EDITORES:

Manuel A. Serrano - Eduardo Fernández-Medina

Cristina Alcaraz - Noemí de Castro - Guillermo Calvo

Actas de las VI Jornadas Nacionales
(JNIC2021 LIVE)

INVESTIGACIÓN EN ciber segu ridad

Ediciones de la Universidad
de Castilla-La Mancha

Investigación en Ciberseguridad

Actas de las VI Jornadas Nacionales (JNIC2021 LIVE)

Online 9-10 de junio de 2021
Universidad de Castilla-La Mancha

Investigación en Ciberseguridad

Actas de las VI Jornadas Nacionales (JNIC2021 LIVE)

Online 9-10 de junio de 2021
Universidad de Castilla-La Mancha

Editores:
Manuel A. Serrano,
Eduardo Fernández-Medina,
Cristina Alcaraz
Noemí de Castro
Guillermo Calvo

Ediciones de la Universidad
de Castilla-La Mancha

Cuenca, 2021




Edita: Ediciones de la Universidad de Castilla-La Mancha

Colección JORNADAS Y CONGRESOS n.º 34

Esta editorial es miembro de la UNE, lo que garantiza la difusión y comercialización de sus publicaciones a nivel nacional e internacional.

I.S.B.N.: 978-84-9044-463-4
D.O.I.: http://doi.org/10.18239/jornadas_2021.34.00

Hecho en España (U.E.) – *Made in Spain (E.U.)*

Bienvenida del Comité Organizador

Tras la parada provocada por la pandemia en 2020, las VI Jornadas Nacionales de Investigación en Ciberseguridad (JNIC) vuelven el 9 y 10 de Junio del 2021 con energías renovadas, y por primera vez en su historia, en un formato 100% online. Esta edición de las JNIC es organizada por los grupos GSyA y Alarcos de la Universidad de Castilla-La Mancha en Ciudad Real, y con la activa colaboración del comité ejecutivo, de los presidentes de los distintos comités de programa y del Instituto Nacional de Ciberseguridad (INCIBE). Continúa de este modo la senda de consolidación de unas jornadas que se celebraron por primera vez en León en 2015 y le siguieron Granada, Madrid, San Sebastián y Cáceres, consecutivamente hasta 2019, y que, en condiciones normales se habrían celebrado en Ciudad Real en 2020.

Estas jornadas se han convertido en un foro de encuentro de los actores más relevantes en el ámbito de la ciberseguridad en España. En ellas, no sólo se presentan algunos de los trabajos científicos punteros en las diversas áreas de ciberseguridad, sino que se presta especial atención a la formación e innovación educativa en materia de ciberseguridad, y también a la conexión con la industria, a través de propuestas de transferencia de tecnología. Tanto es así que, este año se presentan en el Programa de Transferencia algunas modificaciones sobre su funcionamiento y desarrollo que han sido diseñadas con la intención de mejorarlo y hacerlo más valioso para toda la comunidad investigadora en ciberseguridad.

Además de lo anterior, en las JNIC estarán presentes excepcionales ponentes (Soledad Antelada, del Lawrence Berkeley National Laboratory, Ramsés Gallego, de Micro Focus y Mónica Mateos, del Mando Conjunto de Ciberdefensa) mediante tres charlas invitadas y se desarrollarán dos mesas redondas. Éstas contarán con la participación de las organizaciones más relevantes en el panorama industrial, social y de emprendimiento en relación con la ciberseguridad, analizando y debatiendo el papel que está tomando la ciberseguridad en distintos ámbitos relevantes.

En esta edición de JNIC se han establecido tres modalidades de contribuciones de investigación, los clásicos artículos largos de investigación original, los artículos cortos con investigación en un estado más preliminar, y resúmenes extendidos de publicaciones muy relevantes y de alto impacto en materia de ciberseguridad publicados entre los años 2019 y 2021. En el caso de contribuciones de formación e innovación educativa, y también de transferencias se han considerado solamente artículos largos. Se han recibido para su valoración un total de 86

contribuciones organizadas en 26, 27 y 33 artículos largos, cortos y resúmenes ya publicados, de los que los respectivos comités de programa han aceptado 21, 19 y 27, respectivamente. En total se ha contado con una ratio de aceptación del 77%. Estas cifras indican una participación en las jornadas que continúa creciendo, y una madurez del sector español de la ciberseguridad que ya cuenta con un volumen importante de publicaciones de alto impacto.

El formato online de esta edición de las jornadas nos ha motivado a organizar las jornadas de modo más compacto, distinguiendo por primera vez entre actividades plenarias (charlas invitadas, mesas redondas, sesión de formación e innovación educativa, sesión de transferencia de tecnología, junto a inauguración y clausura) y sesiones paralelas de presentación de artículos científicos. En concreto, se han organizado 10 sesiones de presentación de artículos científicos en dos líneas paralelas, sobre las siguientes temáticas: detección de intrusos y gestión de anomalías (I y II), ciberataques e inteligencia de amenazas, análisis forense y cibercrimen, ciberseguridad industrial, inteligencia artificial y ciberseguridad, gobierno y riesgo, tecnologías emergentes y entrenamiento, criptografía, y finalmente privacidad.

En esta edición de las jornadas se han organizado dos números especiales de revistas con elevado factor de impacto para que los artículos científicos mejor valorados por el comité de programa científico puedan enviar versiones extendidas de dichos artículos. Adicionalmente, se han otorgado premios al mejor artículo en cada una de las categorías. En el marco de las JNIC también hemos contado con la participación de la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC), impulsando la ciberseguridad a través de la entrega de los premios al *Mejor Trabajo Fin de Máster en Ciberseguridad* y a la *Mejor Tesis Doctoral en Ciberseguridad*. También se ha querido acercar a los jóvenes talentos en ciberseguridad a las JNIC, a través de un CTF (Capture The Flag) organizado por la Universidad de Extremadura y patrocinado por Viewnext.

Desde el equipo que hemos organizado las JNIC2021 queremos agradecer a todas aquellas personas y entidades que han hecho posible su celebración, comenzando por los autores de los distintos trabajos enviados y los asistentes a las jornadas, los tres ponentes invitados, las personas y organizaciones que han participado en las dos mesas redondas, los integrantes de los distintos comités de programa por sus interesantes comentarios en los procesos de revisión y por su colaboración durante las fases de discusión y debate interno, los presidentes de las sesiones, la Universidad de Extremadura por organizar el CTF y la empresa Viewnext por patrocinarlo, los técnicos del área TIC de la UCLM por el apoyo con la plataforma de comunicación, los voluntarios de la UCLM y al resto de organizaciones y entidades patrocinadoras, entre las que se encuentra la Escuela Superior de Informática, el Departamento de Tecnologías y Sistemas de Información y el Instituto de Tecnologías y Sistemas de Información, todos ellos de la Universidad de Castilla-La Mancha, la red RENIC, las cátedras (Telefónica e Indra) y aulas (Avanttic y Alpinia) de la Escuela Superior de Informática, la empresa Cojali, y muy especialmente por su apoyo y contribución al propio INCIBE.

Manuel A. Serrano, Eduardo Fernández-Medina
Presidentes del Comité Organizador
Cristina Alcaraz
Presidenta del Comité de Programa Científico
Noemí de Castro
Presidenta del Comité de Programa de Formación e Innovación Educativa
Guillermo Calvo Flores
Presidente del Comité de Transferencia Tecnológica

Índice General

Comité Ejecutivo

Juan Díez González	INCIBE
Luis Javier García Villalba	Universidad de Complutense de Madrid
Eduardo Fernández-Medina Patón	Universidad de Castilla-La Mancha
Guillermo Suárez-Tangil	IMDEA Networks Institute
Andrés Caro Lindo	Universidad de Extremadura
Pedro García Teodoro	Universidad de Granada. Representante de red RENIC
Noemí de Castro García	Universidad de León
Rafael María Estepa Alonso	Universidad de Sevilla
Pedro Peris López	Universidad Carlos III de Madrid

Comité Organizador

Presidentes del Comité Organizador

Eduardo Fernández-Medina Patón	Universidad de Castilla-la Mancha
Manuel Ángel Serrano Martín	Universidad de Castilla-la Mancha

Finanzas

David García Rosado	Universidad de Castilla-la Mancha
Luis Enrique Sánchez Crespo	Universidad de Castilla-la Mancha

Actas

Antonio Santos-Olmo Parra	Universidad de Castilla-la Mancha

Difusión

Julio Moreno García-Nieto	Universidad de Castilla-la Mancha
José Antonio Cruz Lemus	Universidad de Castilla-la Mancha
María A Moraga de la Rubia	Universidad de Castilla-la Mancha

Webmaster

Aurelio José Horneros Cano	Universidad de Castilla-la Mancha

Logística y Organización

Ignacio García-Rodriguez de Guzmán	Universidad de Castilla-la Mancha
Ismael Caballero Muñoz-Reja	Universidad de Castilla-la Mancha
Gregoria Romero Grande	Universidad de Castilla-la Mancha
Natalia Sanchez Pinilla	Universidad de Castilla-la Mancha

Comité de Programa Científico

Presidenta

Cristina Alcaraz Tello	Universidad de Málaga

Miembros

Aitana Alonso Nogueira	INCIBE
Marcos Arjona Fernández	ElevenPaths
Ana Ayerbe Fernández-Cuesta	Tecnalia
Marta Beltrán Pardo	Universidad Rey Juan Carlos
Carlos Blanco Bueno	Universidad de Cantabria
Jorge Blasco Alís	Royal Holloway, University of London
Pino Caballero-Gil	Universidad de La Laguna
Andrés Caro Lindo	Universidad de Extremadura
Jordi Castellà Roca	Universitat Rovira i Virgili
José M. de Fuentes García-Romero de Tejada	Universidad Carlos III de Madrid
Jesús Esteban Díaz Verdejo	Universidad de Granada
Josep Lluis Ferrer Gomila	Universitat de les Illes Balears
Dario Fiore	IMDEA Software Institute
David García Rosado	Universidad de Castilla-La Mancha
Pedro García Teodoro	Universidad de Granada
Luis Javier García Villalba	Universidad Complutense de Madrid
Iñaki Garitano Garitano	Mondragon Unibertsitatea
Félix Gómez Mármol	Universidad de Murcia
Lorena González Manzano	Universidad Carlos III de Madrid
María Isabel González Vasco	Universidad Rey Juan Carlos I
Julio César Hernández Castro	University of Kent
Luis Hernández Encinas	CSIC
Jorge López Hernández-Ardieta	Banco Santander
Javier López Muñoz	Universidad de Málaga
Rafael Martínez Gasca	Universidad de Sevilla
Gregorio Martínez Pérez	Universidad de Murcia

David Megías Jiménez	Universitat Oberta de Cataluña
Luis Panizo Alonso	Universidad de León
Fernando Pérez González	Universidad de Vigo
Aljosa Pasic	ATOS
Ricardo J. Rodríguez	Universidad de Zaragoza
Fernando Román Muñoz	Universidad Complutense de Madrid
Luis Enrique Sánchez Crespo	Universidad de Castilla-La Mancha
José Soler	Technical University of Denmark-DTU
Miguel Soriano Ibáñez	Universidad Politécnica de Cataluña
Victor A. Villagrá González	Universidad Politécnica de Madrid
Urko Zurutuza Ortega	Mondragon Unibertsitatea
Lilian Adkinson Orellana	Gradiant
Juan Hernández Serrano	Universitat Politécnica de Cataluña

Comité de Programa de Formación e Innovación Educativa

Presidenta

Noemí De Castro García	Universidad de León

Miembros

Adriana Suárez Corona	Universidad de León
Raquel Poy Castro	Universidad de León
José Carlos Sancho Núñez	Universidad de Extremadura
Isaac Agudo Ruiz	Universidad de Málaga
Ana Isabel González-Tablas Ferreres	Universidad Carlos III de Madrid
Xavier Larriva	Universidad Politécnica de Madrid
Ana Lucila Sandoval Orozco	Universidad Complutense de Madrid
Lorena González Manzano	Universidad Carlos III de Madrid
María Isabel González Vasco	Universidad Rey Juan Carlos
David García Rosado	Universidad de Castilla - La Mancha
Sara García Bécares	INCIBE

Comité de Transferencia Tecnológica

Presidente

Guillermo Calvo Flores	INCIBE

Miembros

José Luis González Sánchez	COMPUTAEX
Marcos Arjona Fernández	ElevenPaths
Victor Villagrá González	Universidad Politécnica de Madrid
Luis Enrique Sánchez Crespo	Universidad de Castilla – La Mancha

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.

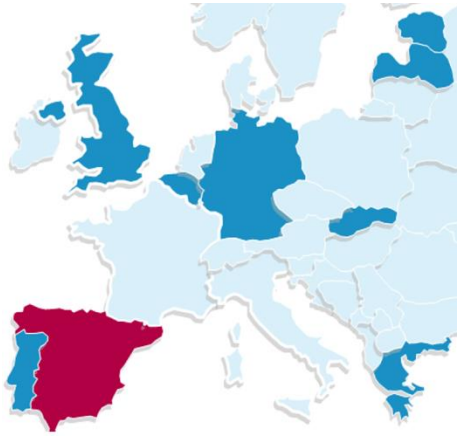

Fig. 2 RAYUELA's consortium map. In bold the countries where the project has footprint.

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

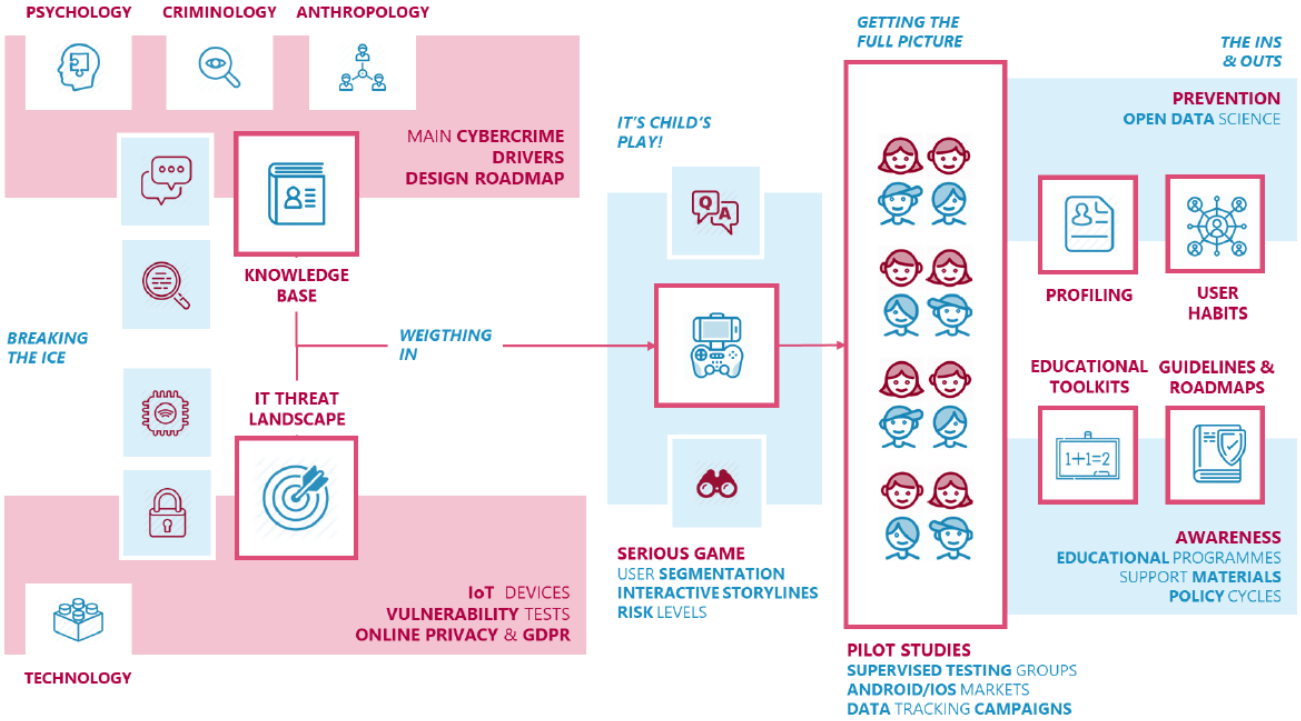

Fig. 4 Overview of the project.

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).

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.

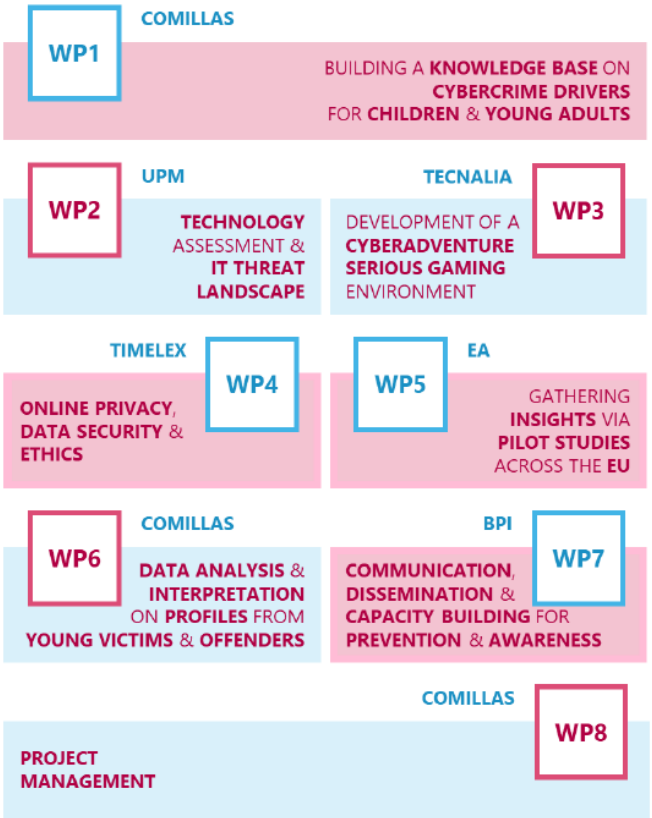

Fig. 5 RAYUELA's work package structure including work package leaders.

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.