escaped poverty; today we have access to consumer goods that was inconceivable a few years ago; we travel and communicate more easily; we trade by the minute and can invest anywhere in the world. In short, the new information technologies approached economies, regions and cultures.

The Internet – product of the scientific and technological revolution that keeps pace with globalization – has become an absolutely central instrument for the development of this process. Nevertheless, this centrality, whilst rendering potential, also entails risks, with implications in all areas – first and foremost for national security and defence.

In this strategic environment, analysis and ponderation on the options to make cannot lose sight of the interactions that exist between the globalization process, the "Global Commons" – which are the common areas where this works –, and the national security policy.

According to the information collected in recent years, there is a growing use of the Internet, particularly of the darknet, by isolated individuals and criminal groups to market very different types of illicit products.

On the other hand, the explosive growth of connected devices, within and beyond the still poorly defined borders of the Internet-of-things, could contribute to an increase in the complexity of creating attacks directed against a single person or entity and to an increment in the possibilities of using dispersed mechanisms as crime enhancer vectors. When the GNR decided to implement the project, there was no consolidated national cyberprevention programme outlined to prevent the occurrence of crimes related to Internet use. The increased use of cyberspace has led to a natural increase in crime, leading the security forces to have to develop police strategies to reduce crime rates and, on the other hand, to prevent the occurrence of new emerging cybermenaces.

11. Was the context analysed **before** the project was initiated? How, and by whom? Which data were used? (**Max. 150 words**)

The context was previously analysed by our intelligence office, through databases that our security force uses to register crime incidents; the existing data was processed and compiled, in particular those crimes pertaining to Internet use.

[1] For more information on evaluation, see Guidelines on the evaluation of crime prevention initiatives (EUCPN Toolbox No.3): http://www.eucpn.org/library/results.asp?category=32&pubdate

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

This cybersecurity project outlines GNR's view and the actions required, based on strongly protecting and promoting citizens' rights, to make the cyberspace a "safe place to circulate".

12. What were the objective(s) of the project? Please, if applicable, distinguish between main and secondary objectives. (**Max. 150 words**)

The main objective of the project is to increase the capacity of performing in the cyberworld, whereby ensuring that the institution provides an integrated answer to the crime phenomenon in the real and virtual world.

The following are specific objectives of the project:

- Prevent and reduce cybercrime, increasing the feeling of security among citizens.
- Create a global "Cyberawareness" programme that promotes closer cooperation among the various educational institutions, citizens and the GNR, which leads to joint initiatives that can promote cybercrime prevention through the consolidation and deepening of ethical values in cyberspace, using new web 2.0 technologies.
- Promote a greater critical spirit and a more active intervention of the whole population in the area of crime prevention, especially young people that we consider to be the greatest investment that Portugal has.
- Promote a new cyber generation, the CyberGNRation.
- Involve industry and organizations, in a cooperative perspective, so that they themselves may identify their own concerns and be able to prevent cybercrime.
- Cooperate with institutions of social, school and police areas so it can be possible to build a joint crime prevention policy.
- Create new tools to communicate and warn society against cybercrime risks.
- Provide the GNR military staff with competences to tackle new cyberspace challenges.

13. Did you build in internal goals to measure? If so, please describe at what stage of the project and how you measured whether the project was moving in the planned direction. (**Max. 150 words**)

Internal goals were built in to measure the performance of the project and are indicated in the GNR Strategy 2020 directive that the project will continue until the year 2020.

The objectives for the project are defined yearly through the commitment undertaken together with the Ministry of Internal Administration within the Framework of Evaluation and Accountability (QUAR).

Every year, after analysing the results achieved, the outcomes to be attained are defined for the following year in order to meet the project's objectives.

The ultimate goal is to strengthen and contribute to community safety and to collective responsibility in the prevention of crimes related to the Internet through education and training.

14. Has there been a process evaluation? Who conducted the evaluation (internally or externally?) and what where the main results? (**max. 300 words) -** *for more information on process evaluation, see EUCPN Toolbox No.3, p.9-10 & part 2 - section 2A*

This project has adopted a process evaluation that is conducted internally and externally with short and long-term goals. The impact and assessment of the results pertaining to the project's implementation are measured by applying the indicators defined at the start of the project. Every year the results achieved are analysed and assessed, and the goals for the following year are set.

The GNR carries out an internal self-assessment by analysing the statistical evolution of crime, which is incorporated in the Annual Intelligence Report and in the Activity Report, as well as the reports on lessons-learned, which are taken into account before the development of operations, and awareness-raising evaluation sheets (Awareness-raising actions are subject to evaluation by filling out a specific document by youngsters and teachers).

Externally these indicators are externally included in the Framework of Evaluation and Accountability, and in the Annual Report on Internal Security Report. The performance evaluation of each public administration service is based on a Framework of Evaluation and Accountability, subject to ongoing assessment and updated from the GNR intelligence systems, Integrated System for Management and Performance Evaluation of the Public Administration.

The GNR has conducted a systematic evaluation of the project through a (qualitative and quantitative) statistical analysis of the outcomes achieved by the different Special Programme Sections and encouraged carrying out academic research of Master's Theses in coordination with the Military Academy or the

Military University Institute. The GNR is currently developing an investigation project through the Master's made available by the Research and Development Centre of the Military University Institute, whose outcome will be presented in 2017.

By analyzing the indicators provided by the actual social networks, we seek to carry out an analysis and assessment of the number of citizens that have been reached and what their reactions are.

15. Has there been an outcome or impact evaluation? Who conducted the evaluation (internally or externally?), which data and evaluation method where used and what were the main results? (**Max. 300 words**) - *for more information on outcome or impact evaluation, see EUCPN Toolbox No.3, p.7-9 & part 2 - section 2A*

Over the last decades, the Internet and more broadly cyberspace has had a tremendous impact on all aspects of society. The project has been evaluated internally and externally.

At a national level, this evaluation is externally conducted by the Portuguese Board of Assessment and Accountability, which assesses performance in Public Administration, and also internally within the GNR Strategy 2020.

The objectives and the impact of the project in particular have been assessed and the proposed goals have been achieved. The evaluation of the impact on young people is carried out through questionnaires and through the promotion of master's degree studies on the subject in the Military Academy and civilian universities.

The impact is further analysed through evidence pertaining to an increase in security and a reduction in crime, however only on a long-term perspective will we be able to ascertain if the population's behaviour has effectively changed.

III. The project shall, as far as possible, be innovative, involving new methods or new approaches.

16. How is the project innovative in its methods and/or approaches? (**Max. 150 words**)

A Research-Action Method has been adopted to achieve the project, seeking to carry out a descriptive study on criminal phenomena, and sample assessment and signalling.

In order to foster the development of awareness raising actions, partnerships are established with the local councils and civil society organisations, as to guarantee that the GNR Special Programme Sections will have the resources needed to carry out awareness raising actions. The elderly and the nursing homes are

personally contacted to participate in awareness campaigns and related activities.

Some initiatives will use web 2.0 tools for teaching, learning and implementing cyberprevention programmes, namely in student development of cyberprevention games. The objectives pass through the engaging of several actors (academies, industry and organizations) in an overall cooperation perspective.

IV. The project shall be based on cooperation between partners, where possible.

18. Which partners or stakeholders were involved in the project and what was their involvement? (**Max. 200 words**)

The digital world is not controlled by a single entity. There are currently several stakeholders, of which many are commercial and non-governmental entities, involved in the day-to-day management of Internet resources, protocols and standards and in the future development of the Internet. This project aims to reaffirm the importance of all stakeholders in the current internet governance model and support this multi-stakeholder governance approach.

The partnerships made have been essential to quickly solve the problems of those citizens that are identified by the GNR personnel during patrolling or awareness raising and signalling actions and which go far beyond the area of competence of a security force.

In this project, industry and organizations will be involved (e.g.: training, workshops provided by security forces) in a cooperative perspective, in order that they themselves may identify their own concerns in terms of cybercrime with the objective to transmit these concerns to the security forces. Security forces can thus better determine and address crime prevention initiatives and define awareness initiatives to groups of risk.

The partners of the project are:

- Portuguese CERT (*Centro Nacional de Cibersegurança* – National Cybersecurity Centre)
- Microsoft
- Directorate of Innovation and Curriculum Development (*Direção Geral de Inovação e Desenvolvimento Curricular*)
- Disney
- Safer Internet
- Industry, especially "Start-ups"
- Other Police Forces (PSP, PJ)

V. The project shall be capable of replication in other Member States.

19. How and by whom is the project funded? (**Max. 150 words**)

The GNR is a security force of a military nature, constituted by military elements organized in a special body of troops, endowed with administrative autonomy.

The project is funded by the GNR budget and with the support of other partners. Main budget is related to humans resources and the development of contents. The partners support mainly the awareness campaign.

At the end of each year and in accordance with the objectives established for the following year, GNR budgetary funds are allocated to comply with the Activity Plan that includes the activities of several projects to be developed.

20. What were the costs of the project in terms of finances, material and human resources? (**Max. 150 words**)

The costs result from the salaries of the police officers that work in the "special community programmes" department (341) and the logistic resources used to conduct the various programme actions (fuel, paper, printing, etc.), and awareness initiatives to groups of risk and develop the contents.

21. Has a cost-benefit analysis been carried out? If so, describe the analysis, including how and by whom it was carried out and list the main findings of the analysis. (**Max. 150 words**)

A cost-benefit analysis was concisely carried out, whereby finding that the benefits were qualitative and quantitative and that the expenses had already been foreseen in the budget. The costs related to the project are reduced, when we intend to create a cybergeneration, a national consciousness to prepare the society to deal with cybercrime, which increases every year and could cost millions to citizens.

22. Are there adjustments to be made to the project to ensure a successful replication in another Member State?

We believe that no major adjustments are necessary so that the project can be replicated in another Member State, given that all European countries are currently developing a community policing culture by creating their own teams to guarantee greater proximity with citizens.

The partnerships made have been essential to quickly solve the problems of the citizens and to ensure that the project goals have been achieved.

23. How is the project relevant for other Member States? Please explain the European dimension of your project.

The project is relevant in the context of the EU International Cyberspace Strategy and European Security Agenda of 2015 because it outlines the vision and principles on applying core EU values and fundamental rights in cyberspace, permitting the improvement of ethical and moral values that shall be taken into account by Internet users, particularly youngsters.

Please provide a short general description of the project (abstract for inclusion in the conference booklet – **max. 150 words**).

The Safer Internet project includes eight lines of action followed over the scope of the GNR Strategy 2020 on cybersecurity:

- **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" (cyberspace).
- **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 cyberprevention 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.