http://doi.org/10.18239/jornadas_2021.34.27

The H2020 project RAYUELA: A fun way to fight cybercrime

Gregorio López[1], Nereida Bueno[2], Mario Castro[1], María Reneses[2], Jaime Pérez[1], María Riberas[2], Manuel Álvarez-Campana[3], Mario Vega-Barbas[3], Sonia Solera-Cotanilla[3], Leire Bastida[4], Ana Moya[4], Rubén Fernández[5], Violeta Vázquez[6], Germán Zango[6], Pedro Vicente[7]
[1]Instituto de Investigación Tecnológica, ICAI, Universidad Pontificia Comillas, Madrid, Spain
[2]Facultad de Ciencias Humanas y Sociales, Universidad Pontificia Comillas, Cantoblanco, Spain
[3]ETSI Telecomunicación, Universidad Politécnica de Madrid, Madrid, Spain
[4]Fundación Tecnalia Research and Innovation, Derio, Spain
[5]Policía Local de Valencia, Valencia, Spain
[6]Zabala Innovation Consulting, Madrid, Spain
[7]Pedro Vicente, Polícia Judiciária, Lisboa, Portugal
0000-0001-9954-3504, 0000-0003-1442-7905, 0000-0001-6328-8994, 0000-0002-9708-6896, 0000-0001-6044-0022, 0000-0003-2030-0310, 0000-0003-2747-9798, 0000-0003-4506-6284, 0000-0003-3516-4489, 0000-0002-2399-2757, 0000-0001-6180-2662, 0000-0001-8507-070X

Abstract- **As in the case of maieutics, this paper aims to unveil the most important goals and features of the recently funded European project RAYUELA by answering some important questions, such as: why, who, what, how, what the main challenges and novelty of the project are, and what will be next (although the project is still in its earlier stages).**

Index Terms- **Connected devices, Cyberbullying, Cybercriminality, Cybersecurity, Data analysis, Human Trafficking, Misinformation, Online grooming, Serious games**

Tipo de contribución: *Investigación en desarrollo*

I. Why?

Based on the UNICEF report 'The State of the World's Children 2017: Children in a Digital World', children and adolescents under 18 already account for an estimated one in three Internet users around the World [1]. Although these children and teenagers may be considered digital natives, sometimes they are not fully aware of the risks and threats, or of the benefits and opportunities that technology and the Internet offer. This very important issue can be tackled mainly from two different perspectives:

- Prevention: by teaching and training minors to make proper use of the Internet and associated technologies.
- Mitigation: by identifying potential risk profiles and implementing policies to protect them.

And is there a better way to do so than by playing? This is indeed the approach of the EU H2020 project RAYUELA (empoweRing and educAting YoUng pEople for the internet by pLAying) [2]. Fig. 1 shows the logo and motto of the project.

The name of the project is in turn inspired in the kid game hopscotch (*rayuela*, in Spanish) and in the famous Cortazar's novel with the same name, which was very provocative and innovative when it was published because its story depends on the decision the reader makes. In such a novel, Cortazar himself explained the kid game as follows [3]:

"*Hopscotch is played with a pebble that you move with the tip of your toe. The things you need: a sidewalk, a pebble, a toe, and a pretty chalk drawing, preferably in colors. On top is Heaven, on the bottom is Earth, it's very hard to get the pebble up to Heaven, you almost always miscalculate and the stone goes off the drawing. But little by little you start to get the knack of how to jump over the different squares (spiral hopscotch, rectangular hopscotch, fantasy hopscotch, not played very often) and then one day you learn how to leave Earth and make the pebble climb up into Heaven".*

So what is the Heaven of our particular RAYUELA? The answer to this question is that none other than contributing to make the Internet a better and safer place for minors.

Fig. 1. Logo and motto of the project

II. Who?

The RAYUELA project was funded with around € 5M under the subtopic 2 of the call H2020-SU-FCT01-2019, entitled "Understanding the drivers of cybercriminality, and new methods to prevent, investigate and mitigate cybercriminal behaviour". It is a 36-months project that started in October 2020.

The project is led by Universidad Pontificia Comillas and the consortium is composed of 17 partners from 9 different countries covering the main European geographical areas, as Fig. 2 illustrates.

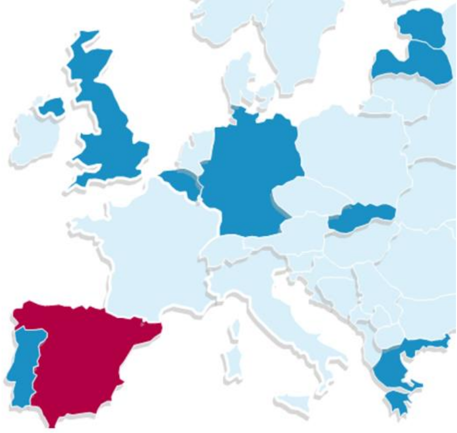
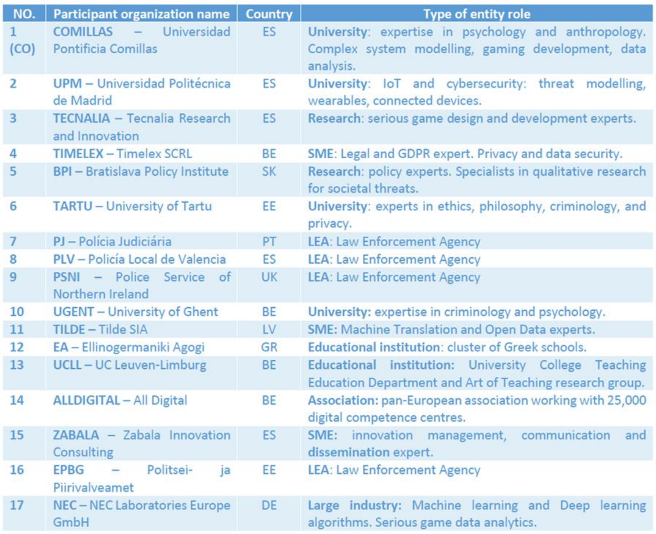


Fig. 2 RAYUELA's consortium map. In bold the countries where the project has footprint.

The consortium includes LEA (Law Enforcement Agencies), large industry companies and SME (Small to Medium Enterprise), research and academia, and educational institutions and associations. It stands out for its interdisciplinarity, bringing together LEAs, sociologists, psychologists, anthropologists, legal experts, ethicists, philosophers, educators, and computer scientists and engineers, as Fig. 3 shows.



NO.	Participant organization name	Country	Type of entity role
1 (CO)	**COMILLAS** – Universidad Pontificia Comillas	ES	**University**: expertise in psychology and anthropology. Complex system modelling, gaming development, data analysis.
2	**UPM** – Universidad Politécnica de Madrid	ES	**University**: IoT and cybersecurity: threat modelling, wearables, connected devices.
3	**TECNALIA** – Tecnalia Research and Innovation	ES	**Research**: serious game design and development experts.
4	**TIMELEX** – Timelex SCRL	BE	**SME**: Legal and GDPR expert. Privacy and data security.
5	**BPI** – Bratislava Policy Institute	SK	**Research**: policy experts. Specialists in qualitative research for societal threats.
6	**TARTU** – University of Tartu	EE	**University**: experts in ethics, philosophy, criminology, and privacy.
7	**PJ** – Polícia Judiciária	PT	**LEA**: Law Enforcement Agency
8	**PLV** – Policía Local de Valencia	ES	**LEA**: Law Enforcement Agency
9	**PSNI** – Police Service of Northern Ireland	UK	**LEA**: Law Enforcement Agency
10	**UGENT** – University of Ghent	BE	**University:** expertise in criminology and psychology.
11	**TILDE** – Tilde SIA	LV	**SME:** Machine Translation and Open Data experts.
12	**EA** – Ellinogermaniki Agogi	GR	**Educational institution**: cluster of Greek schools.
13	**UCLL** – UC Leuven-Limburg	BE	**Educational institution:** University College Teaching Education Department and Art of Teaching research group.
14	**ALLDIGITAL** – All Digital	BE	**Association:** pan-European association working with 25,000 digital competence centres.
15	**ZABALA** – Zabala Innovation Consulting	ES	**SME:** innovation management, communication and **dissemination** expert.
16	**EPBG** – Politsei- ja Piirivalveamet	EE	**LEA**: Law Enforcement Agency
17	**NEC** – NEC Laboratories Europe GmbH	DE	**Large industry:** Machine learning and Deep learning algorithms. Serious game data analytics.

Fig. 3 RAYUELA's list of partners including country, type of entity and expertise.

The project also counts with an IAB (International Advisory Board) which brings together international experts and relevant institutions, including LEA, public administrations and organizations, civil associations, and educational institutions. The main duties of such an IAB include providing guidance on the project direction and goals and feedback on the project progress and results, helping with generating awareness about the project and with reaching target users, and supporting the development of policies. Current members of the IAB are:

- INCIBE (Spanish National Cybersecurity Institute)
- OCC (Spanish Cybernetic Coordination Office)
- Belgian Federal Judicial Police
- Save The Children (Spain)
- Lifelong Learning Platform (Belgium)
- The Regional Department of Education, Youth and Sport of the Community of Madrid (Spain)
- CIPFP Misericordia, one of the Spanish national reference centres in vocational education

In addition, due to the importance of ethics and legal aspects, the project also counts with two external Ethics Advisors: Ofelia Tejerina-Rodríguez and Caroline Gans-Combe.

III. What?

The overall goal of the project is to bring together experts from different areas of knowledge from all over Europe to develop novel methodologies that allow better understanding the drivers and human factors affecting certain relevant ways of cybercriminality, as well as empowering and educating young people (children and teenagers primarily) in the benefits, risks and threats intrinsically linked to the use of the Internet, thus preventing and mitigating cybercriminal behavior.

As it has already been said, the project aims to achieve such an overall goal "by playing", which represents a novel method to do so. In particular, the project aims to develop an interactive story-like game that, on the one side, will allow minors to learn good practices on the use of the Internet and associated technology by playing, and, on the other side, will allow modelling, in a friendly and non-invasive manner, online habits and potential risk profiles related to cybersecurity and cybercriminality, providing LEA with scientifically sound foundations to define appropriate policies.

The cybercriminality and cybersecurity topics covered in the project include cyberbullying, online grooming, human trafficking for sexual exploitation, misinformation and deception, and the technological threats and risks associated to the connected devices used by minors.

IV. How?

Fig. 4 illustrates the research methodology that will be followed to achieve the aforementioned goal.

The first stage of the project (shown in the left-hand side of Fig. 4) will be twofold. On the one side, as it is shown in the upper left-hand side of Fig. 4, thorough research will be carried out on the sociological, anthropological, and psychological factors affecting the considered cybercrimes (i.e., cyberbullying, online grooming, human trafficking for sexual exploitation, and misinformation and deception). Traditional research methods in Social Sciences, such as semi-structured and in-depth interviews to victims, offenders, and experts, or focus group, will be applied in this stage.

On the other side, as it is shown in the lower left-hand side of Fig. 4, thorough research will be also carried out on the technological threats associated to the use of IoT (Internet of Things) devices (e.g., connected toys, wearables, or smart personal assistants), as well as on how human factors affect to the impact of such threats. In this case, traditional research methods in engineering, such as SLR (Systematic Literature Review), will be applied together with hand-in research, such as penetration testing or honeypot deployment and analysis.

As it is show in the centre of Fig. 4, the main findings of this first research stage will be translated into the interactive story-like game, which will address these topics through different cyber-adventures in which players may end up in a risky or safe situation depending on the decisions they make. Thus, the players may "live" different stories depending on the decisions they make while playing (and learn from them), the same way as the well-known Cortázar novel involves different stories depending on the decisions the reader makes while reading it. As a result, the game will be a safe environment where minors will face certain situations, in which they may fail and make wrong decisions, but they will have new chances to make the right ones, so they will learn good practices for behaving online in the real virtual world without taking any risk, the same way as pilots learn how to fly an actual plane in flight simulators.

Once the first prototype of the game is launched, it will be tested in several pilots across Europe, as shown in the right-hand side of Fig. 4. Such pilots will involve at least 150 secondary education students aged from 13 to 15 from the Greek cluster of German schools participating in the project, but also many more youngsters in both controlled (e.g., workshops, organized events) and uncontrolled environments (e.g., downloading the game from a market).

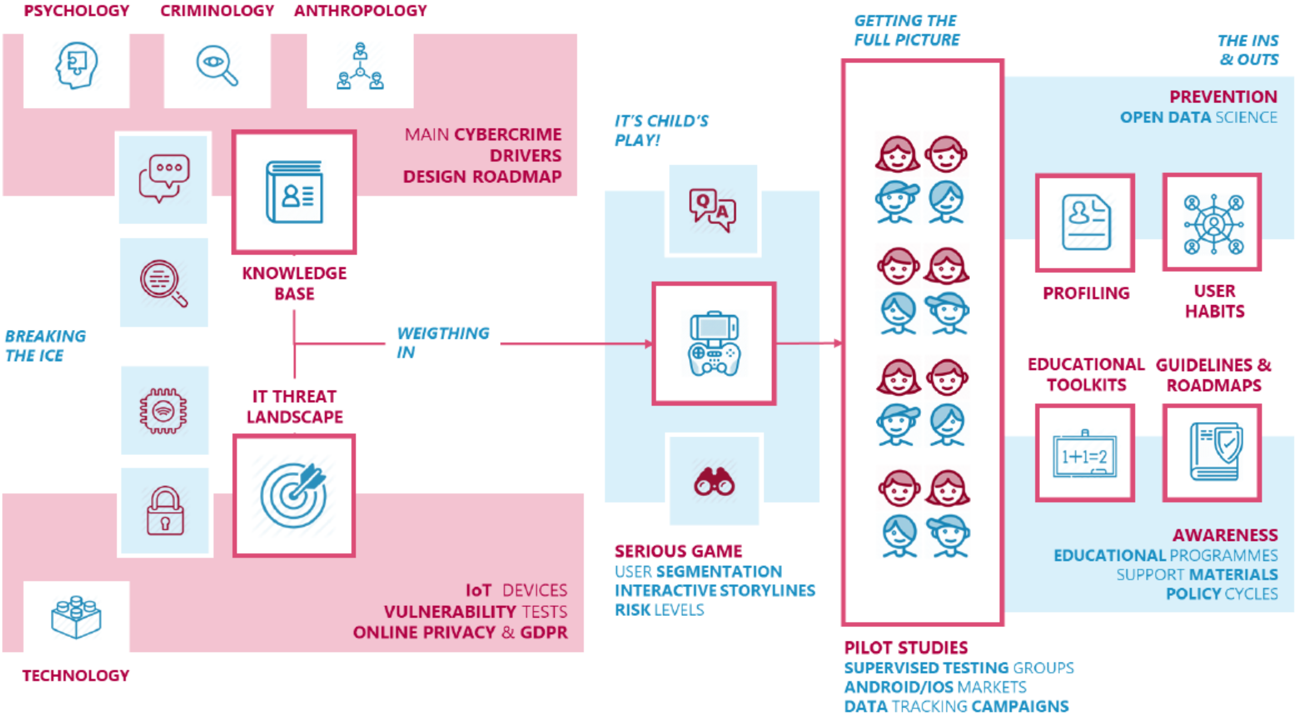


Fig. 4 Overview of the project.

The data gathered through the game will represent a large and diverse sample covering the most representative geographical areas in Europe. Such data will be pseudonymized and processed, combining Bayesian methods and Machine Learning/Deep Learning algorithms, and will be eventually interpreted jointly with the psychologists, sociologists, anthropologist, educators, and LEAs of the project to identify potential risky online habits and user profiles related to the considered topics.

The main conclusions of such analysis and interpretation will serve as input to the LEAs to develop evidence-based policies. Furthermore, the project will generate material to increase awareness and for capacity building among the interested stakeholders (e.g., LEAs, educators, minors, parents).

All this work will be carried out paying special attention to ethical and legal issues to avoid discrimination, stigmatization, or to prepare specific procedures for accidental findings well in advance. The workflow that has just been explained is organized in the work package structure shown in Fig. 5.

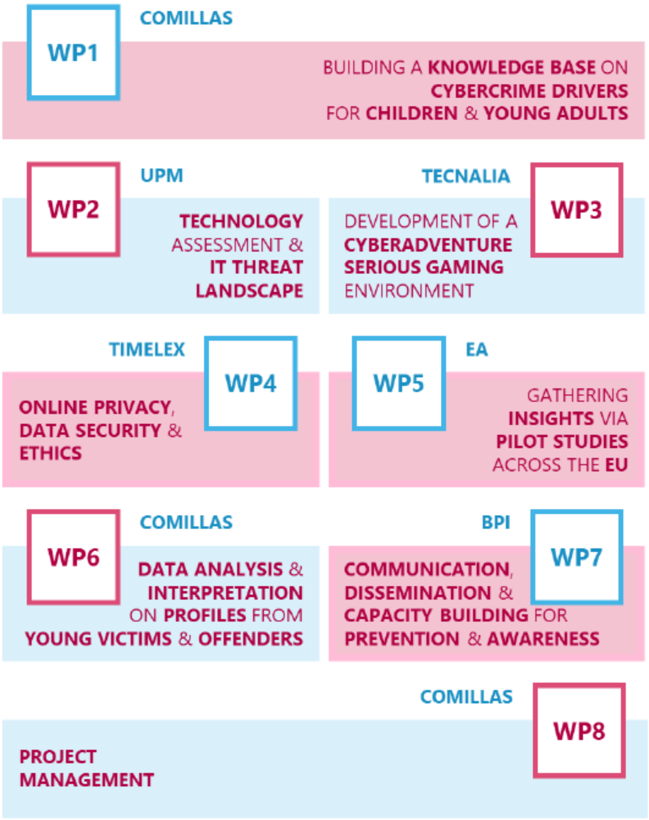

WP1
COMILLAS
BUILDING A KNOWLEDGE BASE ON CYBERCRIME DRIVERS FOR CHILDREN & YOUNG ADULTS
WP2
UPM
TECHNOLOGY ASSESSMENT & IT THREAT LANDSCAPE
TECNALIA
WP3
DEVELOPMENT OF A CYBERADVENTURE SERIOUS GAMING ENVIRONMENT
TIMELEX
WP4
ONLINE PRIVACY, DATA SECURITY & ETHICS
WP5
EA
GATHERING INSIGHTS VIA PILOT STUDIES ACROSS THE EU
WP6
COMILLAS
DATA ANALYSIS & INTERPRETATION ON PROFILES FROM YOUNG VICTIMS & OFFENDERS
BPI
WP7
COMMUNICATION, DISSEMINATION & CAPACITY BUILDING FOR PREVENTION & AWARENESS
COMILLAS
WP8
PROJECT MANAGEMENT

Fig. 5 RAYUELA's work package structure including work package leaders.

V. What are the main Challenges and Novelty?

Although serious games have been out there for quite a while, they have not been extensively applied to the knowledge area the project is focused on, which represents one of the innovations of the project.

Furthermore, serious games have been applied so far mainly for learning purposes and for assessing such a learning, but in this project the data gathered through the game is intended to be processed for profiling purposes as well, which represents one of the main challenges of the project. In this sense, the serious game will work as an amplifier of the traditional research methods used in Social Sciences.

Another great challenge of the project related to data analysis has to do with the lack of available data in this domain, which will make to explore, as part of the project, different approaches to generate synthetic data to test, select, and train the algorithms in advance.

In addition, unlike traditional research approaches where the impact on target users is unclear, in this case the target population will benefit from the main takeaways of the project directly by playing the game.

Last, but not least, ethical and legal issues represent definitely a challenge to carry out the research activities planned in the project being compliant with the highest standards in this regard, required by the target users of the game.

VI. What Next?

Although the project still has 30 months ahead, as a kind of outlook the project will try to promote further research by developing new serious games or by analysing the data gathered through ours for investigating, preventing and mitigating the effects of other online cybercrimes.

Acknowledgements

This work has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 882828. The authors would like to thank all the partners within the consortium for the fruitful collaboration and discussion. The sole responsibility for the content of this document lies with the authors and in no way reflects the views of the European Union.

References

[1] UNICEF, “The State of the World’s Children 2017: Children in a Digital World,” 2017

[2] RAYUELA’s webpage: https://www.rayuela-h2020.eu

[3] J. Cortázar, “Hopscotch,” 1963.