ILEAnet
Innovation by Law Enforcement Agencies networking

SCIENTIFIC NEWSLETTER ILEANET

The ILEAnet scientific newsletter provides scientific news in the security research area. Published every two months, it is intended to highlight and promote the scientific work in the field of technology, human and social sciences. The coordination and scientific leadership of the ILEAnet project is provided by Professor Patrick Laclémence and his team at the ENSP research center.

PORTRAIT OF SECURITY RESEARCHERS

The ILEAnet project offers the opportunity to discover active profiles in university research.

BIBLIOGRAPHY

Find here a recent bibliographical selection of scientific and technical resources related to the four main themes of the ILEAnet project: cybersecurity,terrorism, organized crime and migration.

RESEARCHER'S TOOLBOX

ILEAnet provides tools and tips for researchers in order to help and support them in their scientific production and monitoring missions.

SCIENTIFIC COORDINATION TEAM

Eloïse CHASSAING
ILEAnet scientific facilitator & project manager
Eloïse is in charge of the animation of the ILEAnet scientific community, with the Community Manager. She facilitates the interaction between the law enforcement and academic communities and participates in the promotion of the European researchers in ILEAnet. She has a leading role in the drafting of scientific reports and monitors the scientific aspect of the tendering activity. Besides her role as the scientific facilitator, she supports the rest of the project's activities in close cooperation with the Work Packages leaders and the coordination team.

Audrey ROCHARD
ILEAnet legal expert & project manager
Audrey is in charge of two open calls launched by ILEAnet, aiming at providing studies with innovative solutions to law enforcement's daily needs and challenges. She is also in charge of the animation of the network of ILEAnet national contacts (INC), facilitating interactions between practitioners. Finally, she supports the rest of the project's activities as needed, in close cooperation with the Work Packages leaders and the coordination team.

Virginie SOLDAT
Community Manager
Virginie is in charge of managing and animating the ILEAnet network of security forces and scientists, assisting the European coordinator of this project and interacting with the scientific coordination. She is also in charge of monitoring and document management.

PORTRAIT OF RESEARCHERS

Karen Nuvoli

PhD Candidate in Communication and Media Studies
Sapienza University of Rome (Italy)
Aix Marseille University (France), linked to the IMSIC Institute

karen.nuvoli@uniroma1.it

Thesis directors:

- Alexandre Joux (EJCAM director)
- Christian Ruggiero (Associate Professor in Sociology of Cultural and Communicative Processes, Sapienza University of Rome)

Thesis coordinator: Mihaela Gavrila (Associate Professor in Television Studies and Sociology of Cultural and Communicative Processes, Sapienza University of Rome)

What is your background Karen?

I have a degree in Investigative Sciences, a Master 1 in Criminology and a Master 2 in Communication and Social Research. Currently I am a PhD student in Communication and Social Research and my thesis is co-supervised by two universities: La Sapienza di Roma University and Aix-Marseille University. This co-supervision was important for me because it represents a great advantage for my research: it is an opportunity to study in a multicultural environment which allows me to acquire a pedagogical culture, develop my critical thinking and my capacities of adaptability and resilience. It also allowed me to carry out a comparative analysis between France and Italy. The aim of my thesis work is to understand the main issues in the process of cognitive radicalisation leading to extremism and to make a comparison on the state of thinking in two European countries, such as France and Italy.

When did you realise you wanted to search?

I became interested in the problem of radicalisation during my master's studies, even before Daesh declared its caliphate. This is when I was working on al-Qaeda propaganda that I realised that I wanted to do research. Since my master in criminology, I have never stopped working on terrorism, radicalisation and all security-related issues. I has been working deeper on the communication aspect to answer the following question: “how are communication instruments used and how can we protect ourselves against radicalisation?”.

> “Fake truth and real threat: fake news and disinformation as a possible factor for violent action”

What is your current research focus?

My research is entitled "Fake news and misinformation as possible activators of violent extremism". It is in line with the long-term observation that I started in 2014. I designed this study to understand what kind of individual and collective impulses fake news can trigger (with the aim of analysing the opportunity structures and cognitive reasoning leading to violent extremism). The methodological approach is a qualitative study supported by semi-structured research interviews with experts from different disciplines, both in academia and in law enforcement organisations (such as Europol). This choice of interviews was motivated by the problematic and the exploratory and multidisciplinary vocation that I wanted to attribute to my research. The objective of my studies and of this thesis is essentially prevention (preventing and identifying hateful signs) but also promoting training (training of operators, of the community and at schools).

How do you think research on this subject will develop?

In contemporary societies the traditional socialisation is being replaced by another type of socialisation that we can call media socialisation. So I think that the war of influence will become increasingly important. We should broaden the spectrum of prevention of violent extremism to include emerging radicalities. As the media expresses ideologies more easily and is able to polarise ideological groups, I think we will find a continuous presence of actors, movements, networks and we will be confronted with increasingly unstructured, highly suggestible and conditionable individuals. More importance should be given today to the assessment of the individual risk of violence.

What could be done to limit online radicalisation?

All the topics I study are related to security and cybersecurity. The EU is working on several fronts but there should be a stronger response in order to create a truly open and secure cyber space, to increase trust. Indeed, there is a lack of trust in traditional institutions and that is why individuals are attracted by discourses, including conspiracy speeches. It is therefore important to stimulate research in this direction, and it will only be possible if researchers, private institutions and law enforcement agencies work together. It is essential to stay in touch with academics and to facilitate the exchange of information between experts at European level. For example, I very much appreciate the EMPACT platform which is the European Multidisciplinary Platform against Criminal Threats: it is a security initiative led by the EU Member States to identify and combat the threats posed by international organised crime. Why not open up these platforms to researchers, why not integrate them into projects already in place?

How do you see your role as a researcher?

I feel a great responsibility because radicalisation and related topics are developing rapidly, and I have seen the extent to which they have grown since the beginning of my study. In addition, we are behind in the answers we need to give and we should really include these subjects in our training, particularly at school. Today, there is no longer any separation between online and offline discourse among young people and there are risks linked to the use of social networks. We need to train today’s young people because they are tomorrow’s citizens.

In your opinion, how can law enforcement agencies (LEAs) and researchers be brought together better?

Apart from organising workshops in this sense, perhaps creating laboratories that will act as a link between LEAs and researchers, and above all without setting any limits. I see many projects with age or membership limits for researchers: it should be an open and free brainstorming so that the researchers feel they can talk and the experts perceive the researcher not only as someone who is enclosed in a laboratory but as someone who can bring solutions and a different vision. The multidisciplinary and multicultural approaches are very important as I noticed it in my interviews: sociologists, anthropologists and police forces differently perceive the same subject. Solutions can emerge only if there is a discussion and a collaboration between the stakeholders. I'd like to see more platforms like ILEAnet, encouraging discussions, organising events between researchers, communities and law enforcement.

How do you communicate your research results?

I participate in international conferences and seminars. For example, with the EJCAM in Marseille (School of Communication and Journalism) we held an international conference on the subject of information manipulation. Besides, I wrote for the Italian police academy and trained law enforcement practitioners on this topic.

How do you think European research will develop?

When I started my co-supervision process, there was no real link between European universities. The following year, CIVIS (a network of European universities) was created. It is only the beginning of the initiative but it is beneficial because there are already meetings between researchers from different countries. Due to its geographic nature as a global hub of international collaboration, Europe is at the frontline of innovation and research. Creative environments for staff and students, high standards of research integrity and ethical rules with the support to local and international communities via research-lead projects might have a key role in the future of European research.

Thank you very much Karen for your time and for this very interesting exchange!

To find out more about Karen's work, here are some of her publications:

2021 - (publication in progress) Manipulation de l'information et radicalisation - Actes de conférence, Colloque international Journalisme et Plateformes 2 : information, infomédiation et « fake news » - Marseille

2021 - (publication in progress) Pandemia, social media e complotti – Actes de conférence, V Conferenza Nazionale delle Dottorande e dei Dottorandi in Scienze Sociali

2020 - L'evoluzione dei conflitti, tra sicurezza, culture e complessità, Recensione al testo di Mary Kaldor, Global security cultures, Polity Press, Cambridge, Rivista trimestrale della scuola di perfezionamento per le forze di polizia, n.2-3

2020 - La disinformazione nel sistema mediale ibrido. Dalle fake-news al deepfake pp. 85-96. ISBN 978-88-9377-155-9

2018 – Dalle fake-news alle verità alternative: una nuova sfida per il giornalismo della post-verità, Comunicazionepuntodoc n. 20 12/2018, Lupetti Editore, ISBN 9788868742553

2018 - L'evoluzione del jihadismo online, Rivista di Studi Politici - ISSN 1120-4036. - Gennaio/Marzo, pp. 160-177

BIBLIOGRAPHY

The ILEAnet scientific coordination team suggests a recent bibliographical selection of scientific and technical resources related to the four main themes of the ILEAnet project: cybersecurity, terrorism, organised crime and migration. Resources can be found in the ILEAnet Knowledge Library. If you want to share a publication, please contact us at ensp-ileanet@interieur.gouv.fr

ILEAnet is collecting the most recent or relevant publications in the following areas, but does not necessarily endorse their contents.

Cybersecurity

Scientific Information

Hemdan, E.E.-D., Manjaiah, D.H., 2021. **An efficient digital forensic model for cybercrimes investigation in cloud computing**. Multimed Tools Appl. https://doi.org/10.1007/s11042-020-10358-x

In recent times, cloud computing adopted numerous organizations and enterprises for offering services with securely certifying that cloud providers against illegitimate activities. However, cost-effective forensics design and implementation for support the cloud-based cybercrimes investigation. To build cloud architecture support forensics is a significant and complex issue such as voluminous intricate legal, organizational, and technical defies due to the virtualization, distributing, and dynamic nature of cloud systems. Therefore, this paper presents an efficient Cloud Forensics Investigation Model (CFIM) to investigate cloud crimes in a forensically sound and timely fashion.

Maurushat, A., Al-Alosi, H., 2021. **Policing cybercrime: an inside look at private and public cybercrime investigations**, in: Australian Policing: Critical Issues in 21st Century Police Practice. pp. 333-348. https://researchdirect.westernsydney.edu.au/islandora/object/uws%3A59040

This article addresses the issue of policing cybercrime, based on the Australian example and the Australian law. It focuses on terminology and overview, case studies, and an analysis of key issues and challenges for policing. Where possible, the *chapter refers to case studies in which Australia had either a victim link or where and Australian private or law enforcement was involved in the investigation.*

Nespoli, P., Gomez Marmol, F., Maestre Vidal, J., 2021. **Battling against cyberattacks: towards pre-standardization of countermeasures**. Cluster Computing 24, 1-25. https://doi.org/10.1007/s10586-020-03198-9

Cyberattacks targeting ICT systems are becoming every day more sophisticated and disruptive. Such malevolent actions are performed by ill-motivated entities, often featuring almost unlimited resources, but also by skilled individuals due to the accessibility of the attacks source code. The paper at hand aims at contributing to the reaction ecosystem by proposing a standard representation of the countermeasure instances. With such a proposition, we address one of the critical challenges found in the literature, that is, the absence of a commonly-shared definition of remediations. To demonstrate the feasibility of our approach, we present several scenarios where some relevant countermeasures are efficiently enforced, resulting in mitigating the ongoing cyberthreat. Then, the advantages and disadvantages of our proposal are extensively discussed, opening the debate for novel and effective contributions in this research line.

Technical information - news

Enisa. **Artificial Intelligence Cybersecurity Challenges**. URL https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

This report presents the Agency's active mapping of the AI cybersecurity ecosystem and its Threat Landscape, realised with the support of the Ad-Hoc Working Group on Artificial Intelligence Cybersecurity. The ENISA AI Threat Landscape not only lays the foundation for upcoming cybersecurity policy initiatives and technical guidelines, but also stresses relevant challenges.

Europol. **DarkMarket: world’s largest illegal dark web marketplace taken down**. URL https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down

DarkMarket, the world's largest illegal marketplace on the dark web, has been taken offline in an international operation involving Germany, Australia, Denmark, Moldova, Ukraine, the United Kingdom (the National Crime Agency), and the USA (DEA, FBI, and IRS). Europol supported the takedown with specialist operational analysis and coordinated the cross-border collaborative effort of the countries involved.

Europol. 2021. **New major interventions to block encrypted communications of criminal networks.** URL https://www.europol.europa.eu/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks

Judicial and law enforcement authorities in Belgium, France and the Netherlands have in close cooperation enabled major interventions to block the further use of encrypted communications by large-scale organised crime groups (OCGs), with the support of Europol and Eurojust.

Lemnitzer, J., **Ransomware gangs are running riot – paying them off doesn’t help**. The Conversation. URL http://theconversation.com/ransomware-gangs-are-running-riot-paying-them-off-doesnt-help-155254

In the past five years, ransomware attacks have evolved from rare misfortunes into common and disruptive threats. Hijacking the IT systems of organisations and forcing them to pay a ransom in order to reclaim them, cybercriminals are freely extorting millions of pounds from companies – and they’re enjoying a remarkably low risk of arrest as they do it.

Parent, M., **Cyberattacks are on the rise amid work from home - how to protect your business. The Conversation**. URL http://theconversation.com/cyberattacks-are-on-the-rise-amid-work-from-home-how-to-protect-your-business-151268

This article deals with the subject of cyber-attacks. An increasingly true statement, Organisations are more vulnerable to cyber-attacks when employees work from home.

Security Magazine., **Cybercrime report finds young adults and adults over 75 most vulnerable to fraud attacks** URL https://www.securitymagazine.com/articles/94684-cybercrime-report-finds-young-adults-and-adults-over-75-most-vulnerable-to-fraud-attacks

LexisNexis Risk Solutions released its biannual Cybercrime Report covering July 2020 through December 2020, which details how the evolving threat landscape created new opportunities for cybercriminals around the world, particularly as they targeted new online users.

Terrorism

Scientific Information

Fu, L., Wang, X., Liu, B., Li, L., 2020. **Investigation into the role of human and organizational factors in security work against terrorism at large-scale events**. Safety Science 128, 104764. https://doi.org/10.1016/j.ssci.2020.104764

The pervasive human and organizational factors (HOFs) in security work at large-scale events (LSEs) contribute greatly to preventing terrorist attacks. This study contributes to the establishment of a systematic causation model for analyzing the root causes of the failure of security against terrorism at LSEs, which will enable more holistic incident investigation and more accurate formulation of precautions, as well as helping the development of risk analysis methods in the public security field.

Lissaris, E., Giataganas, G., Kavallieros, D., Myttas, D., Kermitsis, E., 2021. **Terrorist Activities in the Dark and the Surface Web**, in: Akhgar, B., Gercke, M., Vrochidis, S., Gibson, H. (Eds.), Dark Web Investigation, Security Informatics and Law Enforcement. Springer International Publishing, Cham, pp. 49-84. https://doi.org/10.1007/978-3-030-55343-2_3

This chapter presents terrorists' activities both at Surface Web and the Dark Web. Recently terrorists turned to the anonymity and secrecy that the Dark Web provides in order to stay undetected from law enforcement agencies. That way, their online activity cannot be controlled by any government, and they can easily and undisturbed plan their actions. In order to communicate, beyond the Dark Web, terrorists use end-to-end encrypted apps such as Telegram and WhatsApp. With these mobile apps, the communication and coordination of their actions are immediate and secret. Lastly, the Dark Web is precious for terrorist groups as all the funding of their operations, and in general significant part of their overall income, comes from Dark Web transactions using cryptocurrencies such as Bitcoin.

Technical information - news

Memetic Warfare, **the dark irony that may become terrorism**, 2021. Formiche.net. URL https://formiche.net/2021/02/memetic-warfare/

The strategic significance of the militarized use of memes lies in their ability to transform citizens into weapons of xenophobic, Islamophobic, anti-Semitic guerrillas, and more generally to instil hatred towards minorities. Social media is where most of the radicalisation happens at the global level, between information warfare and cyberwarfare. The first chapter of the research by Arije Antinori, Professor of Criminology and Sociology of Deviance at the Sapienza University in Rome.

Organised Crime

Scientific Information

Basu, K., Sen, A., 2021. **Identifying individuals associated with organized criminal networks: A social network analysis**. Social Networks 64, 42-54. https://doi.org/10.1016/j.socnet.2020.07.009

In this paper, we primarily focus on two types of networks – (i) Drug Trafficking Organizations, and (ii) Terrorist Organizations, and present a methodology for the surveillance of individuals associated with these networks. Our methodology is based on the mathematical notion of *Identifying Codes, which ensures reduction in resources on the part of law enforcement authorities, without compromising the ability to* uniquely identify *a suspect, when they become "active" in drug/terror related activities. Furthermore, we show that our approach requires far lesser resources when compared to strategies adopting standard network centrality measures for the unique identification of individuals.*

Rebovich, D., 2021. **The Changing Face of Financial Crime: New Technologies, New Offenders, New Victims, and New Strategies for Prevention and Control**. Victims & Offenders 16, 283-285. https://doi.org/10.1080/15564886.2021.1876196

Financial crime is a growing crime problem throughout the world. It is a trillion-dollar industry that takes an enormous social and economic toll on the lives it touches. The primary goal of this special issue was to explore the many dimensions of financial crime from the perspectives of victims (both individual and organizational) and offenders.

Technical information - news

Euronews, **Organised crime setting sights on EU Recovery Fund money, experts warn**, 2020. euronews. URL https://www.euronews.com/2020/09/18/corona-mafia-organised-crime-setting-sights-on-eu-recovery-fund-experts-warn

Corona-mafia? Organised crime setting sights on EU Recovery Fund, experts warn. Very interesting video of Executive Director at Transparency International Italy Davide Del Monte.

Migration

Scientific Information

Binder, S., Iannone, A., Leibner, C., 2020. **Biometric technology in "no-gate border crossing solutions" under consideration of privacy, ethical, regulatory and social acceptance. Multimed Tools Appl 1-14.** https://doi.org/10.1007/s11042-020-10266-0

Biometric technologies have become the main focus in the design of state-of-the-art border security solutions. While respective research in the field of multimedia vision has been centred around improving quality and accuracy of identity recognition, the impact of such technologies upon society and legal regulations still remains a topic unaddressed, specifically within the engineering community. Building on participation in the EU funded research project PERSONA, authors of this *paper look at the challenges associated with biometrics-based solutions in no-gate border crossing point scenarios. technology due to fraudulent activities.*

Bove, V., Böhmelt, T., Nussio, E., 2021. Terrorism abroad and migration policies at home. Journal of European Public Policy 28, 190-207. https://doi.org/10.1080/13501763.2020.1729227

Do security concerns lead to more restrictive immigration policies? In this article, we contend that transnational influences can shape legislative output on immigration at home. Terrorist attacks in a neighboring country affect the salience of security concerns in the focal state, the policy solutions for addressing them, and the political will to implement these changes. Using data on 33 OECD countries, we find that proximity to targeted countries leads to the implementation of a more restrictive migration policy regime. The public's common perception of a linkage between migration and terrorism thus has important policy consequences.

Chamie, J., 2020. International Migration amid a World in Crisis. Journal on Migration and Human Security 8, 230-245. https://doi.org/10.1177/2331502420948796

This article comprehensively examines international migration trends and policies in light of the coronavirus disease 2019 (COVID-19) pandemic. It begins by reviewing migration developments throughout the past 60 years. It then examines pandemic-related migration trends and policies. It concludes with a series of general observations and insights that should guide local, national, regional, and international policymakers, moving forward.

RESEARCHER'S TOOLBOX:

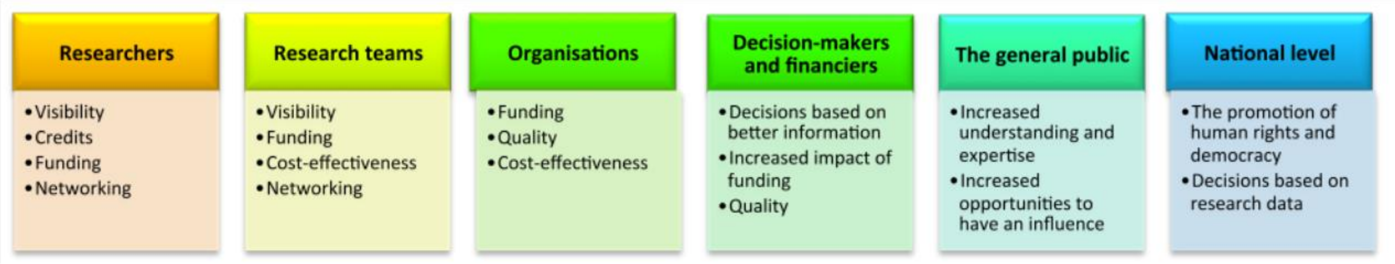
« THE CHALLENGES OF OPEN SCIENCE FOR RESEARCH »

What does "open science" mean?

Open Science represents a new approach to the scientific process based on cooperative work and new ways of diffusing knowledge by using digital technologies and new collaborative tools. The idea captures a change to the way science and research have been carried out for the last fifty years: **shifting** from the standard practices of publishing research results in **scientific publications towards sharing and using all available knowledge at an earlier stage in the research process**.[1]

What are the benefits of open science?

Find below a summary of the benefits of open science for the different parties[2]:



Researchers	Research teams	Organisations	Decision-makers and financiers	The general public	National level
• Visibility • Credits • Funding • Networking	• Visibility • Funding • Cost-effectiveness • Networking	• Funding • Quality • Cost-effectiveness	• Decisions based on better information • Increased impact of funding • Quality	• Increased understanding and expertise • Increased opportunities to have an influence	• The promotion of human rights and democracy • Decisions based on research data

[1] Source: https://www.openscience.nl/en/open-science/what-is-open-science

[2] Source: https://www.fosteropenscience.eu/content/what-are-benefits-open-science

What is the difference between Open Science and Open Access?

Open Access (OA) is the terminology used for the practice of making peer-reviewed scholarly research and literature (published journal articles, book chapters, monographs, research data…) freely available in online repositories to anyone interested in reading it. Contrary to Open Access, Open Science (or Open Research) is a much broader term which is the **conduction and dissemination of research in a more transparent and collaborative way**. In many ways, Open Science is no different to traditional science with research data and lab notes at various stages of research cycle being made freely available as early as possible. So Open Science includes Open Access to content and information but also could encompass things like scholarly communication networks, citizen science projects, open lab notebooks and open source software[3].

Are there many open archives?

More and more universities and research centres have their own open archives, starting with world-renowned universities such as Harvard with DASH (Digital Access to Scholarship at Harvard). In general, open archives are either institutional or thematic, for example arXiv for Physics and Maths. Some open archives are not limited to articles and may also include theses, dissertations, books, teaching materials, audio and video files, among others. The number of open archives is steadily increasing, with two major global directories, ROAR (Registry of Open Access Repositories) and OpenDOAR (Directory of Open Access Repositories), to help you find your way.

What about the European Commission?

Open science is a policy priority for the European Commission and the standard method of working under its research and innovation funding programmes as it improves the quality, efficiency and responsiveness of research.[4] So let's discover one of the last initiatives of the European Commission…

The new Open Research Europe (ORE) platform – funded by the European Commission

ORE is a new, **free, open access, peer-review publishing platform for the publication of results stemming from EU-funded research**. It publishes articles categorised in six subject areas: Natural Sciences, Engineering and Technology, Medical Sciences, Agricultural Sciences, Social Sciences, Humanities and Arts.

The new platform will make it easy for **Horizon 2020 beneficiaries** to comply with the EU Open Access terms of funding **at no cost** to them. It offers to the researchers a free publishing venue to **share their results and insights rapidly** and **facilitate open and constructive research discussions**. Even if the EU-funded project has ended, publications stemming from the project can be submitted. Each publication must have at least one author who has been, or still is, a recipient of an EU grant.

[3] Source : www.mysciencework.com/omniscience/open-science-open-access-far-apart

[4] Source : https://ec.europa.eu/info/research-and-innovation/strategy/goals-research-and-innovation-policy/open-science_en

The ORE website currently contains all necessary guidance (policies, publishing process, Scientific Advisory Board and FAQ) as well as information and instructions for the submission workflow. **The platform is now open for submissions** but the full range of functionalities (search, grouping per areas and thematic gateways) will become active only at the time of the formal launch, in March 2021.[5]

More information: https://open-research-europe.ec.europa.eu/

CONTACT

ENSP
ÉCOLE NATIONALE
SUPÉRIEURE DE LA POLICE
CENTRE DE RECHERCHE

You wish to publish? You are a researcher and would like to share your profile? You would like to have information about the ILEAnet project and the scientific coordination? Do not hesitate to contact us.

Virginie SOLDAT virginie.soldat@interieur.gouv.fr
Scientific Coordination ensp-ileanet@interieur.gouv.fr

[5] Source : https://ec.europa.eu/programmes/horizon2020/en/news/new-open-research-europe-ore-platform-has-opened-its-wings