Who we are

Defence Research Institute is a French SME based in Paris with strong networks across European LEAs and MoDs.

DRI is a research think tank with a multidisciplinary approach that combines an expertise on technology with a strong focus on defence, strategic and security issues.

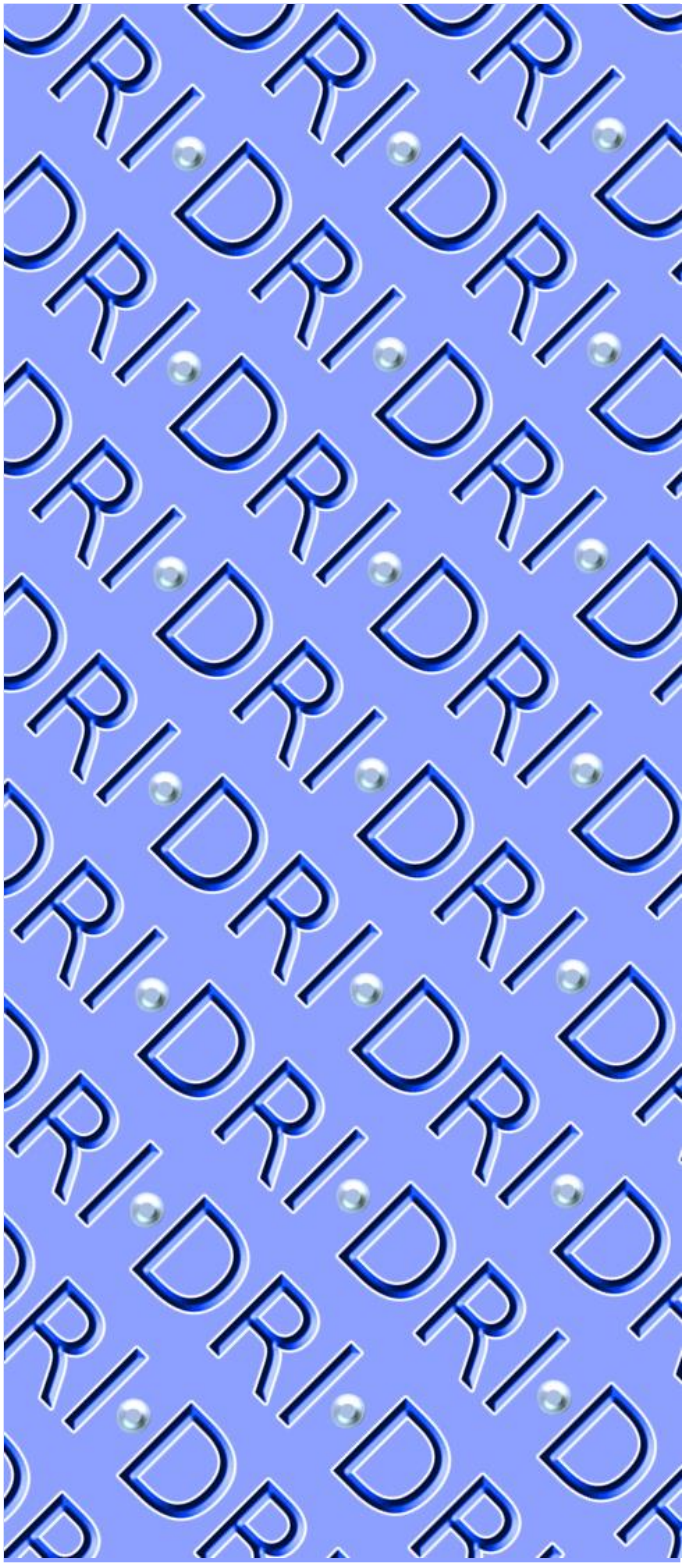
DRI is composed by personnel who has strong and different backgrounds and has participated in projects at the international level connected to terrorism prevention, counter-narrative against radicalization, prevention, investigation and mitigation of cyber criminality. Our professional are OSCE and GENERALI executives as well as former UN agencies officers

DRI's areas of research range many fields of competence as International Relations, Geopolitics and Geostrategy issues, IT, Cybersecurity and Cyber Defence.

Key Personnel

Pier Giuseppe CASUCCINI BONCI holds a Master Degree in Economics with a specialisation in Econometrics as part of project supported by the European Community.
After a period as manager responsible of Data Management and International Relations in A.BIOTEC (Italy), he joined IBM (Italy) where he worked as System Engineer and Sales Representative for Financial Markets.

After leaving IBM, since 1993 he has been working with Companies of Generali Group, first in Italy, at the Trieste Head Office, then in French Subsidiaries. He covered the roles of IT, Support and Security Functions Manager, Chief Data Privacy Officer, Compliance and Security Manager. He is fluent in Italian, French, Russian and English.



DRI

Defence Research Institute

24 Rue Erlanger, 75016
Paris (France)

info@defenceresearchinstitute.eu

www.defenceresearchinstitute.eu/

Our expertise

Artificial Intelligence for Defence

Systems that are able to learn from experience, perform cognitive analysis and much more. Artificial intelligence is a game-changer in Defence, radically changing military operations and practices.

Cybersecurity

The enormous expansion of the Internet occurred recently has not been matched by adequate improvements in terms of cyber-security. Most of our devices are now interconnected and vulnerable to cyber-attacks. We focus on researching risk assessment and mitigation strategies for the Critical Infrastructure Protection.
.

Cyber warfare

What is the real measure of the cyber war threat? What will be the next cyber-weapons, and the defence strategies? While our critical infrastructures are more dependent than ever on Information Communication technologies, are they ready for a cyber war?

Forecast and foresight

What will be the breakthrough technologies of the next years? Which areas will see the most radical changes? We research on methodologies for defence and security technology forecasting exploiting Big Data Analytics and Predictive Algorithms

Research projects

NEMO

EDF

Call: EDF-2023-LS-RA-CHALLENGE-DIGIT-HLTP

The project will build a human language technology (HLT) demonstrator for Defence, usable by military personnel and users without any developer intervention. The project will rely on sophisticated AI methods based on machine learning (ML), deep learning (DL), and large language models (LLMs) industrialised by a multinational consortium. The demonstrators will be evaluated in a series of technological challenges.

Acting

Advanced Cybersecurity Training

EDF

Call: EDF-2021-CYBER-D

The (ACTING) project will develop a network of advanced, interconnected (federated) domain-oriented gaming cyberspaces for training and exercises. It aims to integrate sophisticated methods and techniques for user simulation, and cybersecurity situational awareness assessment.

NOTIONES

H2020

Call: SU-GM01-2020

The project's objective is to create a network of practitioners from the security and intelligence services of EU Member States and associated countries, industry and academia, to identify how emerging technologies can meet the needs of security services.

DECISMAR

Maritime Surveillance Decision Support Toolbox

EDIDP

Call: EDIDP-SME-2019

The objective of the DECISMAR project is to develop a Decision Support Toolkit (DSTx) to provide future technology scenarios and conduct feasibility studies to support the upgrading of maritime surveillance as part of the requirements current and future high-level operational activities defined by PESCO "Upgrading maritime surveillance" project.

Q-ARM

EDF

Call: ---

The Q-ARM (Quantum Agile Resilient Military communications) project will provide crypto-agile, decentralised and quantum secure identity management for defence and critical infrastructure environments.