R1.6 ANNEX 4 – Set of Fiches of 2023

Dissemination level: PU (public) ~~/ **RE** (restricted) / **CO** (confidential)~~

Co-funded by the Erasmus+ Programme of the European Union

The European Commission's support for the production of this document does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications

Description	In addition to cutting edge research paper presentations in human-computer interaction, optimization and robotics areas, the congress serves as a multi-disciplinary platform for discussing current issues in the engineering areas.
Goal	The congress aims to bring scientists, experts, instructors, non-govermental organizations and private sector representatives together to share and discuss theoretical and practical knowledge in a scientific framework.
Organizer	National Technical University “Kharkiv Polytechnic Institute” and Tokat Gaziosmanpasa University
Co-organizers/ Patrons	
Topics	• Human-Computer Interaction • Machine Learning • Intelligent Control Systems and Optimization • Robotics, Mechatronics and Automation • Signal Processing • Data Mining
Date	June 8-10, 2023
Costs	€ 350 - € 500
www	https://www.horacongress.com/index.php

Nr 378/2022

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

5th International Conference on Industry 4.0 and Smart Manufacturing (ISM 2023)

Description	The International Conference on Industry 4.0 and Smart Manufacturing (ISM) is a yearly open forum fostering the smart culture and exploring the transformative impact of digital technologies characterizing the 4th industrial revolution across the full breadth of economic sectors.
Goal	The 2023 International Conference on Industry 4.0 and Smart Manufacturing (ISM) represents a new platform for knowledge exchange, the review and discussion of theoretical advances, research results, and industrial experiences, among scientists, researchers, decision makers, practitioners and students dealing with the topics under the umbrella of Industry 4.0 and Smart Manufacturing.
Organizer	
Co-organizers/ Patrons	
Topics	• Additive Manufacturing • Autonomous production • Big Data Analytics in Manufacturing and Logistics • Cloud Computing • Cyber Physical Production Systems • Cyber Security • Digital Twins • Industrial Engineering Education 4.0 • Human-Machine Interaction • Industrial Internet of Things • Maintenance and Lifecycle Management • Manufacturing Technologies • Production Systems and Supply Network Engineering • Quality Management & Assurance • Robotics in Industry • Simulation in Production and Logistics • Smart Operators and Human-centric Systems • Sustainability-oriented production
Date	November 22-24, 2023
Costs	395 EUR - 495 EUR
www	https://www.msc-les.org/ism2023/

Nr 379/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

International Experts Summit on Artificial Intelligence and Robotic Technology (IESAIRT2023)

Description	IESAIRT2023 provides a platform of international standards where you can discuss and share knowledge on Artificial Intelligence and Robotic Technology to bring a unique forum for exchanging the information regarding the latest developments, finding solutions and enriching the knowledge. In addition to Presentations, Workshops, and Discussions, the conference also offers a unique venue for renewing professional relationships, and providing plenty of networking opportunities during the summit.
Goal	
Organizer	Meghaz Meetings
Co-organizers/ Patrons	
Topics	• Machine learning • Cognitive Intelligence • Intelligent interactive technology • Human-robot interaction • Human-machine interface/integration • Teleoperation/ telerobotics/ haptics • Behavioral Intelligence • Neuroscience based control • Genetic Intelligence • Artificial Intelligence • Computational intelligence • Nanorobots • Environmental interaction and navigation • Intelligent Mechatronics and Robotics • Frontiers in Robotics and AI • Robotic Mapping • Autonomous Robot • Cognitive Robotics • Soft Robotics and Mobile Robot • And more
Date	September 07-09, 2023
Costs	$ 939 - $ 389
www	https://www.meghazmeetings.com/iesairt-2023/

Nr 380/2023

Fiche develop in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

High Studies for Security and Defence (HSSD)

Description	The HSSD are intended for senior officers or civilians employed by Belgian Defence, as well as senior managers or civilian officials whose professional activity has an explicit link with security or defence, working for different public services or international institutions, in civil society, with an economic, industrial, political or academic background, etc. The selection of candidates is a prerogative of the Minister of Defence, which decides on a proposal from the HSSD's steering committe for candidates outside Defence, or from the Chief of Defence for candidates from Defence. All participants should have the Belgian nationality.
Organizer	Royal Higher Institute for Defence
Cooperation with	Royal Institute for International Relations – Egmont
Duration	10 monthly residential seminars of two days, each focussing on a specific issue +10 visits to Belgian institutions active in the field of security and defence
Thematic Scope	
Costs	1950 €
No of ECTS credits	
E-learning	No
Tools	
Job opportunities	
Additional info	
www	https://www.defence-institute.be/en/high-studies/

Nr 381/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

Multi-year Defence Science and Technology Research Programme

Financing entity	Royal Higher Institute for Defence
Managing entity	Royal Higher Institute for Defence
Programme	Multi-year Defence Science and Technology Research Programme
Type of action	**Research action**
Call	
Objectives of the call	The backbone of research conducted at Defence is the multi-year Defence Science and Technology Research Programme. Currently, this programme is entirely funded by Defence and is primarily directed to Defence research institutions. Nevertheless, collaborations with external partners are encouraged. The projects making up the programme are selected each year following a call for projects, internal to Defence. They are subject to various evaluations, notably on their scientific merit (carried out by high-level external scientific experts) and their appropriateness (interest for Defence, but also the collaborative nature and the potential at the societal and economic level). After approval by the RHID's Scientific Committee and Board of Directors, it is submitted to the Minister of Defense and the Council of Ministers for approval. The current program consists of 120 studies.
Who can apply?	
How to apply?	
Duration	
Deadline	
Maximum amount/ Call budget	
www	https://www.defence-institute.be/en/about-us/strd/research-programme/

Nr 382/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Neural Computing and Applications

Description	Neural Computing & Applications is an international journal which publishes original research and other information in the field of practical applications of neural computing and related techniques such as genetic algorithms, fuzzy logic and neuro-fuzzy systems.
Goal / Target audience	This journal provides an international forum for publication original research and other information in practical applications of neural computing and related techniques.
Publisher	Springer London
Topics/ Content	All items relevant to building practical systems are within its scope, including but not limited to: adaptive computing, algorithms, applicable neural networks theory, applied statistics, architectures, artificial intelligence, benchmarks, case histories of innovative applications, fuzzy logic, genetic algorithms,hardware implementations, hybrid intelligent systems, intelligent agents, intelligent control systems, intelligent diagnostics, intelligent forecasting, machine learning, neural networks, neuro-fuzzy systems, pattern recognition, performance measures, self-learning systems, software simulations, supervised and unsupervised learning methods, system engineering and integration
ISSN	09410643, 14333058
www	https://www.springer.com/journal/521

Nr 583/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Intelligent Systems with Applications

Description	Intelligent Systems with Applications (ISWA) is a peer reviewed open-access journal which focuses on the achievements of research and applications related to intelligent systems (IS).
Goal / Target audience	The journal audience comprises academia, industry, and practitioners.
Publisher	Elsevier BV
Topics/ Content	The journal aims to publish papers dealing with, but not limited to, the following research fields: • Knowledge Representation and Reasoning, • Machine Learning (ML) and Neural Computing, E • volutionary Computation, • Fuzzy Systems, • Intelligent Information Processing, • Intelligent Control and Robotics, • Multi-agent Systems and Programming. The journal welcomes submissions of IS-applications in various areas: Intelligent Cities, Industries, Consuming, Medical Treatment and Health, Agriculture, Business and Finance, Internet of Things (IoT). Research addressing IS-applications in other fields is also encouraged.
ISSN	26673053
www	https://www.sciencedirect.com/journal/intelligent-systems-with-applications

Nr 584/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

International Conference on Advanced Research in Technologies, Information, Innovation and Sustainability (ARTIIS 2023)

Description	ARTIIS, is an international forum for researchers and practitioners to present and discuss the most recent innovations, trends, results, experiences, and concerns in the area of Information Systems (IS), focusing on four topics: computing solutions, data intelligence, sustainability, Ethics, Security, and Privacy; with some particularities being addressed within each of them. IS encompasses the use of technology and data to support various organizational and societal functions. The topics are closely related to the field of IS because all of them involve the use and management of technology and data to achieve specific purposes or goals.
Goal	
Organizer	
Co-organizers/ Patrons	
Topics	• Computing Solutions (Applied Information Systems (e. g. Healthcare, Law, Economics, Education), Web and Mobile Applications, Networks, Mobility, Ubiquity and Pervasive Systems, Innovative Computing, Gamification Application and Technologies, Software Engineering) • Data Intelligence (Advanced Computational Intelligence, Computer Vision and Image Processing, Artificial Intelligence and Data Science, Data Engineering, Analytics, and Applications, Intelligent and Decision Support Systems, Information and Knowledge Management) • Sustainability (Immersive Tech and the Future of Smart Cities, Industrial Advanced Internet of Things, Internet of Things Environment, Sustainable Infrastructure Development, Technology, Marketing and Socio-economic challenges) • Ethics, Security, and Privacy (Information and Telecommunication Systems Security, Innovative Communication Networks and Security, Vulnerabilities of Interoperability and Information system, Interdisciplinary Information Studies, Ethics of Social Sciences for Computer Applications)
Date	October 18-20, 2023
Costs	
www	https://www.artiis.org/

Nr 385/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

Evening conferences of the Royal Higher Institute for Defence – Belgium, Europe and Strategic Autonomy in Space

Description	The guests of the conference will be Mr Thomas Dermine, state secretary for Economic Recovery and Strategic Investments, in charge of Science Policy, Dr Octávia Portugal Frota, consultant on aerospace, security and defence matters for the EU, NATO and the European Defence Agency (EDA) as well as Air Force Major Nicolas Gérôme, head of the Space office within the Belgian Defence's Strategy department, who will share their analyses on the European space sector and Belgium's position in this field.
Goal	
Organizer	Royal Higher Institute for Defence
Co-organizers/ Patrons	
Topics	• In the context of Russia's invasion of Ukraine and the fierce competition in the launch market, how can the EU ensure its strategic autonomy in the space sector? • What is Belgium's position in this respect within the European Union in general, and in the scientific and industrial fabric in particular? • What are the major challenges of the militarisation of space and the role of the Belgian Defence in space security at national and international level?
Date	February 16, 2023
Costs	
www	https://www.defence-institute.be/en/events/conference-2023-02-16/

Nr 386/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

Evening conferences of the Royal Higher Institute for Defence – Why does Belgium need a Cyber Command?

Description	The guests of the conference will be Major General Michel Van Strythem, commander of the Cyber Command, and Professor Dr Alexander Mattelaer (VUB and Egmont Institute), who will share their analyses on the cyber command's missions as well as on current and future challenges for its implementation.
Goal	
Organizer	Royal Higher Institute for Defence
Co-organizers/ Patrons	
Topics	• Why is it important for Belgium to develop a Cyber Command? • What are the structural and organisational characteristics of this new staff? • What are the current and future challenges for its implementation? • What role does the Cyber Command play in the national and international ecosystem?
Date	March 2, 2023
Costs	
www	https://www.defence-institute.be/en/events/conference-2023-03-02/

Nr 387/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

Master's Degree in Senior management in international security

Description	The Master's Degree in Senior Management in International Security taught by the CUGC is an official title of 60 ECTS , which meets the quality requirements of the European Higher Education Area (EEES) that arises from the Bologna Declaration and is officially recognized in the 49 EHEA states.
Organizer	Carlos III University of Madrid (UC3M)
Cooperation with	
Duration	1 year
Thematic Scope	• MODULE I: ESTRATEGIC ANALYSIS ON INTERNATIONAL SECURITY: Geopolitics and International Security, Security policies and strategies, Public security sectoral • MODULE II: THE CHALLENGES OF THE MAIN SECURITY THREATS FROM A GLOBAL PERSPECTIVE: Global risks and threats, Organized crime and cybercrime, Corruption and police ethics • MODULE III: PUBLIC AND PRIVATE SECURITY IN THE INTERNATIONAL CONTEXT: Corporate security strategies, Technologies and innovation applied to security, Strategic management on human resources • MODULE IV: ACADEMIC RESEARCH AND PRACTICES: Command and Strategic Control Practices, Master's Thesis
Costs	
No of ECTS credits	60 ECTS
E-learning	Blended Modality - it is carried out along the year course (from December to September) through an advanced academic programme which contains three modules remotely, using the CUGC virtual classroom with three weeks of on-site activities in each module.
Tools	
Job opportunities	
Additional info	Final Recipients: Members of Law Enforcement Agencies from Latin America, Europe and Maghreb, Senior Police Officers of the Guardia Civil and professionals of other groups related to security (Judges, Prosecutors, Armed Forces, diplomats, private security directors, etc).
www	https://www.cugc.es/estudios-postgrados/postgrados/masters/master-universitario-madsi/presentacion-del-master-madsi.html

Nr 388/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

Master's Degree in Operational Security Management

Description	Master's Degree in Security Operations Management is an official university master's degree of 60 ECTS developed in the field of legal and social sciences, which can be taken by Civil Guard students who have completed the University Degree in Security Engineering (240 ECTS). However, it may be open to other national security professionals and from other countries who meet the necessary requirements.
Organizer	Carlos III University of Madrid (UC3M)
Cooperation with	
Duration	1 year
Thematic Scope	
Costs	
No of ECTS credits	60 ECTS
E-learning	No
Tools	
Job opportunities	
Additional info	
www	https://www.cugc.es/estudios-postgrados/postgrados/masters/master-direccion-operativa-de-la-seguridad-mdos/presentacion-del-master-mdos.html

Nr 389/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Unmanned Ground Systems (CUGS)

Description	Combat Unmanned Ground Systems (CUGS), was launched to develop highly autonomous combat unmanned ground systems and it's brings together nine member states and 28 European industry partners.
Goal	The project aims to choose and adapt 3 different categories of platforms, and to define, design and develop a set of functional modules which will be articulated in full demonstrators for highly autonomous combat unmanned ground systems. The platforms and functional modules will provide solutions for: • Navigation, • Communications, command and control (C3), and cooperation (including secure C3 for firing chain), • Effector management. The project will be constituted by the following three phases: • Phase 1: requirements and standard-based system architecture of the full CUGS demonstrator. • Phase 2: adaptation of platforms and development of combat functional modules, in parallel. • Phase 3: integration of all the functional modules and associated intelligent functions into the platforms to demonstrate combat abilities on operational scenarios.
Lead Partner	Leonardo (Italy)
Partners involved	Iveco, Larimart and MBDA IT (Italy), John Cockerill Defence, FN Herstal and the Royal Military Academy of Belgium (Belgium), Diehl Defence, KMW, MBDA DE and Rheinmetall (Germany), Milrem Robotics, Estonia and the Estonian Military Academy (Estonia), Patria and Bittium (Finland), Nexter, Safran, Thales, MBDA FR and Arquus (France), TNO, Demcon and NCIM (Netherlands), Kongsberg and FFI (Norway), WAT, PIAP, ZMT and ASW (Poland)
Duration	36 months (2022-2024)
Results	
Funding	European Defence Agency (EDA), co-funded by Member States
www	https://eda.europa.eu/news-and-events/news/2023/02/03/new-eda-project-seeks-to-enhance-combat-unmanned-ground-systems-technology

Nr 390/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference, **Fair**, Exhibition	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

International Defence and Security Exhibition FEINDEF

Description	The international Defence and Security Exhibition FEINDEF, organized by the FEINDEF Foundation, is the only exhibition in Spain from this sector with the institutional support of the Ministry of Defence, and it is positioned as the most important event held in Spain in this sector, that opens to the world by offering network opportunities: 40.000 m2 of exhibition space, with an attendance of over 450 exhibitors from 20 countries and 100 foreign delegations.
Goal	FEINDEF is the reference forum that encompasses the defence and security sector in Spain, to innovate, coopera-te internationally and share knowledge between companies, institutions, universities, and other organisms, as a global response to security.
Organizer	FEINDEF Foundation
Co-organizers/ Patrons	
Topics	• Technology: C41 arms and munitions, Cyberdefence / Cybersecurity consulting and engineering, PPE, Space, Infrastructures, Fold-out infrastructures, IoT, Big Data, AI, Logistics, Maintenance and life cycle, CBRNE, Air, naval and land RPA systems and aircraft, Robotics, Electronic sensors and system services, Simulation, Information technologies • Dual-use: Simulation and artificial intelligence, Generation of energy and water, Waste management, Drones, Semi-permanent buildings and quality of life, Cyberdefence
Date	May 17 – 19, 2023
Costs	
www	https://www.feindef.com/index.php/en/

Nr 391/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Elevating Women in Cyber

Description	During the event the UK Cyber Security Council will be joined by inspirational speakers, partners, members, funders, and a collection of special guests. The event will host a workshop on how to bridge the skills and gender gap in the cyber world.
Goal	The event will provide an opportunity for professionals, organisations, stakeholders, and partners to collaborate to address the barriers faced by women when looking to enter the field and offer a platform to those already paving the way for the next generation of women in cyber.
Organizer	UK Cyber Security Council
Co-organizers/ Patrons	
Topics	• Learning about emerging pathways for the new generation of talent • Driving the conversation and steering the Council's future outreach work during the workshops • Networking with peers in the sector and making new connections
Date	March 8, 2023
Costs	General Admission - free
www	https://www.ukcybersecuritycouncil.org.uk/events/elevating-women-in-cyber/

Nr 392/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

18th Conference on Computer Science and Intelligence Systems FedCSIS 2023

Description	FedCSIS is an annual international conference, this year organized jointly by the Polish Information Processing Society (PTI), IEEE Poland Section Computer Society Chapter, and Department of Mathematics and Information Sciences, Warsaw University of Technology. It is technically sponsored by a number of IEEE units and other professional organizations.
Goal	The goal of the Conference is to provide a presentation, discussion and a reputable publication forum in computer science and intelligence systems.
Organizer	Polish Information Processing Society, IEEE Poland Section Computer Society Chapter, Department of Mathematics and Information Sciences (Warsaw University of Technology)
Co-organizers/ Patrons	
Topics	• Advanced Artificial Intelligence in Applications (AI in Agriculture, Challenges for Natural Language Processing, Distributed Edge AI – Risks and Challenges, Rough Sets: Theory and Applications, Computational Optimization) • Computer Science & Systems (Computer Aspects of Numerical Algorithms, Multimedia Applications and Processing, Scalable Computing) • Network Systems and Applications (Complex Networks – Theory and Application, Internet of Things – Enablers, Challenges and Applications, Cyber Security, Privacy and Trust) • Information Technology for Business and Society (International Workshop on AI in Digital Humanities, Computational Social Sciences and Economics Research, Data Science in Health, Ecology and Commerce, Information Systems Management, Knowledge Acquisition and Management, Meta Environment for Citizens, Business and Entertainment) • Software, System and Service Engineering (Cyber‑Physical Systems, Practical Aspects of and Solutions for Software Engineering, Software Engineering, Advances in Programming Languages)
Date	September 17–20, 2023
Costs	Early registration (payment before August 15, 2023) • Regular fee: 600€ / $650 • IEEE and PTI member fee: 550€ / $585 • Student fee: 450€ / $480 • Accompanying person fee (paper publication NOT included): 500€ / $550
www	https://fedcsis.org/

Nr 393/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

10th International Conference on Human Interaction and Emerging Technologies IHIET 2023

Description	IHIET Conference will focus on advancing the theory and applications for human-interaction requirements as part of an overall system and product solution, by adopting a human-centered design approach that utilizes and expands on the current knowledge of user-centered design and systems engineering supported by cognitive software and engineering, data analytics, simulation and modeling, and next generation visualizations.
Goal	IHIET Conference aims to provide a global forum for presenting and discussing novel human-interaction, healthcare, sport medicine and engineering approaches, tools, methodologies, techniques, and solutions for integrating people, concepts, trends and applications in healthcare and artificial intelligence all areas of human interaction endeavor in industry, economy, government, and education, including but not limited to energy, transportation, urbanization and infrastructure development, digital manufacturing, social development, human health, sustainability, new generation of service systems, as well as safety, risk assessment, healthcare, and cybersecurity in both civilian and military contexts.
Organizer	
Co-organizers/ Patrons	
Topics	• Human-centered Design • Artificial Intelligence, Computing and Intelligent Design • Augmented, Virtual and Mixed Reality Simulation • Wearable Technologies, Social and Affective Computing • Human–computer Interaction • Human-Technology and Future of Work • Emerging Technologies and Business Applications • Applications in Medicine and Healthcare • Management, Training and Business Applications
Date	August 22-24, 2023
Costs	Early Bird (before 25 March 2023): • discounted fee: $695 • regular fee: $795 • half day tutorial: $255
www	http://ihiet.org/

Nr 394/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-IA HORIZON Innovation Actions
Call	Increased Cybersecurity 2023 (HORIZON-CL3-2023-CS-01)
Objectives of the call	Projects' results are expected to contribute to some or all of the following outcomes: • Tools to support cybersecurity resilience, preparedness, awareness, and detection within critical infrastructures and across supply chains; • Cloud infrastructures vulnerabilities mitigation; • Secure integration of untrusted IoT in trusted environments; • Use of Zero-Trust architectures; • Trust & Security for massive connected IoT ecosystems & lifecycle management; • Secure interoperability and integration of systems; • AI-based automation tools for cyber threat intelligence; • Secure infrastructure, secure Identities and usability for a security chain covering communication, data collection, data transport, and data processing.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations (including international European research organisations) is eligible to participate (whether it is eligible for funding or not), provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	23 November 2023
Maximum amount/ Call budget	Call budget: EUR 20 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2023-cs-01-01

Nr 395/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Collaborative intelligence – combining the best of machine and human (AI Data and Robotics Partnership) (RIA)

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-RIA HORIZON Research and Innovation Actions
Call	A human-centred and ethical development of digital and industrial technologies (HORIZON-CL4-2024-HUMAN-01)
Objectives of the call	Projects are expected to contribute to the following outcomes: • Demonstrate the value of human-machine collaboration and interaction by improved effectiveness, intuitiveness, efficiency, completeness, limits of knowledge indication and other objective or quantifiable subjective measures. • Demonstrate how collaborative decision-making improves over human decision-making and that the collaborative decisions cover all stages of reasoning (that they are based on an improved coverage of data and knowledge sources, on an improved analytic ability to reason from input to output, and on a well-communicated decision).
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations (including international European research organisations) is eligible to participate (whether it is eligible for funding or not), provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	19 March 2024
Maximum amount/ Call budget	Call budget: EUR 20 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl4-2024-human-01-07

Nr 396/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Novel paradigms and approaches, towards AI-powered robots – step change in functionality (AI, data and robotics partnership) (RIA)

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-RIA HORIZON Research and Innovation Actions
Call	Digital and emerging technologies for competitiveness and fit for the Green Deal (HORIZON-CL4-2024-DIGITAL-EMERGING-01)
Objectives of the call	Projects are expected to contribute to all of the following primary outcomes: • Achieve the substantial next step in the ability of robots to perform non-repetitive functional tasks in realistic settings, based on underlying robot functions, demonstrated in key high impact sectors where robotics has the potential to deliver significant economic and/or societal benefits. • Step change in the enabling conditions essential for the accelerated diffusion of robots in various industries, sectors and services which can handle tasks efficiently, robustly, and safely and interact naturally and smoothly to support humans in their daily activities, based on a strong multidisciplinary approach, including the relevant SSH dimension. • The development, use and exploitation of major advances in science and technology for the enhancement of European robotics.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate (whether it is eligible for funding or not), provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	19 March 2024
Maximum amount/ Call budget	Call budget: EUR 30 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl4-2024-digital-emerging-01-03

Nr 397/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Robotics: Autonomous or semi-autonomous UGV systems to supplement skills for use in hazardous environments

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-RIA HORIZON Research and Innovation Actions
Call	Disaster-Resilient Society 2023 (HORIZON-CL3-2023-DRS-01)
Objectives of the call	Projects' results are expected to contribute to some or all of the following outcomes: • Broad acceptance of autonomous systems by first responders and affected people in civil protection; • Higher safety and security standards for operational forces working in hazardous environments; • Get ahead of future shortcomings of trained first responder personnel by increasing first responder efficiency; • Increased ability to conduct on-scene operations remotely without endangering first responders; • European robotics industry is strengthened through engagement in the civil protection research as well as an economic and political advantage through building up know-how for innovative technologies; • Reduction of false positive redouts from various sensors carried by robots.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate (whether it is eligible for funding or not), provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	23 November 2023
Maximum amount/ Call budget	Call budget: EUR 6 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2023-drs-01-04

Nr 398/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Enhancing tools and capabilities to fight advanced forms of cyber threats and cyber-dependent crimes

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-RIA HORIZON Research and Innovation Actions
Call	Fighting Crime and Terrorism 2023 (HORIZON-CL3-2023-FCT-01)
Objectives of the call	Projects' results are expected to contribute to some or all of the following outcomes: • Development of modular toolbox for Police Authorities, facilitating gathering and processing of data relevant for cybercrime and cyber; • Detection of crypto-jacking, compromised registration forms, malware attacks and other cybercrimes perpetrated using cryptocurrencies; • Development of training curricula, for Police Authorities, prosecutors, as well as judicial actors on major contemporary cybercriminal activities; • Recommendations on public cybercrime awareness actions contributing to early detection and prevention; • Identification of best practices of international law enforcement and judicial cooperation networks; • Development of multi-stakeholders strategies, including novel investigation schemes and information sharing mechanisms.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate (whether it is eligible for funding or not), provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	23 November 2023
Maximum amount/ Call budget	Call budget: EUR 8 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2023-fct-01-06

Nr 399/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Explainable and Robust AI (AI Data and Robotics Partnership) (RIA)

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-RIA HORIZON Research and Innovation Actions
Call	A human-centred and ethical development of digital and industrial technologies (HORIZON-CL4-2024-HUMAN-01)
Objectives of the call	Projects are expected to contribute to one of the following outcomes: • Enhanced robustness, performance and reliability of AI systems, including awareness of the limits of operational robustness of the system; • Improved explainability and accountability, transparency and autonomy of AI systems, including awareness of the working conditions of the system.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations (including international European research organisations) is eligible to participate (whether it is eligible for funding or not), provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	19 March 2024
Maximum amount/ Call budget	Call budget: EUR 30 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl4-2024-human-01-06

Nr 400/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Security of robust AI systems

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-RIA HORIZON Research and Innovation Actions
Call	Increased Cybersecurity 2023 (HORIZON-CL3-2023-CS-01)
Objectives of the call	Projects' results are expected to contribute to some or all of the following outcomes: • Security-by-design concept and resilience to adversarial attacks; • Inclusion of context awareness in machine learning in order to boost resiliency.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations (including international European research organisations) is eligible to participate (whether it is eligible for funding or not), provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	23 November 2023
Maximum amount/ Call budget	Call budget: EUR 12 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2023-cs-01-03

Nr 401/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Assessing and strengthening the complementarity between new technologies and human skills

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-RIA HORIZON Research and Innovation Actions
Call	A sustainable future for Europe (HORIZON-CL2-2024-TRANSFORMATIONS-01)
Objectives of the call	Projects should contribute to all of the following expected outcomes: • Deepened our understanding on the potential and impact of new technologies such as artificial intelligence technologies and robotics to substitute or complement human skills and in performing job tasks. • Development and deployment of technologies that complement and enhance human skills, and development of the corresponding skills in the workforce.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations (including international European research organisations) is eligible to participate (whether it is eligible for funding or not), provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	07 February 2024
Maximum amount/ Call budget	Call budget: EUR 10 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl2-2024-transformations-01-11

Nr 402/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Supporting operators against cyber and non-cyber threats to reinforce the resilience of critical infrastructures

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-IA HORIZON Innovation Actions
Call	Resilient Infrastructure 2023 (HORIZON-CL3-2023-INFRA-01)
Objectives of the call	• A reliable state-of-the-art analysis of physical/cyber detection technologies and risk scenarios is created, in the context of an operator in a specific sector in sectors that have not yet been covered by previous research projects; • Strengthened cooperation against natural or human-made threats and subsequent disruptions of infrastructures in Europe; • Improved situational awareness, preparedness and governance by the implementation of effective solutions that enhance detection and anticipated projection of a determined threating situation, as well as implementation of prevention, mitigation, response, and recovery types of intervention; • Significant reduction of risks and exposures to anomalies or deliberate events on cyber-physical systems, or on complex and critical infrastructures/systems; • Enhanced preparedness and response by definition of operational procedures of operators as well as public authorities.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate (whether it is eligible for funding or not), provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	23 November 2023
Maximum amount/ Call budget	Call budget: EUR 9 400 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2023-infra-01-02

Nr 403/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference, **Fair**, Exhibition	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

Women's Engineering Day

Description	Women's Engineering Day is an event addressed to women and organized by GE Aerospace Warsaw. GE Aerospace Warsaw hire more than 1200 people who specialize in the design of aircraft propulsion and composite airframe, create and test software applications for aviation and develop advanced technologies. GE Aerospace foster the culture of inclusion, collaboration and knowledge sharing and enable employees to not only work in an international organization but also travel around the world and gain hands-on experience in the shops. GE Aerospace hire the best experts in the industry, that willingly act as mentors, coaches, and instructors.
Goal	Looking for talented women to join GE Aerospace.
Organizer	General Electric Company Polska Sp. z o.o.
Co-organizers/ Patrons	-
Topics	During the event participants will have an opportunity to: • Get to know GE Aerospace better; • Learn about GE Aerospace current recruitment needs ; • Visit GE Aerospace laboratories; • Talk to managers who are recruiting for their teams in GE Aerospace.
Date	April 15, 2023
Costs	-
www	https://jobs.gecareers.com/aviation/global/en/event/6408f27c791f23747f3a96b1/Women-Engineering-Day-at-GE-Aerospace-Warsaw

Nr 404/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Optronics detector technologies

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-RA EDF Research Actions
Call	Call for EDF research actions implemented via actual cost grants (EDF-2023-RA)
Objectives of the call	• This topic aims at consolidating a fully sovereign common supply chain of some critical technology building blocks for the next generation of high performance infrared detectors for defence applications in all battlespace dimensions. • The proposals must address IR detector technologies based on Type-II Superlattice (T2SL) materials. • The proposals should also address advanced silicon ROIC technology with the objective to develop a common post-processing of future ROICs to prepare them for bumping and bumping technology. • The proposals must aim to improve the fundamental knowledge of cryocoolers and find innovative solutions in order to improve the performances of European cryocoolers solutions for IR sensors.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 157 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-ra-sens-optd

Nr 405/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Threat surveillance and protection of space-based assets

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-RA EDF Research Actions
Call	Call for EDF research actions implemented via actual cost grants (EDF-2023-RA)
Objectives of the call	The general objective of this topic is to conduct research activities on space-based technologies contributing to the protection of space-based assets against a wide range of threats and to demonstrate the feasibility of selected technological solutions.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 157 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-ra-space-psa

Nr 406/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Dedicated hardware architectures for energy-efficient AI

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-RA EDF Research Actions
Call	Call for EDF research actions implemented via actual cost grants (EDF-2023-RA)
Objectives of the call	The proposals must address research on new hardware architectures for AI that offer very significant gains in term of power consumption, processing speed and latency, as well as in terms of size, weight and cost. Any type of architecture deemed suitable to address the objectives may be investigated (e.g. magnetic tunnel junctions (MTJ), memristors, in-memory computing, etc., possibly combined with other relevant hardware and software technologies in hybrid architectures).
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 157 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-ra-digit-haai

Nr 407/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Demonstrators and technologies to defeat threats posed by Unexploded Explosives Ordnances (UXO) and Improvised Explosive Devices (IED)

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-RA EDF Research Actions
Call	Call for EDF research actions implemented via actual cost grants (EDF-2023-RA)
Objectives of the call	The main objective of this topic is to prepare a next generation of explosive hazards countermeasures using innovative technologies in order to perform the following functional tasks: • threat detection (including identification, classification and data fusion) - Rapid and improved detection of buried or hidden UXO/IED, including threat identification and classification, including area monitoring for the presence of explosive threats. Sensor fusion to achieve a more reliable output is considered under this topic, as well as the use of UAV/UGV for remote detection; • threat investigation - Following the UXO/IED first alert, obtained either by means of device/explosive detection or from a suspicious behaviour/event, the confirmation of it being a real or false alarm may be necessary.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 157 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-ra-protmob-dexplo

Nr 408/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

Automation of security penetration tests

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-RA EDF Research Actions
Call	Call for spin-in EDF research actions implemented via actual cost grants (EDF-2023-RA-SI)
Objectives of the call	This research topic aims to overcome defence-specific obstacles associated to the automation of penetration tests, and at least partially automate the process by developing a user-friendly software solution that performs network security penetration tests for cyber defence actors. The proposals should address research that is based on use cases where the system owner administrates the penetration tests. Thus, non-cooperative computer networks are outside the scope of this topic. For instance, the use cases can include a) whitelisting of payloads in antivirus software, or b) release of initial information about the targeted network to the penetration testing system.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 59 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-ra-si-cyber-aspt

Nr 409/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

Non-thematic research actions targeting disruptive technologies for defence

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-LS EDF Lump Sum Grants
Call	Call for disruptive EDF research actions implemented via lump sum grants (EDF-2023-LS-RA-DIS)
Objectives of the call	The proposals are sought for cutting-edge, high-risk/high-impact research leading to game-changing impact in a defence context. The proposals may address any area of interest for defence, such as, but not limited to, the following ones: • tools and applications improving cybersecurity talents screening; • artificial intelligence and robotic autonomous systems; • future naval platform control and management; • smart damage control related to future naval platforms; • secure and reliable underwater communication solutions and interfaces; • solutions for mechanical and “green” chemical recycling of waste of soldier individual equipment; • concepts and corresponding technologies to ensure a safe water reuse; • synthetic fuel production from waste and biomass for military use.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: be legal entities, be established in one of the eligible countries, i.e.: EU Member States, non-EU countries: listed EEA countries, have their executive management structure established in eligible countries, must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 16 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-ls-ra-dis-nt

Nr 410/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Agile and robust human language technologies for defence – Participation to a technological challenge

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-LS EDF Lump Sum Grants
Call	Call for EDF research actions, in the form of a technological challenge, implemented via lump sum grants (EDF-2023-LS-RA-CHALLENGE)
Objectives of the call	The proposals should address technological solutions to process linguistic information in its different forms, i.e. spoken and written (handwriting, printed documents or typed text), in order to recognise, understand and translate it. These solutions should be evaluated in the framework of the technological challenge organised under this call topic. The proposals should in particular address the issue of user-driven system adaptation, i.e. the ability of systems to learn from user supervision without intervention from developers and without regression in terms of performances. Technologies should be integrated into demonstrators with user-friendly interfaces and be easy to integrate into other defence systems.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 25 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-ls-ra-challenge-digit-hltp

Nr 411/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Federating CBRN systems

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-DA EDF Development Actions
Call	Call for EDF development actions implemented via actual cost grants (EDF-2023-DA)
Objectives of the call	The general objective of this topic is to create an overarching information system that enables interoperability between the different existing national CBRN defence information management systems, or subsystems, with the aim to improve and to better use and coordinate available CBRN defence resources within the EU Member States and EDF associated countries (Norway) to obtain greater endurance for their armed forces. The proposals should focus on integration of CBRN defence technologies into a comprehensive software system. However, the proposals may also provide analysis of the relevance and feasibility of novel CBRN technologies, mapping of CBRN defence capacities across the EU and EDF associated countries, as well as options for ensuring access and availability of CBRN technologies.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 714 500 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-da-mcbrn-fcs

Nr 412/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Laser communications

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-DA EDF Development Actions
Call	Call for EDF development actions implemented via actual cost grants (EDF-2023-DA)
Objectives of the call	The proposals must address activities to design a prototype for airborne laser communication system to be used on various types of aircraft, manned or unmanned. In detail, the proposals must address: • an overview about a suitable configuration for airborne laser communication including all parts of the communication chain (RPAS terminal, satellite terminal, satellite orbit position, inter-satellite communication, downlink); • identification, analysis and mitigation of critical technical risks especially those relating to integration and certification; • definition of a set of requirements, considering the whole product cycle; • life cycle cost analysis and management; • developing of a prototype to demonstrate the possible airborne integration.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 714 500 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-da-c4isr-lcom

Nr 413/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Agile and robust human language technologies for defence – Organisation of a technological challenge

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-LS EDF Lump Sum Grants
Call	Call for EDF research actions, in the form of a technological challenge, implemented via lump sum grants (EDF-2023-LS-RA-CHALLENGE)
Objectives of the call	The objective evaluation of artificial intelligence (AI) technologies such as human language technologies (HLT) requires a specific organisation whereby systems are tested in a blind manner on data that is representative of the tasks under study, using common protocols. This scheme, which has been pioneered by the HLT community under the term "evaluation campaign", is also often called a "technological challenge". One objective of the call is to organise a technological challenge driving research toward enhanced HTL systems for defence applications. The proposals should address the organisation of a technological challenge on HLT. This includes the collection, annotation and distribution of data, and the writing of the evaluation plans.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 22 November 2023
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-ls-ra-challenge-digit-hlto

Nr 414/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Tactical RPAS

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-DA EDF Development Actions
Call	Call for EDF development actions implemented via actual cost grants (EDF-2023-DA)
Objectives of the call	The specific objective of this topic is to develop a multi-purpose/multi-role T-RPAS, for the potential use by units of mainly up to divisional size. It will collect tactical level intelligence (real-time target cinematics, terrain, enemy location and movements) with high-performance multi-sensor equipment, through ISR (ground, maritime and air) and targeting missions, in addition to other related tasks (target acquisition, identification, tracking).
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 714 500 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-da-c4isr-trpas

Nr 415/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Detect and avoid

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-DA EDF Development Actions
Call	Call for EDF development actions implemented via actual cost grants (EDF-2023-DA)
Objectives of the call	The specific objective is to take the necessary steps towards a standardised, qualified and certified Detect and Avoid (DAA) systems solution to be integrated in many different unmanned aerial systems (UAS), hence allowing a full integration for civil and military airspace and U-space services where applicable, and operational use of current and near-term platforms to be used, such as MALE RPAS.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-da-c4isr-daa

Nr 416/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Sensor grid

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-DA EDF Development Actions
Call	Call for EDF development actions implemented via actual cost grants (EDF-2023-DA)
Objectives of the call	The proposals must address the establishment of a European Architecture Framework for multiple interoperable and collaborating sensors. Efforts should aim at overall sensor performance optimisation (e.g. in terms of coverage, accuracy and efficient use of electromagnetic spectrum) against diverse and evolving challenging threats. The Architecture Framework should enable the integration and optimal use of EU Member States and EDF associated countries (Norway) sensor assets that exist or are under development and collaborative use of the sensors data.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 714 500 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-da-sens-grid

Nr 417/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

Full-Spectrum Cyber Situational Awareness for enhanced Cyberspace Operations Support

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-DA EDF Development Actions
Call	Call for EDF development actions implemented via actual cost grants (EDF-2023-DA)
Objectives of the call	The proposals must focus on developing capabilities for mission-centric Cyber Situational Awareness (CySA), which as a System of Systems (SoS), must comprise independent enablers able to act jointly towards facilitating human decision-making through synergies between them. The proposals should address challenges in all the following areas: • full-spectrum cyber situational awareness, • decision, command, and control support, • interoperability,
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-da-cyber-csa

Nr 418/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

Deployable Autonomous AI Agent

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-DA EDF Development Actions
Call	Call for EDF development actions implemented via actual cost grants (EDF-2023-DA)
Objectives of the call	The proposals must focus on the development of an autonomous and adaptive deployable AI agent. All proposed activities must ultimately support the creation of an AI agent that is able to conduct automated and semi-automated incident management on different cyber defence systems for the entire process of the incident management cycle. The solutions must support human operators, analysts and decision-makers at technical, tactical, operational, strategic and political level. In addition, solutions are expected to contribute to enhanced cyber situational awareness, increased military infrastructure resilience and improved protection against AI-based and other advanced cyber threats.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 714 500 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-da-cyber-daai

Nr 419/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Initial operational capacity for Space situational awareness C2 and sensors

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-DA EDF Development Actions
Call	Call for EDF development actions implemented via actual cost grants (EDF-2023-DA)
Objectives of the call	The general objective is to develop interconnected military space situational awareness (SSA) centres with their respective sensors to foster a larger degree of European autonomy with respect to awareness of the situation in space in order to contribute to a Recognised Space Picture (RSP), and support space operations, taking also benefit of relationships which may be established with other partner nations and organisations and their capabilities.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 714 500 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-da-space-ssa

Nr 420/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

Smart technologies for next generation fighter systems

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-DA EDF Development Actions
Call	Call for EDF development actions implemented via actual cost grants (EDF-2023-DA)
Objectives of the call	The proposals must address the study and the development of key technologies supporting the next generation of military integrated modular avionics (NG-MIMA). The proposals should consider multiple military aerial platforms that should operate in a defence air cloud context, both manned and unmanned, including other than fighters.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 714 500 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-da-air-stfs

Nr 421/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

Self-protection systems

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-DA EDF Development Actions
Call	Call for EDF development actions implemented via actual cost grants (EDF-2023-DA)
Objectives of the call	The specific objective is to develop an enhanced self-protection systems SPS able to protect against: • direct threats (e.g. missiles, loitering munition, RPG, etc.); • indirect threats (e.g. surveillance/acquisition/tracking systems also with Low Probability of Intercept (LPI) radar capability; • new proliferating types of threats, such as those in the field of loitering munitions, directed energy weapons (DEW) and cyber electromagnetic activity (CEMA) capabilities.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 714 500 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-da-air-sps

Nr 422/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Counter unmanned aerial systems

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-DA EDF Development Actions
Call	Call for EDF development actions implemented via actual cost grants (EDF-2023-DA)
Objectives of the call	The proposals must address the development of a counter unmanned aerial system (C-UAS) system, from a detailed design up to a system prototype to be tested and qualified in relevant defence operational scenarios, demonstrating its ability to: • with a selection of passive and active sensors, detect, track, classify, identify, support decision making and counter class I UAS (single and/or multi-UAS) through an optimal selection and activation of relevant effectors using multiple technologies; • ensure effective protection of critical defence infrastructure, installations and assets; • operate with limited impact on existing communications or position and navigation infrastructures.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 714 500 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-da-airdef-cuas

Nr 423/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

Main battle tank platform systems

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-DA EDF Development Actions
Call	Call for EDF development actions implemented via actual cost grants (EDF-2023-DA)
Objectives of the call	The proposals must address studies and design for the upgrade of current and development of future main battle tank technologies, including enabling and green technologies, leading to a system level, capable of outstanding operational effectiveness and mission success in all possible future scenarios. Furthermore, the proposals must take into account aspects such as mobility, deployability, autonomy, firepower, protection and cybersecurity.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 714 500 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-da-ground-mbt

Nr 424/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Unmanned anti-submarine and seabed warfare

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-DA EDF Development Actions
Call	Call for EDF development actions implemented via actual cost grants (EDF-2023-DA)
Objectives of the call	The specific objective of this topic is to develop and assess, in a real environment, unmanned platforms and other new assets along with traditional platforms to manage efficiently anti-submarine warfare (ASW) and seabed warfare (SBW) operations to face current and future threats in the new security context.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 714 500 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-da-uww-asw

Nr 425/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Future maritime mine countermeasures capability

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-DA EDF Development Actions
Call	Call for EDF development actions implemented via actual cost grants (EDF-2023-DA)
Objectives of the call	The specific objective is to enable solutions that are easily deployable both on current (by retrofit) and future naval assets. The focus is on interoperability and interchangeability as from the design phase of the systems, including data-sharing. The aim is to provide capable and cost-effective technologies for MCM operations. These include enabling systems for mine warfare platforms (such as launch and recovery (LARS) and command and control (C2) systems), development of unmanned platforms, decision support, planning, and evaluation tools.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 714 500 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-da-uww-mcmc

Nr 426/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Endo-atmospheric interceptor – concept phase

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-2021 European Defence Fund Action
Call	Protection against high velocity aerial threats (EDF-2021-AIRDEF-D)
Objectives of the call	The proposals must address surface-to-air interceptor solutions including interceptor concepts studies, and associated early maturation activities, until an interceptor mission definition review (MDR) and a preliminary requirements review (PRR) approved by the cooperating Member States.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	09 December 2021
Maximum amount/ Call budget	Call budget: EUR 28 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2021-airdef-d-eatmi

Nr 427/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Electromagnetic signal propagation

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-RA EDF Research Actions
Call	Call for EDF research actions implemented via actual cost grants (EDF-2023-RA)
Objectives of the call	The main objective is to develop and test an efficient model of electromagnetic wave propagation capable of assessing and predicting EM signal propagation conditions to contribute to the creation of a tactical decision-making aid (TDA).
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), non-EU countries: listed EEA countries, • have their executive management structure established in eligible countries, • must not be subject to control by a non-associated third country or nonassociated third-country entity.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 157 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-ra-sens-emsp

Nr 428/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

7th International Conference on Computer Science and Application Engineering (CSAE 2023)

Description	The 7th International Conference on Computer Science and Application Engineering (CSAE 2023) will be held during October 17 to 19, 2023 in Wuhan, China. It is held annually.
Goal	The goal is to provide a comprehensive global forum for experts and participants from academia to exchange ideas and present results of ongoing research in the most state-of-the-art areas of computer science and application engineering.
Organizer	-
Co-organizers/ Patrons	-
Topics	The topic of the paper submitted to this conference is included but not limited to: • AI, • Algorithm and Data Structure, • Big Data, • Computational Intelligence and Complexity, • Control, • Electronics, • Geographical Information Systems, • Human–Computer Interaction, • Image Processing, • Information Systems and Applications, • Intelligent Transportation System, • Machine Translation, • Programming, • Robotics, • Security and Cryptology, • Signals, • Software Engineering.
Date	October 17 - 19, 2023
Costs	Regular Author with Full Paper: RMB 3400 (USD 530) per paper Oral / Poster Presentation only: RMB 1500 (USD 240) per person Listener: RMB 1500 (USD 240) per person
www	http://www.csaeconf.org

Nr 429/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Bachelor in Cyber Security Engineering

Description	The students will acquire necessary knowledge and skills to make IT-systems malware-proof and how to combat cyber-attacks. The curriculum combines theoretical and practical studies (e.g. labs/practice lessons in which students can go through all the steps of setting up and securing the network and services of a company.
Organizer	TalTech (Tallinn University of Technology, Estonia), School of Information Technologies
Cooperation with	-
Duration	3 years
Thematic Scope	By the end of their students, the student will be able to independently design, implement and maintain IT-systems that follow security requirements by: • understanding the life span of an information system; • mastering the basics of information system administration, including development and testing environments; • knowing how to programme, test and implement an information system from the viewpoint of security and maintainability; • knowing how to perform security testing for an information system based on set standards and the best practice; • knowing how to implement processes guaranteeing the security information systems and being capable of taking part in developing and improving them; • following ethical norms in professional activity.
Costs	€6000 per year; free for EU/EEA citizens
No of ECTS credits	180 ECTS
E-learning	No
Tools	-
Job opportunities	Upon successful completion of their studies, students will be able to find error made during the setup of computer networks and devices, organise the cyber security of an institution, implement the best practices etc. Graduates will be able to work as IT specialists, become members of computer emergency readiness teams. Also, they can continue studies on master's level in cyber security and later work as Chief Security Officers.
Additional info	-
www	https://taltech.ee/en/bachelors-programmes/cyber-security-engineering

Nr 430/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

Danish Defence Annual Conference (DDAC)

Description	Danish Defence Annual Conference (DDAC) is the premium annual event and two-day conference in the defence and security industry in Denmark and attracts +300 participants. The event is hosted in collaboration by CenSec, Danish Defence and Security and Industry Association and Naval Team Denmark and the conference alternates between Copenhagen and Aalborg.
Goal	The conference offers a unique opportunity to meet and network with leaders of the defence industry, and discuss with and gain knowledge from high-level decision-makers from the Danish Ministry of Defence, the armed forces, and a wide range of professional defence industry companies.
Organizer	CenSec, Danish Defence and Security and Industry Association, Naval Team Denmark
Co-organizers/ Patrons	
Topics	All topics related with defence and security industry
Date	7-8 February 2024
Costs	DKK 2600 (members) - 6800 (non-members)
www	Different every year, in 2023 http://ddac.censec.dk/

Nr 431/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

7th WORLDS4 2023

Description	This world conference will provide the participants with opportunities to discuss and explore areas related to the Theory, Development, Applications, Experiences and Evaluation of Interaction Sciences with fellow students, researchers and practitioners. Conference may concern any topic within the conference scope. Workshops may be related to any topics within the conference scope.
Goal	• The conference is anticipated to attract a large number of high quality submissions and stimulate the cutting-edge research discussions among many academic pioneering researchers, scientists, industrial engineers, students from all around the world and provide a forum to researcher. • Propose new technologies, share their experiences and discuss future solutions for design infrastructure. • Provide common platform for academic pioneering researchers, scientists, engineers and students to share their views and achievements. • Enrich technocrats and academicians by presenting their innovative and constructive ideas. • Focus on innovative issues at international level by bringing together the experts from different countries.
Organizer	Global Knowledge Research Foundation, G R Scholastic LLP, Springer, Springer Nature
Co-organizers/ Patrons	
Topics	The topics of interest include but are not limited to the following: • Information and Communication Technologies for infrastructure and computation; • Information and Communication Technologies for sustainable engineering applications; • Information and Communication Technologies for secured e-governance and government; • intelligent systems and health informatics
Date	21 - 24 August 2023
Costs	
www	https://www.worlds4.co.uk/index.html

Nr 432/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Homeland Security Conference

Description	As an innovation and technology conference, Homeland Security Conference bring together representatives from the entire Homeland Security and cyber security community; leading experts, industry decision makers, governmental authorities, and academics, in order to share knowledge and strengthen capabilities.
Goal	The overall objective is to explore potential business opportunities within the industry and connect stakeholders.
Organizer	CenSec
Co-organizers/ Patrons	
Topics	The conference has an overall focus on issues, challenges and possible countermeasures within the Homeland Security context and will take a dive into the following areas: • Homeland Security Perspectives 2023 • Securitization of Energy Supplies • Territorial Control and Surveillance Innovations and Technologies • Securing Critical Infrastructure • Investments and Collaboration Opportunities for Innovative Security Solutions
Date	3 October 2023
Costs	DKK 495 (members) 995 (non-members)
www	https://censec.dk

Nr 433/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

5G COMPAD (Communications for Peacekeeping and Defence)

Description	5G COMPAD connects partners from European telecom and defence industries, who will work together on developing the communication system architecture and specifications as well as create joint testbeds to demonstrate the integration of 5G standalone networks with existing defence infrastructures. This approach combines the use of commercial and defence hardware and software components. The established 5G network procedures that are enhanced with domain-specific orchestration functions provide interoperability between the triad of defence communication systems, public 4G and 5G operator networks, and 5G national security networks across coalition members from the EU.
Goal	5G seeks to break down the challenges faced by European armed forces, which currently rely on expensive hardware-locked communications with limited interoperability and data rates. The project will provide a robust high-speed communication system and enable the rapid introduction of new capabilities by: • designing a reference architecture for 5G-based communications system compatible with existing systems and platforms, and; • enabling the recurrent integration of 5G. This will ensure sustained information superiority for operational success across the conflict spectrum (including peacetime, grey-zone and armed conflicts).
Lead Partner	SAAB (Sweden)
Partners involved	Ericsson (Sweden), Rheinmetall (Germany), Bittium (Finalnd), Nokia (Finland), Thales (France), Leonardo (Italy), INSTER (Spain), Eight Bells Hellas PC (Greece), Intracom Defence (Greece), CAFA Tech (Estonia), Telenor Group (Norway), Norwegian Defence Research Establishment (FFI), LMT (Latvia), Austrian Institute of Technology, Synkzone (Sweden), BHE (Hungary), APR Technologies AB (Sweden), CNIT (National, Inter-University Consortium for Telecommunciations) (Italy), Fraunhofer (Germany), The French Alternative Energies and Atomic Energy Commission (CEA), Space Hellas (Greece)"
Duration	December 2022 - December 2025
Results	https://5gcompad.eu/
Funding	Co-financed by the European Defence Fund
www	https://5gcompad.eu/

Nr 434/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

EU-GUARDIAN (European framework and proofs-of-concept for the intelliGent aUtomAtion of cybeR Defence Incident mAnagemeNt)

Description	EU-GUARDIAN seeks to explore and lay the foundations for prompting the EU autonomy in the development of AI-based resources. The project will develop Cyber Mosaic Warfare concepts and applications and create related capabilities. Mosaic warfare refers to the combined use of AI and automation to implement decision center operations to ensure improved efficiency, greater adaptability for commanders, easier incorporation of new tactics and technologies. The project mainly focuses on the ability to detect, mitigate and respond to security challenges semi-automatically or automatically; support human operators, analysts and decision-makers at all levels; and contributing to enhance cyber situational awareness, military infrastructure resilience and protection against advanced cyber threats.
Goal	EU-GUARDIAN will create an AI-based solution to automate incident management and cyber defence processes. The AI-based solution is contingent on multiple steps, which are considered as the objectives of the project: 1. the categorisation of related incidents and data assesment to establish whether multiple problems share a common underlying cause; 2. enhanced support for cyber security and cyber defence related human operators, analysts, and decision-makers at all levels; 3. the contribution to an enhanced cyber situtational awareness, improving contextual knowledge of the enterprises, processes, and decision-making where AI should be utilised; 4. increasing military infrastructure resilience and improved protection against advanced cyber threats; 5. supporting the creation of fit-for-purpose proof-of-concept prototypes of an automated or semi-automated incident management and cyber defence system; 6. referencing systems and appropriate tests cases to generate training data and evaluate the efficacy of different solutions will be created, both with and without human operators interacting with the system; 7. identifying opportunities for long-term improvement, wide cross-border cooperation between legal entities, and foster better exploitation of the industrial potential of innovation, research, and technological development; 8. better explainability of the whole process of analysis, response and execution, which will be heavily oriented to contributing to the regulation and standardization of the achieved outcomes; 9. achieving excellence, trust, and a boost in research and industrial capacity; 10. ensuring an appropriate ethical and legal framework based on the Union's values and in line with the Charter of Fundamental Rights of the EU.

Lead Partner	Indra Sistemas S.A. (Spain)
Partners involved	• Airbus Cybersecurity (France) • Leonardo (Italy) • Cybernetica (Estonia) • Bianor (Bulgaria) • Bulgarian Defence Institute • Universidad de Murcia (Spain) • Sapienza Universita di Roma (Italy) • Baltic Institute for Advanced Technology (Lithuania)
Duration	December 2022 - December 2025
Results	https://www.eu-guardian.eu/work_streams.html
Funding	EU-funded
www	https://www.eu-guardian.eu/index.html

Nr 435/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

REWIRE (Cybersecurity Skills Alliance - New Vision for Europe)

Description	REWIRE develops a Blueprint strategy of skills development for the cybersecurity industry in Europe. Buidling upon four pilot projects - CONCORDIA, SPARTA, ECHO, CyberSec4Europe - the project consolidates relevant aspects of cybersecurity education across Europe. The global vision for the skills strategy for cybersecurity in Europe, as developed in REWIRE, includes: • A skills framework, describing the various job profiles, skills and knowledge relevant for cybersecurity, in an organized manner, and building upon already existing work (ENISA ECSF, ESCO, and output from the pilot projects); • Attractiveness of the cybersecurity sector, describing an analysis of the cybersecurity job market and the demand for cybersecurity professionnals; • Tools for skills identification, enabling interested parties to provide better job descriptions and courses descriptions; • Tools for skills development, identifying courses and programs for acquiring skills and knowledge, as well as career pathways to enable skills development over time; • Governance, describing how such a cybersecurity skills framework could be maintained in the long term for the benefit of the European community.
Goal	By addressing the skill gaps and shortages in different occupational profiles and qualifications of the cybersecurity sector, REWIRE seeks to acheive a coherent strategy through following specific objectives in Innovation, Impact, and Sustainability. Innovation: • design and deliver the European Cybersecurity Blueprint; • develop the European Cybersecurity Skills Framework, update existing and create 4 new occupational profiles; • deliver training programmes on highly innovative fields; • develop a digital on-line publicly accessible Skills Observatory for cybersecurity skills merging the market needs, the profiles, the competencies and the available training courses. Impact: • involve all stakeholders for exploiting the VET potential in cutting-edge subjects for creating growth and jobs in the Cybersecurity sector; • enhance the use of cyberranges; • promote the application of EQAVET and EQF/ECVET frameworks that ensure both quality and better transferability of the project's results. Sustainability: • create a lasting partnership of all types of stakeholders that will monitor and

	adjust to changes in the sector's needs; • facilitate transnational mobility between the sectors' stakeholders; • provide transversal skills as well as career guidance, career management skills and access to the labour market, thus improving their long-term employability.
Lead Partner	Mykolas Romeris University (Lithuania)
Partners involved	EKT (Lithuania), NRD Cyber Security (Lithuania), InfoBalt (Lithuania), TÜV AUSTRIA , APIROPLUS Solutions (Cyprus), European University Cyprus, Cyprus Certification Company, Brno University of Technology (Czechia), Masaryk University (Czechia), EC-Council (International Council of E-Commerce Consultants) (United States), EFVET (European Forum of Technical and Vocational Education and Training), EVTA (European Vocational Training Association) , Télécom SudParis (France), Télécom Nancy (France), Technical University of Crete (Greece), Metropolitan College (Greece), ReadLab (Greece), LRQA (Greece), Műegyetem (Budapest University of Technology and Economics) (Hungary), Tecnico Lisboa (Portugal), Unicom Telecom (Serbia), Caixa Bank (Spain), la Salle Ramon Llull University (Spain), KTH Royal Institute of Technology
Duration	November 2020 - October 2024
Results	https://rewireproject.eu/deliverables/
Funding	EU-funded
www	https://rewireproject.eu/about/

Nr 436/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Erasmus Mundus Joint Master in Applied Cybersecurity (CyberMACS)

Description	This Erasmus Mundus Joint Master in Applied Cybersecurity (CyberMACS) prepares future cybersecurity experts to detect, prevent, mitigate, and manage cyber-attacks. The students will be trained on basics of cybersecurity in the first year at Kadir HAS University (Istanbul), which will be followed by a two month compulsory industrial training. After that the students will continue on a specialisation track in either: • SRH Berlin University of Applied Sciences (Germany), where they can focus on one of the following: Advanced Technologies in Cybersecurity (30 ECTS), Cyber Security Management (30 ECTS), Long-Term Practical Training (30 ECTS); • Cyril and Methodius University, UKIM (Skopje, North Macedonia), where they can focus on either Web & Cybersecurity (30 ECTS) or Cryptology (30 ECTS).
Organizer	Kadir HAS University (Istanbul, Turkey)
Cooperation with	SRH Berlin University of Applied Sciences (Germany) Cyril and Methodius University, UKIM (Skopje, North Macedonia)
Duration	2 years
Thematic Scope	The covered topics include web and security; the socio-economic and legal issues relating to cybersecurity; the implementation of cybersecurity tools and norms within large and small organisations; security awareness and security escalations issues; data exploration methods; tools and techniques for systems security; cryptology research and data management.
Costs	About one third of students will be required to pay €5175 tuition fees for the whole programme, while one third is eligible for tuition fee and registration fee waivers. The final third will be eligible for Erasmus Mundus scholarships based on merit, amounting to €1400 /month for the duration of the studies
No of ECTS credits	120 ECTS
E-learning	No
Tools	-
Job opportunities	Possible career paths for CyberMACS graduates include: cybersecurity expert, cybersecurity analyst, data protector, cybersecurity vulnerability assessor, security architect or product integrator, system penetration tester, incidence response expert, cryptographer, malware analyst, application security expert.
Additional info	-
www	https://cybermacs.eu/

Nr 437/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course **Postgraduate studies**	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

International Master Security, Intelligence & Strategic Studies

Description	The IMSISS (International Master Security, Intelligence & Strategic Studies) programme takes an interdisciplinary approach to examine a range of contemporary security challenges related to terrorism, civil war and conflict, mass migration, energy supply security, organised crime and cybersecurity and new technologies. The degree combines theoretical, applied and empirical knowledge and skills in the study of security on an international mobility structure that takes the students to three different universities across two years to complete their degree. In the first semester, all students will begin the degree programme at the University of Glasgow, where they focus on intelligence analysis and international security strategies. For the second semester, students will choose to take either the intelligence, peace-building and terrorism pathway at Dublin City University (Ireland), or the causes of conflicts pathway at the University of Trento (Italy). The students will spend their third semester at the Charles University Prague (Czechia), where they have to specialise in one of the following themes: strategic and war studies; global and regional security; security, technology and society; or, peace and conflict studies. The final semester will be spent working on an independent study portfolio that includes a dissertation.
Organizer	University of Glasgow
Cooperation with	Dublin City University (Ireland), University of Trento (Italy), Charles University Prague (Czechia)
Duration	2 years (4 semesters)
Thematic Scope	Interdisciplinary security studies
Costs	EU (including UK) students €10,217 per annum / £8,540 per annum. Erasmus Mundus scholarships also available.
No of ECTS credits	120 ECTS
E-learning	No
Tools	-
Job opportunities	-
Additional info	-
www	https://www.securityintelligence-erasmusmundus.eu/

Nr 438/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

Master's Programme in Security and Cloud Computing

Description	The Erasmus Mundus joint masters SECCLO (Security and Cloud Computing) combines strong security knowledge with hands-on R&D skills in cloud computing to educate highly professional engineers to meet immediate hiring requirements and long-term needs of the European ICT industry. The first year of the curriculum is offered by Aalto University in Finland, wherein students will focus on secure systems engineering, distributed application development, network and service architectures, ubiquitous computing, cloud and mobile computing platforms. At the end of the first year, students will do a summer internship at one of the industrial partners of the consortium. In the second year, the students will continue at another consortium university by specialising in one of the following fields: communications systems (The Royal Institute of Technology, Sweden), information security (The Norwegian University of Science and Technology, NTNU), reliable distributed systems (Technical University of Denmark), cryptography (University of Tartu, Estonia), big data security (EURECOM co-deliverance with Institut Mines Télécom, France).
Organizer	Aalto University (Finland)
Cooperation with	The Royal Institute of Technology KTH, Sweden, The Norwegian University of Science and Technology, Technical University of Denmark, University of Tartu, Estonia, EURECOM co-deliverance with Institut Mines Télécom, France
Duration	2 years (4 semesters)
Thematic Scope	Cloud computing (highly distributed and scalable computation and data storage in data centers as well as physically accessible devices) and information security (protection of computation, communication and data from unauthorized access).
Costs	Tuition fees €3000/year. Erasmus Mundus scholarships available based on merit.
No of ECTS credits	120 ECTS
E-learning	No
Tools	-
Job opportunities	The dual perspective of security plus R&D skills for the cloud environment gives the graduates multiple options for their future career in the European labour market in international industrial R&D jobs, security engineering and consulting, various expert roles, doctoral studies in the field.
Additional info	-
www	https://www.secclo.eu/

Nr 439/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Marine and maritime Intelligent Robotics (MIR)

Description	The Erasmus Mundus Marine & Maritime Intelligent Robotics (MIR) master's degree integrates marine science, maritime technologies, AI and robotics to develop highly specialised and sought after skills in the maritime sector. In this format, the students will be able to have a deeper understanding of marine processes and challenges and the potential of developing robotic and AI-driven technologies in this environment. The first year of studies takes place at the University of Toulon, where students build a common background in marine science, robotics and AI. In the second year, the students will be able to specialise at one of the consortium universities: 1. Applied robotics for underwater intervention missions (Universitat Jaume I, Spain). These technologies using manipulators are mainly applied in offshore industry, scientific research, aquaculture and marine defence. 2. Safe autonomous subsea operations (Norwegian University of Science and Technology). With an increased level of automation and autonomy, these technologies seek to make subsea operations safer, more efficient and cost-effective. 3. Cooperative marine robotics for scientific and commercial applications (Tecnico Lisboa, Portugal). At the core of such applications are engineers in charge of cooperative motion planning with temporal and energy cost criteria, cooperative navigation and control, and networked operations which are often enabled by acoustic communication links.
Organizer	University of Toulon (France)
Cooperation with	University Jaume I (Spain), Norwegian University of Science and Technology, Tecnico Lisboa (Portugal)
Duration	2 years (4 semesters)
Thematic scope	Robotics and AI, marine and maritime science
Costs	€4500 per year, Erasmus Mundus scholarships are available based on merit.
No of ECTS credits	120 ECTS
E-learning	No
Tools	
Job opportunities	Oceanographic research, offshore renewables, ocean farming, oil and gas surveying as well as security and surveillance (harbours, critical infrastructures and marine reserves).
Additional info	-
www	https://www.master-mir.eu/

Nr 440/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Intelligent Field Robotic Systems (IFROS)

Description	The Erasmus Mundus joint master in Intelligent Field Robotic Systems (IFROS) offers an engineering programme for future developers of field robots. Integration of technologies like AI, computer vision, control, sensorization, machine learning, and manipulation. The masters' program addresses the shortage of engineers in field robotics development. Students will spend the first two semsters at the University of Girona to build a common foundation in field robotics with a focus on land and marine robots. In the third semester, they will be able to choose between specialisations in: • multiple robots and aerial vehicles (University of Zagreb, Croatia), and; • autonomous systems and self-driving land vehicles (Eötvös Loránd University, Hungary). The degree will be finalised with a thesis project, which the students can complete at any of the consortium universities or associated partners (industry stakeholders like NATO, GRAAL Tech, or Coronis Computing).
Organizer	University of Girona (Spain)
Cooperation with	University of Zagreb (Croatia) Eötvös Loránd University (Hungary)
Duration	2 years (4 semesters)
Thematic scope	Field robotic systems engineering, automation and AI.
Costs	€4500 per year. Erasmus Mundus scholarships available.
No of ECTS credits	120 ECTS
E-learning	No
Tools	-
Job opportunities	-
Additional info	-
www	https://ifrosmaster.org/

Nr 441/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Erasmus Mundus Joint Master in Artificial Intelligence (EMAI)

Description	The Erasmus Mundus Joint Master in Artificial Intelligence (EMAI) gives students the foundational knowledge needed to explore key contextual areas and complex technical applications of AI systems. All students will begin their studies at the Universitat Pompeu Fabra in Barcelona for a common introduction to the different paradigms of AI and to the basic computational mathematical background with compulsory courses on autonomous systems, symbolic reasoning, machine learning, natural language interaction and reinforcement learning. The students will spend the second semester at one of the other consortium universities. In the second year, the students will specialise at one of the four consortium universities, where they will develop their master theses: • Intelligent Decision Making (University Pompeu Fabra, Spain) • Robotics (Sapienza University Rome, Italy) • Cybersecurity (Radboud University Nijmegen, Netherlands) • Data Science (University of Ljubljana, Slovenia)
Organizer	University Pompeu Fabra (Spain)
Cooperation with	Sapienza University Rome (Italy), Radboud University Nijmegen (Netherlands), University of Ljubljana (Slovenia)
Duration	2 years (4 semesters)
Thematic scope	Artificial Intelligence
Costs	Out of 25 students admitted, five will be offered a fee waiver and 20 will be offered the full Erasmus Mundus scholarship (€1400 monthly)
No of ECTS credits	120 ECTS
E-learning	No
Tools	-
Job opportunities	EMAI integrates machine learning and modern symbolic AI in theory, methods and applications. The students learn to use AI technologies, and to develop new tools that go beyond the state-of-the-art. This competitive advantage of the program will prepare students for careers in a large number of sectors of the digital industry (ICT, cybersecurity, data science, robotics, digital health, renewable energy etc.) as well as to continue a scientific career.
Additional info	-
www	https://www.upf.edu/web/emai

Nr 442/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Erasmus Mundus Joint Master in Cybersecurity (CYBERUS)

Description	The CYBERUS Erasmus Mundus Joint Master in Cybersecurity prepares graduates for careers in cybersecurity by offering a combination of courses meant to develop technological, research and horizontal skills. All students spend the first two semesters of studies at the University Bretagne Sud to ensure a solid common cybersecurity foundation. During the winter break, they will attend the Winter School at Tallinn University of Technology (Estonia) on 'Cyberthreats to the EU and Cyberactors'. In the third semester, the students will specialise in either: • IoT Cybersecurity (Université libre de Bruxelles, Belgium), or; • Software Cybersecurity (University of Luxmebourg). In the final semester, students will conduct a five month internship at their selected institute anywhere in the world and write a master's thesis under joint supervision of either UBS and ULB, or UBS and UL researchers.
Organizer	University Bretagne Sud (UBS) (France)
Cooperation with	Université libre de Bruxelles (ULB) (Belgium) University of Luxembourg (UL)
Duration	2 years (4 semesters)
Thematic scope	Cybersecurity
Costs	Annual fee €4500. Erasmus Mundus scholarships available based on merit.
No of ECTS credits	120 ECTS
E-learning	No
Tools	-
Job opportunities	CYBERUS graduates will be able to hold diverse positions depending on their chosen specialisation track and final internship, for example as cybersecurity engineer, cybersecurity analyst/assessor, security architect, security product integrator, penetration tester, software developer/engineer, cryptographer, malware analyst, and application security expert.
Additional info	
www	https://master-cyberus.eu/

Nr 443/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Advanced European platform and network of cybersecurity training and exercise centres (ACTING)

Description	The ACTING project will develop a network of advanced interconnected domain-oriented cyber ranges for training and exercises. The project will incorporate sophisticated methods and techniques for simulation of users, analysis of the performance of cyber operators, and scoring cyber security situational awareness.
Goal	The goal of ACTING is to provide solutions to improve the efficiency of cyber defense training and exercises. The project aims to create and use advanced tools for user simulation, automated performance analysis, language development for comprehensive and large-scale scenarios, federation of cyber ranges, and a federated scoring system for end information exchange for common cyber situational awareness.
Lead Partner	Institut Po Otbrana (Bulgarian Defense Institute); RHEA BV (technical coordinator)
Partners involved	Defence Research Institute (France), Ecole Royale Militaire/Koninklijke Militaire School (Belgium), 8bells Independent Research & Consultancy (Athens), Enquirya BV (Netherlands), Military Academy (Portugal), Information Technologies Institute (Greece), European Software Institute - Center Eastern Europe (Bulgaria), GMV Innovating Solutions Skysoft SA (Portugal), Institute of Communication and Computer Systems (Greece), Managing & Innovation Business Partners (Spain), VisionSpace (Portugal), National Laboratory of Computer Virology (Bulgaria), National University of Ireland Maynooth, Naval Group Belgium, Pravo i Internet Foundation (Bulgaria), Safetech (Romania), Sidroco (Cyprus), Space Hellas (Greece), STAM Srl (Italy), Telefonica (Spain), Telelink Business Services (Bulgaria), University of Vienna (Austria), University of Cyprus, VisionSpace Gmbh (Germany), Wings ICT Solutions (Greece), Zanasi Alessandro SRL (Italy)
Duration	January 2023 - January 2027
Results	-
Funding	EU-funded
www	https://acting-project.eu/

Nr 444/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

NOTIONES (iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and acadEmia actorS)

Description	The timely identification of emerging technologies and analysis of their potential impact on the intelligence community but also on terrorist and criminal organisations is crucial. To ensure that intelligence practitioners are updated with most recent technologies and their impact, NOTIONES will establish a network to connect researchers and industries with the intelligence community. The aggregated information from both sides will be consolidated in roadmaps, priorities and recommendations for future research projects and development activities.
Goal	NOTIONES seeks to build and maintain a pan-European ecosystem of security and intelligence practitioners in order to monitor technologic opportunities and advancements and best practices, and define and refine requirements and standardization needs.
Lead Partner	Fundacion Tecnalia Research & Innovation (Spain)
Partners involved	Zanasi Alessandro srl (Italy), Laurea University of Applied Sciences (Finland), Bulgarian Defence Institute , Defence Research Institute (France), Intelligence Culture and, Strategic Analysis (Italy), Bar-Ilan University (Israel), APRE (Agency for the Promotion of European Research) (Italy), Teknologian Tutkimuskeskus VTT OY (Finland), Expert.ai (EXPSYS), SAHER (Estonia), MarketScape (MS), Tecoms srl (Italy), SYNYO GmbH (Austria), Police Service of Northern Ireland (PSNI), Durzhavna Agentsiya Natsionalna Sigurnost (DANS) (Bulgaria), LESO Leonardo (LL) (Italy), Financial Intelligence Unit Latvia (FIU), International Security and Emergency Management Institute (ISEM) (Slovakia), Kharkiv National University of Internal Affairs (KhNUIA) (Ukraine), Politsei- ja Piirivalveamet (EPBG) (Estonia), Ministry of the Interior of Georgia, Masovian Police (KWPR) (Poland), Polismyndigheten Swedish Police Authority (SPA) , Ministerio da Justicia (PJ) (Portugal), Military Academy Skopje (MAGMA), Hochschule fur den Oeffentlichen Dienst in Bayern (HföD) (Germany), Beyond the Horizon (Belgium)
Duration	September 2021 - September 2026
Results	-
Funding	EU-funded
www	https://www.notiones.eu/

Nr 445/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	**Training**	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

DeepLearn 2023 Summer

Description	DeepLearn 2023 Summer is part of a multi-event called Deep&Big 2023 consisting also of BigDat 2023 Summer. DeepLearn 2023 Summer participants will have the opportunity to attend lectures in the program of BigDat 2023 Summer as well if they are interested.
Goal	DeepLearn 2023 Summer will be a research training event with a global scope aiming at updating participants on the most recent advances in the critical and fast developing area of deep learning.
Organizer	
Prerequisites	Graduate students, postgraduate students and industry practitioners will be typical profiles of participants. However, there are no formal pre-requisites for attendance in terms of academic degrees, so people less or more advanced in their career will be welcome as well.
Duration	July 17, 2023 8:00 AM - July 21, 2023 10:00 PM
Exams	-
Prize	Regular registration: 550 €, On-site registration: 580 €
No of ECTS credits	-
E-learning	Full live online participation will be possible. The organizers highlight, however, the importance of face to face interaction and networking in this kind of research training event.
Job opportunities	-
www	https://deeplearn.irdta.eu/2023su/

Nr 446/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

International Conference on Robotics and Artificial Intelligence Engineering (ICRAIE-2024)

Description	ICRAIE-2024 Meeting is where professionals meet to share ideas and advance scientific and technical knowledge. By attracting thousands of professionals, the meeting provides excellent opportunities for sharing your passion for Robotics and Artificial Intelligence, connecting with the world's largest scientific society, and advancing your career in this ever-changing global economy.
Goal	This event is anticipated attendees all over the world come together to collaborate and network.
Organizer	The Iconic Meetings
Co-organizers/ Patrons	
Topics	Robot Manipulation and Grasping, Robot Perception and Sensing, Robot Localization and Mapping, Robot Learning and Adaptation, Robot Motion Planning and Control, Swarm Robotics, Human-Robot Interaction, Autonomous Robots, Robot Ethics and Safety, Soft Robotics, Medical and Surgical Robotics, Field Robotics, Robotic Vision and Perception, Cloud Robotics, Robotics in Education and Outreach, Machine Learning Algorithms and Models, Natural Language Processing and Understanding, Computer Vision and Image Processing, Explainable AI and Interpretability, AI for Robotics and Autonomous Systems, Knowledge Representation and Reasoning, AI for Healthcare and Medical Applications, AI for Smart Cities and Urban Planning, AI in Finance and Banking, AI in Internet of Things (IoT) Systems, AI Ethics and Responsible AI, AI in Education and E-Learning, AI for Cybersecurity and Privacy, AI in social media and Recommendation Systems, AI Engineering and Deployment
Date	March 28-30, 2024
Costs	$399.00-$1329.00 (Early bird on/before July 26, 2023)
www	https://www.artificialintelligence.theiconicmeetings.com/

Nr 447/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

International Conference on Artificial Intelligence and Machine Learning

Description	This Artificial Intelligence conference and Machine Learning meeting will focus on "Advances in Deep Learning and Neural Networks," aiming to engage, empower, and develop new ideas in this platform for the development of intelligent healthcare systems.
Goal	Attendees will have the unique opportunity to learn from leading experts in the field, network with peers and industry professionals, and explore the latest research and developments in Deep Learning and Neural Networks which have the potential to revolutionize healthcare and improve patient outcomes.
Organizer	Mindspace Conferences
Co-organizers/ Patrons	
Topics	• Bayesian Networks and Heuristics • Overfitting and Underfitting • Transfer Learning and Ensemble Learning • Recurrent Neural Networks (RNN) • Convolutional Neural Networks (CNN) • Backpropagation • Gradient Descent • Dimensionality Reduction • Clustering Algorithms • Support Vector Machines (SVMs) • Artificial Neural Networks (ANNs) • Decision Trees and Random Forests • Generative Adversarial Networks (GANs) • Robotics and Chatbots • Image and Speech Recognition • Predictive Analytics
Date	May 12-14, 2025
Costs	Early Bird On/Before July 28, 2023: • E poster/ Poster Presentation: $200-$300 • Student: $399 • Delegate: $499-$599 • Speaker Registration: $799-$899
www	https://mindspaceconferences.com/artificialintelligence/

Nr 448/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

The European Simulation and Modelling Conference

Description	The European Simulation and Modelling Conference is one of the oldest European international conferences on computer simulation and modelling concerned with state of the art technology in modelling and simulation.
Goal	The conference aims to provide an overview of academic basic research in the field of computer simulation.
Organizer	European Multidisciplinary Society for Modelling and Simulation Technology (EUROSIS)
Co-organizers/ Patrons	
Topics	• General Simulation Methodology and Tools • Discrete Simulation Modeling Techniques and Tools • Queueing Models • Simulation and AI • Agent-Based Simulation • Simulation and Optimization • IoT and Smart Industry" (Internet of Things & Industry 4.0) • High Performance and Large Scale Computing • Simulation in Education and Graphics/Data Visualization Simulation • Simulation in Environment, Ecology and Marine Biology • Analytical and Numerical Modelling Techniques • Web Based Simulation • Cloud Based Simulation • Physics modelling and Cosmological Simulation • Simulation in Aerospace • Simulation of Autonomous Systems • Simulation and Systems Engineering
Date	October 24-26, 2023
Costs	Before September 23, 2023: • Author: € 520 • Members: € 520 • Non-members: € 565
www	https://www.eurosis.org/conf/esm/2023/index.html

Nr 449/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	**C4ISTAR: command, control, communications, computers,information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Administration in the Security System

Description	Administration in the Security System postgraduate studies focuses on the practical aspects of the operation of central and local government administration, with particular emphasis on the defence duties of public administration towards the local community. They are aimed at preparing students for the challenges (opportunities and threats) faced by public and private sector administration in the 21st century, including equipping students with the appropriate amount of knowledge necessary to perform specific administrative functions in government and local government bodies and to manage units organizational and auxiliary services of these local governments. The studies are delivered in Polish.
Organizer	Military University of Technology (Faculty of Security, Logistics and Management Military University of Technology)
Cooperation with	-
Duration	2 semesters
Thematic Scope	Legal basis of functioning of public administration, Administrative law, Administrative proceedings, Public administration in the security and defence system, Organization and tasks of government administration, Organization and tasks of local government administration, Military administration, Control in public administration, Public administration in state defense preparations, Crisis management system, HR management, Defense Benefits, Selected problems of functioning of EU bodies, Public finance and financial law, Public policies, Information security
Costs	PLN 3,800
No of ECTS credits	N/D
E-learning	-
Tools	-
Job opportunities	The offer is addressed to public administration employees, citizens and other entities performing tasks related to the security and defence of the state.
Additional info	-
www	https://irk.wat.edu.pl/en-gb/offer/SP_23_24/programme/AAAA5/?from=registration:SP_23_24

Nr 450/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Management in the Military Equipment Procurement System

Description	The offer is addressed to officers and employees of the military organizational units of the Ministry of National Defence dealing with the issue of obtaining military equipment. The studies are delivered in Polish.
Organizer	Military University of Technology (Faculty of Security, Logistics and Management Military University of Technology)
Cooperation with	-
Duration	2 semesters
Thematic Scope	The system of acquisition, operation and withdrawal of military equipment of the Polish Armed Forces, The life cycle of military equipment, Project management in the organization, Fundamentals of team management, Armament spending analysis, Arms market and defense technologies, Designing logistic systems and processes, Military equipment procurement system in NATO and the EU, Quality management systems in accordance with AQAP requirements in the process of acquiring military equipment, Prince 2 Foundation, Diploma seminar
Costs	PLN 4,800
No of ECTS credits	N/D
E-learning	No
Tools	-
Job opportunities	Graduates are prepared to: • carrying out managerial, programming and project tasks within the organizational structures of the Ministry of National Defences in the area of acquiring military equipment; • provide knowledge and skills-based support for the military equipment procurement system by adapting international standards and experience and creating a human resource competent in the management of programs and projects; • use of theoretical knowledge and practical skills based on project management in accordance with the PRINCE 2 Foundation methodology and quality management in the process of acquiring military equipment.
Additional info	-
www	https://wlo.wat.edu.pl/wp-content/uploads/2021/10/Zarzadzanie-w-systemie-pozyskiwania-sprzetu2022.pdf

Nr 451/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

MBA Cyber Security Management

Description	The studies allow students to gain in-depth knowledge, e.g. in the field of modern methods of managing organizations and their information resources, implementing information strategies in many aspects of cyber security, learning about legal issues related to cyber security, including dealing with an IT incident. Thanks to the studies, students will also learn about the latest technologies related to information security, securing resources and information, as well as managing IT security systems and assessing risk in the security of information systems of an organization.
Organizer	Military University of Technology (Faculty of Cybernetics)
Cooperation with	-
Duration	3 semesters
Thematic Scope	Cybersecurity systems, Protection of transactional and statistical databases, Managerial decisions, The theory of information warfare, Crisis management in cybersecurity, National Cybersecurity System, Cybersecurity risk management, NATO Cybersecurity Policy, Cybercrime, Project management and systems engineering in cybersecurity, IT service management, Cyber conflicts in international relations, Diploma seminar
Costs	PLN 17,900
No of ECTS credits	N/D
E-learning	No
Tools	-
Job opportunities	-
Additional info	-
www	https://irk.wat.edu.pl/en-gb/offer/SP_23_24/programme/WCYIXCNP/?from=org-unit:W5000

Nr 452/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

2nd International Forum on Artificial Intelligence and Robotics (ROBOTFORUM2024)

Description	ROBOTFORUM2024 feature plenary talks, keynote talks, special sessions, poster presentations, workshops, and contributed papers.
Goal	The aim of ROBOTFORUM2024 is to be a premier international forum to highlight novel developments, share new ideas, research results, and development experiences, and provide networking opportunities with peers to help establish connections for early-career scientists to meet a diverse mix of researchers, decision-makers to strengthen existing connections and forge new ones. Also, the main agenda of this conference is to bring together world-leading academics, practitioners, industry leaders, policymakers, and business professionals from the fields of Artificial Intelligence and Robotics to develop practical solutions for current challenges in these fields.
Organizer	Continuum Forums
Co-organizers/ Patrons	-
Topics	Artificial Intelligence and Applications, Machine Learning Methods, Robotic Aspects and their Applications, Bio-Inspired Robotics, Artificial Neural Networks, Medical Robots and Systems, Artificial Intelligence in Robotics, Education Robotics, Drones, Industrial Applications of Robotics, Aerial and Underwater Robotics, Rehabilitation Robotics, Emergency Assistance Robots, New Approaches in Robotics and Automation, Mechatronics, Bionics and Biomimetics, Importance of Modeling and Simulation in Internet of Things (IOT), Computer Vision, Human Computer Interaction, Nano Technology and Medical Applications, Machine Learning Research and Cybernetics, Artificial Intelligence in Education, Human-robot Interface, Hardware and Software Brains, Cognitive and Computational Intelligence, Design and Simulation of Robotics, Intelligent Systems for Communication Networks, Agricultural Automation, Energy and Environment-Aware Automation, Brain Machine Interface, Genetic Algorithms and Reinforcement Learning, Intelligent Mechatronics and Robotics, Intelligent Transportation Systems, Statistics and Computing
Date	June 17-19, 2024
Costs	Early Bird Registration (July 24, 2023): Speaker Registration $ 749, Delegate Registration $ 899, Poster Registration $ 449, Student $ 299, Exhibition $ 1500
www	https://www.continuumforums.com/2024/robotforum

Nr 453/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

International Conference on Unmanned Aircraft Systems, ICUAS '23

Description	ICUAS '23 offered unique opportunities to meet, interact and shape the future of unmanned aviation, worldwide, bringing together the technical, regulatory, and legal communities. ICUAS '23 included the UAV Competition.
Goal	ICUAS '23 aimed to bring together different groups of qualified representatives worldwide, funding agencies, industry, academia, end-users, and practitioners, to discuss the current state of unmanned aviation, and the roadmap to their full utilization in civilian and public domains.
Organizer	ICUAS Association, Inc.
Co-organizers/ Patrons	
Topics	Airspace Control, Airspace Management, Airworthiness, Autonomy, Biologically Inspired UAS, Certification, Control Architectures, Energy Efficient UAS, Environmental Issues, Fail-Safe Systems, Frequency Management, Integration, Interoperability, Levels of Safety, Manned/Unmanned Aviation, Micro- and Mini- UAS, Networked UAS, Payloads, Path Planning and Navigation, Reliability of UAS, Risk Analysis, See/Sense-Detect-and-Avoid Systems, Security, Sensor Fusion, Smart Sensors, Standardization, Technology Challenges, Training, UAS Applications, UAS Communications, UAS Testbeds, UAS Transportation Management (UTM)
Date	June 6 – 9, 2023
Costs	$325 - $660
www	https://uasconferences.com/2023_icuas/

Nr 454/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

23rd European Conference on Cyber Warfare and Security (ECCWS 2024)

Description	This conference attracts an interesting combination of academic scholars, military personnel, practitioners and individuals who are engaged in various aspects of the cyber security community. ECCWS is generally attended by participants from more than 30 countries. The Journal of Information Warfare regularly publishes a number of the papers presented at this conference.
Goal	The ECCWS provides a privileged forum for technical exchange about the study, management, development and implementation of systems and concepts to combat cyber warfare or to improve information systems security. There are several strong strands of research and interest that are developing in the area including the understanding of threats and risks to information systems, the development of a strong security culture, as well as incident detection and post incident investigation.
Organizer	Academic Conferences International
Co-organizers/ Patrons	-
Topics	• Critical Infrastructure Protection • Incident response strategies • Risk analysis and modelling • Gamification strategies for awareness/education and training • Cyber conflict • Cyber terrorism • Cyber security • Information warfare • Information warfare and security education • Information Assurance • Digital forensics • Psychological warfare
Date	27 - 28 June 2024
Costs	£280 - £425 (Physical Conference), £75 - £295 (Virtual Conference)
www	https://www.academic-conferences.org/conferences/eccws/

Nr 455/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

International Conference on Electronic Warfare and Sensor Systems (ICEWSS 2023)

Description	XVII. International Electronic Warfare and Sensor Systems is the premier interdisciplinary forum for the presentation of new advances and research results in the fields of Electrical and Computer Engineering.
Goal	International Conference on Electronic Warfare and Sensor Systems aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Electronic Warfare and Sensor Systems. It also provides a premier interdisciplinary platform for researchers, practitioners and educators to present and discuss the most recent innovations, trends, and concerns as well as practical challenges encountered and solutions adopted in the fields of Electronic Warfare and Sensor Systems.
Organizer	International Research Conference
Co-organizers/ Patrons	-
Topics	Electronic warfare, Electronic warfare applications, Electronic attack, Electronic protection, Electronic warfare support, Electromagnetic spectrum management, Electronic warfare environment, Kinetic and non-kinetic weapons, Developing the ability to recognize and electronic warfare, Image and optoelectronic based recognition, Radio recognition, defense and radio jamming, Monitoring and management of the electromagnetic spectrum, Signal processing, Data fusion and semantic processing, Sensor networks, The use of unmanned platforms, Devices and systems for electronic warfare, Electromagnetic compatibility and high-energy pulses, Defensive and offensive capabilities, Autonomous and semi-autonomous weapons, Swarm technology, Detection and countermeasures, Energy and laser weapons, Future warfare, Spectrum management and network enabled capability, Information operations, Cyber warfare, Cyber EM activities, Social media, Mining big data, Information operations and EW
Date	August 10-11, 2023
Costs	€ 300 - € 500
www	https://waset.org/electronic-warfare-and-sensor-systems-conference-in-august-2023-in-venice

Nr 456/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

SPIE Sensors + Imaging 2023

Description	SPIE Sensors + Imaging 2023 combines two of photonics conferences – SPIE Remote Sensing and SPIE Security + Defence.
Goal	The event showcases the latest sensor and photonic technologies for imaging and monitoring the Earth's atmosphere and environment, as well as sensor technologies that address homeland security, defence, and counterterrorism. Additionaly, the event gives the opportunity to meet face-to-face with top companies at the free 2-day exhibition.
Organizer	SPIE (Society of Photo-Optical Instrumentation Engineers)
Co-organizers/ Patrons	-
Topics	• Remote Sensing: Sensor and photonic technologies for imaging and monitoring the Earth's atmosphere and environments. • Security + Defence: Photonic technologies that address homeland security, defence, and counterterrorism.
Date	September 3 – 6, 2023
Costs	SPIE Member: €275-€630, Nonmember: €775
www	https://spie.org/conferences-and-exhibitions/sensors-and-imaging

Nr 457/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

2nd European Military Additive Manufacturing Symposium

Description	This symposium will address all the advantages and limitations of additive manufacturing from the perspective of industry, research and armed forces. It is setup to foster the mutual understanding of: what is already possible, what is expected to come in the future, where are the limits of the diverse stakeholders and what needs to be done to raise the treasure built in Additive Manufacturing.
Goal	This symposium aims to achieve higher visibility on certain levels and bring European stakeholders from military, industry and research together.
Organizer	German Association for Defence Technology - Centre for Studies and Conferences
Co-organizers/ Patrons	-
Topics	This symposium plan to focus on the following aspects: • Military Use Cases More than an increase in autonomy? • Industrial Solutions Capabilities of state of the art printers - what's useful for armed forces? • Best practice / experiences Industrial Use Cases and potential spillover effects. • Research Is there more to come? What's next? • QM / safety / human factors / education / legal aspects How to turn a piece of molded material into a usable product? • Circular Economy AM for military purpose: A potential contribution to circular economy?
Date	October 17-18, 2023
Costs	Public Services: 75,00 €, Research:280,00 €, Industries: 1190,00 €
www	https://eda.europa.eu/news-and-events/events/2023/10/17/default-calendar/2nd-european-military-additive-manufacturing-symposium

Nr 458/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

GLOBAL MILSATCOM 2023

Description	The 14th annual Cyber Security & Data Protection Summit is the central platform to build infrastructure resilience and to secure UK's Cyber capabilities to fight domestic and international threats. It brings together Cyber Security, Data Protection, Technology and Business leaders across Government, Public Sector and from highly regulated industries.
Goal	The conference has been specially designed for cyber security professionals across central and local government, the wider public sector and voluntary and non-profit organisations. It brings an agenda packed with case studies, expert insight and practical takeaways from across the public sector.
Organizer	GovNet Events
Co-organizers/ Patrons	-
Topics	• Cyber Culture • Skills and Training • Crime and Trends • Leadership and Recruitment • Emerging Technology
Date	15 November 2023
Costs	Public and Voluntary Sectors: FREE to Attend, Private Sector: £699 + VAT Per Delegate
www	https://cybersecuritysummit.co.uk/

Nr 459/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

12th International Conference on Natural Language Processing (NLP 2023)

Description	12th International Conference on Natural Language Processing (NLP 2023) is a programmed approach to analyze text that is based on both a set of theories and a set of technologies.
Goal	This forum aims to bring together researchers who have designed and build software that will analyze, understand, and generate languages that humans use naturally to address computers.
Organizer	International Conference on Natural Language Processing (NLP)
Co-organizers/ Patrons	-
Topics	• Chunking/Shallow Parsing • Dialog Systems • Discourse • Information Extraction • Information Retrieval • Lexical Semantics • Linguistic Resources • Machine Translation • Ontology • Paraphrasing/Entailment/Generation • Parsing/Grammatical Formalisms • Phonology, Morphology • POS tagging • Question Answering • Semantic Processing • Speech Recognition and Synthesis • Spoken Language Processing • Statistical and Knowledge based methods • Text Mining
Date	October 28-29, 2023
Costs	350 US Dollar (Estimated)
www	https://www.csen2023.org/nlp/index

Nr 460/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

ICCTAI 2023: 17. International Conference on Computational Techniques and Artificial Intelligence

Description	XVII. International Computational Techniques and Artificial Intelligence is the premier interdisciplinary forum for the presentation of new advances and research results in the fields of Computer and Information Engineering
Goal	International Conference on Computational Techniques and Artificial Intelligence aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Computational Techniques and Artificial Intelligence. It also provides a premier interdisciplinary platform for researchers, practitioners and educators to present and discuss the most recent innovations, trends, and concerns as well as practical challenges encountered and solutions adopted in the fields of Computational Techniques and Artificial Intelligence.
Organizer	WASET - World Academy of Science, Engineering and Technology
Co-organizers/ Patrons	
Topics	Circuit Modelling and Scientific Computing, Circuit Implementation for Fuzzy Systems, Computational Intelligence, Component based development, Computer Architecture and Computer Aided Design Computer and Information Technology, Computer Networks and Security, Computer Architectures and Digital Systems, Computer Vision and Pattern Recognition, Computer Systems and Networks, Control Systems and Robotics, Control Engineering, Data Mining and Management, Data Mining and Data fusion, Decision Support Systems, Databases and Data Mining, Distributed, mobile, and open architecture, Distributed and Parallel Systems, E-Learning & E-Business, Dynamical Systems, Fuzzy Logic and Circuits Design, Engineering of specific kinds of Information Systems, Fuzzy, ANN &, Expert Approaches, Fuzzy Systems, Grid and Cluster Computing, Genetic Algorithms, Human-Computer Interaction, Hierarchical Control Systems, Hybrid Systems, Human-Machine Systems, and more
Date	August 10-11, 2023
Costs	Listener Registration: € 300, Student Oral/Poster Presenter Registration: € 400, Non-Student Oral/Poster Presenter Registration: € 500
www	https://waset.org/computational-techniques-and-artificial-intelligence-conference-in-august-2023-in-barcelona

Nr 461/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Support for implementation of EU legislation on cybersecurity and national cybersecurity strategies

Financing entity	European Commission
Managing entity	-
Programme	Digital Europe Programme (DIGITAL)
Type of action	DIGITAL-JU-SIMPLE DIGITAL JU Simple Grants
Call	Deployment actions in the area of cybersecurity (DIGITAL-ECCC-2023-DEPLOY-CYBER-04)
Objectives of the call	The action focuses on capacity building and the enhancement of cooperation on cybersecurity at technical, operational and strategic levels, in the context of existing and proposed EU legislation on cybersecurity in particular the NIS2 Directive (Directive (EU) 2022/2555), the Cybersecurity Act and the proposed Cyber Resilience Act, and the Directive on attacks against information systems (Directive 2013/40). It complements the work of SOCs in the area of threat detection. It is a continuation of work currently supported under the previous WP. In addition, the action also aims at improving industrial and market readiness for the cybersecurity requirements set in the proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act bolstering cybersecurity rules to ensure more secure hardware and software products.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), • EEA countries (Norway, Iceland, Liechtenstein).
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	26 September 2023
Maximum amount/ Call budget	Call budget: EUR 30 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-eccc-2023-deploy-cyber-04-eulegislation

Nr 462/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Standardisation in the area of Cybersecurity

Financing entity	European Commission
Managing entity	-
Programme	Digital Europe Programme (DIGITAL)
Type of action	DIGITAL-JU-CSA DIGITAL JU Coordination and Support Actions
Call	Deployment actions in the area of cybersecurity (DIGITAL-ECCC-2023-DEPLOY-CYBER-04)
Objectives of the call	The objective of this topic is to support further standardisation in the area of cybersecurity, notably in view of the implementation of the proposed Regulation on the Cyber Resilience Act (CRA), in particular with a view to improving the awareness and engage stakeholders in such standardisation work. Expected outcome: • Organization of events, workshops, stakeholder consultations, and production of white papers, all fostering the development of harmonised standards and conformity with requirements stemming from above mentioned legislative framework. • Support for participation of relevant European experts in European and international cybersecurity standardization fora.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), • EEA countries (Norway, Iceland, Liechtenstein).
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	26 September 2023
Maximum amount/ Call budget	Call budget: EUR 3 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-eccc-2023-deploy-cyber-04-standardisation

Nr 463/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Coordination between the cybersecurity civilian and defence spheres

Financing entity	European Commission
Managing entity	-
Programme	Digital Europe Programme (DIGITAL)
Type of action	DIGITAL-JU-CSA DIGITAL JU Coordination and Support Actions
Call	Deployment actions in the area of cybersecurity (DIGITAL-ECCC-2023-DEPLOY-CYBER-04)
Objectives of the call	The objective is to enhance exchange and coordination between the cybersecurity civilian (including CSIRTs, law enforcement and cyber diplomacy communities) and defence spheres. This should in particular foster synergies between cybersecurity actions in Horizon Europe, Digital Europe and defence related actions carried out by the Union through its bodies and programmes, such as the European Defence Agency and the European Defence Fund. Expected outcome: • Concrete activities such as discussions, meetings, white papers, workshops, which strengthen the links between the cybersecurity civilian and defence spheres. • Synergies between these communities, such as common activities to exchange know-how and information.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), • EEA countries (Norway, Iceland, Liechtenstein).
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	26 September 2023
Maximum amount/ Call budget	Call budget: EUR 3 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-eccc-2023-deploy-cyber-04-civil-defence

Nr 464/2023

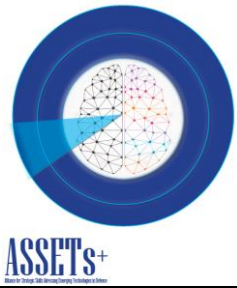
Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Preparedness support and mutual assistance

Financing entity	European Commission
Managing entity	-
Programme	Digital Europe Programme (DIGITAL)
Type of action	DIGITAL-JU-GFS DIGITAL JU Grants for Financial Support
Call	Deployment actions in the area of cybersecurity (DIGITAL-ECCC-2023-DEPLOY-CYBER-04)
Objectives of the call	This mechanism aims to complement and not duplicate efforts by Member States and those at Union level to increase the level of protection and resilience to cyber threats, by assisting Member States in their efforts to improve the preparedness for cyber threats and incidents by providing them with knowledge and expertise. The mechanism should also support mutual assistance between Member States for both preparedness and incident response actions. Expected outcome: • preparedness support services, • threat assessment and risk assessment services, • risk monitoring services, • mutual assistance among Member States.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), • EEA countries (Norway, Iceland, Liechtenstein).
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	26 September 2023
Maximum amount/ Call budget	Call budget: EUR 35 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-eccc-2023-deploy-cyber-04-support-assist

Nr 465/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Highly secure collaborative platform for aeronautics and security industry

Financing entity	European Commission
Managing entity	-
Programme	Digital Europe Programme (DIGITAL)
Type of action	DIGITAL-SIMPLE DIGITAL Simple Grants
Call	Cloud, Data and Artificial Intelligence (DIGITAL-2023-CLOUD-AI-04)
Objectives of the call	• A commercially viable highly-secure cloud-based collaborative platform for the management of industrial programmes in the aeronautics and security sector. • The governance implications that the operations of such a platform would have on the sector, notably how such platform can operate, be deployed, be accessed, and how projects can be managed through their lifecycle. • A significant contribution to the discussions for an EU-level single set of rules and accreditation for data sharing in the aeronautic and security sector.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), • EEA countries (Norway, Iceland, Liechtenstein), • countries associated to the Digital Europe Programme or countries which are in ongoing negotiations for an association agreement and where the agreement enters into force before grant signature.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	26 September 2023
Maximum amount/ Call budget	Call budget: EUR 22 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2023-cloud-ai-04-aerosec

Nr 466/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Network of safer Internet Centres (SICs)

Financing entity	European Commission
Managing entity	-
Programme	Digital Europe Programme (DIGITAL)
Type of action	DIGITAL-SIMPLE DIGITAL Simple Grants
Call	Accelerating the best use of technologies (DIGITAL-2023-DEPLOY-04)
Objectives of the call	• National SICs as a one-stop-shop for reliable and age-appropriate information. • Digital literacy in Member States and associated countries in formal and informal education settings. • Support to parents, carers, teachers, educators and other professionals working with children to better understand the risks and opportunities of children accessing digital content and services. • Timely information to local, national, and European actors on emerging risks through the helpline service. • Access to resources and services by public authorities, including law enforcement agencies, and exchanges with hotline analysts to develop better preventive measures and to remove online child sexual abuse material (CSAM). • Increased cooperation of the private sector with the SICs, including those recognised in the future as "trusted flaggers" to assist the public, in particular children, when confronted with harmful and illegal content.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories).
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	26 September 2023
Maximum amount/ Call budget	Call budget: EUR 16 200 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2023-deploy-04-network-of-sics

Nr 467/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Privacy-preserving and identity management technologies

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-IA HORIZON Innovation Actions
Call	Increased Cybersecurity 2023 (HORIZON-CL3-2023-CS-01)
Objectives of the call	• Improved scalable and reliable privacy-preserving and identity management technologies for federated and secure sharing and for processing of personal and industrial data and their integration in real-world systems; • Improving privacy-preserving technologies for cyber threat intelligence and data sharing solutions; • Contribution to promotion of GDPR compliant European data spaces for digital services and research as well as, contribution to the promotion of eID Regulation compliant European solutions; • Research and development of self-sovereign identity management technologies; • Provide resource efficient and secure digital identity solutions for Small and medium sized enterprises (SME); • Strengthened European ecosystem of open-source developers and researchers of privacy-preserving solutions; • Usability of privacy-preserving and identity management technologies.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	23 November 2023
Maximum amount/ Call budget	Call budget: EUR 15 700 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2023-cs-01-02

Nr 468/2023

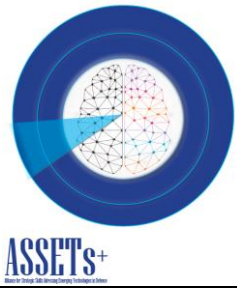
Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Facilitate the engagement in global ICT standardisation development

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-CSA HORIZON Coordination and Support Actions
Call	A human-centred and ethical development of digital and industrial technologies (HORIZON-CL4-2024-HUMAN-01)
Objectives of the call	• Set-up of a facility to support participation of European specialists in international ICT Standard Developing Organisations and global fora and consortia, which should increase the influence of Europe into ICT standardisation; • Develop and update sectorial ICT standardisation landscape and gap analysis of ICT standardisation needs in support of EU policies as outlined in the Rolling Plan for ICT standardisation; • Cooperate, synchronise and achieve capacity building with other similar initiatives or European players including from EU funded R&I projects; provide a forum for foresight analysis in different sectors; • Increase awareness on ICT standardisation development; • Financially support standardisation meetings in Europe of international SDOs and global fora and consortia.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	19 March 2024
Maximum amount/ Call budget	Call budget: EUR 6 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl4-2024-human-01-61

Nr 469/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Post-quantum cryptography transition

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-RIA HORIZON Research and Innovation Actions
Call	Increased Cybersecurity 2024 (HORIZON-CL3-2024-CS-01)
Objectives of the call	• Increasing the maturity of current post-quantum cryptographic algorithms and contribution to further standardisation; • Easy-to-use tools for the large-scale implementation of post-quantum cryptographic algorithms, based on state-of-the-art standards; • Secure and efficient transition from pre- to post-quantum encryption through tools implementing a hybrid approach combining recognised pre-quantum public key algorithms and additional post-quantum algorithms; • Phase-in of post-quantum algorithms or protocols to new or existing applications; • Demonstrators and good-practice implementations of post-quantum cryptographic algorithms on varied hardware and software platforms; • Application-oriented recommendations for the widespread implementation of post-quantum cryptography across the EU.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation5 have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	20 November 2024
Maximum amount/ Call budget	Call budget: EUR 23 400 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2024-cs-01-02

Nr 470/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Mitigating new threats and adapting investigation strategies in the era of Internet of Things

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-RIA HORIZON Research and Innovation Actions
Call	Fighting Crime and Terrorism 2024 (HORIZON-CL3-2024-FCT-01)
Objectives of the call	• Increased understanding of Police Authorities regarding the emerging (digital and especially physical) threats of the fast-developing environment of Internet of Things; • Modern tools to tackle new and emerging forms of crime pertaining to the development of Internet of Things are provided to European Police Authorities and other relevant security practitioners, which take into account legal and ethical rules of operation, EU fundamental rights such as privacy and protection of personal data as well as cost-benefit considerations; • Lawful access and exploitation of evidence in the environment of the Internet of Things are fortified; • Best practices (legal, organisational, technical) to access and exploit Internet of Things in the course of investigation are strengthened, including by developing relevant tools and training materials.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation5 have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	20 November 2024
Maximum amount/ Call budget	Call budget: EUR 5 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2024-fct-01-01

Nr 471/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Approaches and tools for security in software and hardware development and assessment

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-IA HORIZON Innovation Actions
Call	Increased Cybersecurity 2024 (HORIZON-CL3-2024-CS-01)
Objectives of the call	• Improved hardware and software security engineering; resilient systems design; • Improved access to testing of hardware and software in virtual, closed and secure environments; • Systematic and, where possible, automated study of vulnerabilities, software analysis, vulnerability discovery, and dynamic security assessment; • Trustworthy certifiable hardware and software; • AI-based security services e.g. predictive security, advanced anomaly and intrusion detection, system health checks.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation5 have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	20 November 2024
Maximum amount/ Call budget	Call budget: EUR 37 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2024-cs-01-01

Nr 472/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Interoperability for border and maritime surveillance and situational awareness

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON Lump Sum Grant [HORIZON-AG-LS]
Call	Border Management 2024 (HORIZON-CL3-2024-BM-01)
Objectives of the call	• Increased border surveillance capability, better performing and more cost-efficient, with data and fundamental rights protection by design; • Improved surveillance and situational awareness of sea borders, but also of maritime infrastructures as harbours and commercial and civilian maritime security, including in key areas such as the Arctic; • Improved multi-level, multi-authority and cross-border (among Member States and Associated Countries practitioners) collaboration thanks to better interoperability of sensing, analysis and common command-and-control C2 systems.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories), • EEA countries (Norway, Iceland, Liechtenstein).
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	20 November 2024
Maximum amount/ Call budget	Call budget: EUR 6 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2024-bm-01-02

Nr 473/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Innovative technologies for safety and excellence in decommissioning, including robotics and artificial intelligence

Financing entity	European Commission
Managing entity	-
Programme	Euratom Research and Training Programme (EURATOM)
Type of action	EURATOM-IA EURATOM Innovation Actions
Call	Nuclear Research and Training (HORIZON-EURATOM-2023-NRT-01)
Objectives of the call	Project results are expected to contribute to all of the following expected outcomes: • improve safety in the decommissioning of nuclear systems, minimising operational waste, dismantling waste and improving the environmental remediation of nuclear facilities; • fulfil decommissioning requirements of the Nuclear Safety Directive, Basic Safety Standards Directive and Radioactive Waste Management Directive; • contribute to excellence in decommissioning, while developing cutting-edge technological innovation, competitive and resilient industry initiatives, future-proof jobs and skills for a fair transition.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	08 November 2023
Maximum amount/ Call budget	Call budget: EUR 1 660 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-euratom-2023-nrt-01-07

Nr 474/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

European Digital Media observatory (EDMO) - National and multinational hubs

Financing entity	European Commission
Managing entity	-
Programme	Digital Europe Programme (DIGITAL)
Type of action	DIGITAL-SME Digital SME Support Actions
Call	Accelerating the best use of technologies (DIGITAL-2023-DEPLOY-04)
Objectives of the call	The objective of this topic is to finance the work of independent national/multinational hubs for analysis of digital media ecosystems in order to ensure the coverage of geographical areas covered by the EDMO hubs for which the funding is ending at the end of 2023 and in 2024.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: − be legal entities (public or private bodies) , − be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories (OCTs)), listed EEA countries and countries associated to the Digital Europe Programme or countries which are in ongoing negotiations for an association agreement and where the agreement enters into force before grant signature.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	26 September 2023
Maximum amount/ Call budget	Call budget: EUR 10 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2023-deploy-04-edmo-hubs

Nr 475/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Design of crisis prevention and preparedness actions in case of digital breakdown (internet, electricity etc.)

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-RIA HORIZON Research and Innovation Actions
Call	Disaster-Resilient Society 2023 (HORIZON-CL3-2023-DRS-01)
Objectives of the call	Projects' results are expected to contribute to some of the following outcomes: • Development of prevention/preparedness actions based on the (existing) analysis of interdependencies between critical infrastructures and possible cascading effects; • Analysis of existing communication systems and assessment/development of alternative communication tools for Civil Protection and Crisis Management security authorities, including the communication with private sector and actors responsible for critical infrastructures, as well as representatives of regional / local authorities and citizen organisations.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	23 November 2023
Maximum amount/ Call budget	Call budget: EUR 4 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2023-drs-01-02

Nr 476/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Capabilities for border surveillance and situational awareness

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-IA HORIZON Innovation Actions
Call	Border Management 2023 (HORIZON-CL3-2023-BM-01)
Objectives of the call	Examples of technologies and approaches that can be explored by the research projects include (non-prescriptive and non-exhaustive): networked deployable, and possibly mobile, semi-autonomous surveillance towers; IoT and advanced mesh connectivity; Virtual and Augmented Reality for enhanced C2 and situational awareness; integrated wide area RPAS management; advanced sensors for geolocalisation; passive, low-energy systems; artificial intelligence. Equipment and technologies enabling border surveillance should contribute to cost and energy efficiency, limit their environmental impact and be more and more sustainable once operational in the future. This may be addressed, for example, by integrating opportunities of circular economy, self-sustained equipment, lower emissions and/or environmental footprints. The proposed solutions should include, by design, the protection of fundamental rights such as privacy, and/or the application of privacy-enhancing technologies. They should also ensure secure data collection, access, encryption and decision support processes.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	23 November 2023
Maximum amount/ Call budget	Call budget: EUR 8 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2023-bm-01-01

Nr 477/2023

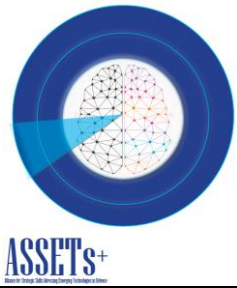
Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Interoperability of systems and equipment at tactical level; between equipment and databases; and/or between databases of threats and materials

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-IA HORIZON Innovation Actions
Call	Border Management 2023 (HORIZON-CL3-2023-BM-01)
Objectives of the call	Projects' results are expected to contribute to some or all of the following outcomes: • Increased interoperability of existing (and foreseeable upcoming) customs control equipment at tactical level, multi-supplier, multi-authority and cross-border; • More efficient and quicker availability, for EU customs practitioners, of reference data (such as spectra) on threats and dangerous and/or illicit materials; • Building capabilities for a more harmonised European application of customs controls based on risk management and trade facilitation.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	23 November 2023
Maximum amount/ Call budget	Call budget: EUR 6 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2023-bm-01-04

Nr 478/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

System approach for grid planning and upgrade in support of a dominant electric mobility (vehicles and vessels) using AI tools

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-IA HORIZON Innovation Actions
Call	Sustainable, secure and competitive energy supply (HORIZON-CL5-2023-D3-03)
Objectives of the call	• AI-based prediction of most convenient locations that optimize grid resources and upgrades around recharging pools for EVs and electric HDVs. • Developing of spatial mapping models and software tool for location decision-making with a comprehensive focus, including major highways, industrial zones, urban nodes and less-densely populated areas. • Simulation, analysis, design, test and demonstration of smart and bidirectional charging schemes and their integration into flexibility markets. • Exploration of the impact of different charging methods. • Analysis, design, testing and developing of a cybersecurity model that can simulate and accurately represent attack propagation from recharging infrastructure entry vectors, informing the development of efficient strategies and lines of defence to mitigate these vulnerabilities for the different relevant stakeholders.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	10 October 2023
Maximum amount/ Call budget	Call budget: EUR 11 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl5-2023-d3-03-03

Nr 479/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

EIC Accelerator Challenge: Customer-driven, innovative space technologies and services

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-EIC-ACC-BF HORIZON EIC Accelerator Blended Finance
Call	EIC Accelerator 2023 (HORIZON-EIC-2023-ACCELERATOR-01)
Objectives of the call	In terms of technological developments, the specific objectives of this Challenge are: • To have the means to inspect spacecraft in orbit, to augment satellite capabilities and resilience; • To develop autonomous and in-space collision avoidance capabilities e.g., use of Artificial Intelligence/Machine Learning for collision avoidance manoeuvres and develop in-space mobility propulsion capabilities; • To collect space debris with a view for recycling, recovering and transforming purposes (e.g., microgravity platforms) and to design and construct a R&I low Earth orbit unmanned platform assembled in orbit and to host in-orbit microgravity experiments or collect/re-use space debris; • To scale up disruptive innovations for space situational awareness (SSA), in-space logistics, Earth observation, navigation, satellite communications (SATCOM), and others.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	11 January 2023, 22 March 2023, 21 June 2023, 04 October 2023 (multiple cut-off)
Maximum amount/ Call budget	Call budget: EUR 1 135 239 839
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-eic-2023-acceleratorchallenges-07

Nr 480/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Security of robust AI systems

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-RIA HORIZON Research and Innovation Actions
Call	Increased Cybersecurity 2023 (HORIZON-CL3-2023-CS-01)
Objectives of the call	More specifically, proposals should contribute to the achievement of one or more of the following impacts: • Strengthened EU cybersecurity capacities and European Union sovereignty in digital technologies • More resilient digital infrastructures, systems and processes • Increased software, hardware and supply chain security • Secured disruptive technologies • Smart and quantifiable security assurance and certification shared across the EU • Reinforced awareness and a common cyber security management and culture.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	23 November 2023
Maximum amount/ Call budget	Call budget: EUR 15 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2023-cs-01-03

Nr 481/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

ATM Excellent science and outreach for Artificial Intelligence (AI) for aviation

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-JU-RIA HORIZON JU Research and Innovation Actions
Call	Digital European Sky Exploratory Research 02 (HORIZON-SESAR-2023-DES-ER-02)
Objectives of the call	Project results are expected to contribute to the following expected outcomes: • Environment: the proposed solutions shall have a positive impact on the environment and on the aviation environmental footprint; • Capacity: AI will play a fundamental role in aviation/ATM to address airspace capacity shortages; • Operational efficiency: the proposed solutions are expected to improve the synchronisation and predictability of the ATM system; • Cost efficiency: AI will enrich aviation datasets with new types of datasets unlocking air/ground AI-based applications; • Safety: the proposed solutions are expected to maintain at least the same level of safety as the current ATM system; • Security: the proposed solutions are expected to maintain at least the same level of security as the current ATM system.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	15 November 2023
Maximum amount/ Call budget	Call budget: EUR 9 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-sesar-2023-des-er2-wa1-8

Nr 482/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

ATM application-oriented research for Artificial Intelligence (AI) for aviation

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-JU-RIA HORIZON JU Research and Innovation Actions
Call	Digital European Sky Exploratory Research 02 (HORIZON-SESAR-2023-DES-ER-02)
Objectives of the call	Project results are expected to contribute to the following expected outcomes. • Environment: the proposed solutions are expected to demonstrate the positive impact of AI-based solutions on operational mitigation of aviation's environmental impact. • Capacity: the proposed solutions are expected to contribute to capacity by addressing AI-based human operator support tools to, for example, ensure the integration of new entrant aircraft types. • Operational efficiency: the proposed solutions are expected to improve the operational efficiency by enabling better traffic predictions and forecasts, thus contributing to punctuality. • Safety: the proposed solutions are expected to maintain at least the same level of safety as the current ATM system. • Security: the proposed solutions are expected to maintain at least the same level of security as the current ATM system.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	15 November 2023
Maximum amount/ Call budget	Call budget: EUR 9 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-sesar-2023-des-er2-wa2-4

Nr 483/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Beyond the horizon: A human-friendly deployment of artificial intelligence and related technologies

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-RIA HORIZON Research and Innovation Actions
Call	A sustainable future for Europe (HORIZON-CL2-2024-TRANSFORMATIONS-01)
Objectives of the call	Projects should contribute to all of the following expected outcomes: • Understanding and awareness raising about successful existing deployment of AI and the impact they have on European economy and society, providing a reality check of capabilities/benefits, but also limitations of current AI solutions, and how the latter are currently addressed. • On the basis of lessons from successful deployment, analysis of the implementation of the ethics principles for trustworthy AI. • Structurally enhanced capacities to foresee, evaluate and manage the future and longer term opportunities and challenges associated with artificial intelligence and related technologies. • Well founded and prioritised recommendations for European policy on R&I and in other key areas.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	07 February 2024
Maximum amount/ Call budget	Call budget: EUR 10 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl2-2024-transformations-01-06

Nr 484/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

AI for advanced and collective perception and decision making for CCAM applications (CCAM Partnership)

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-RIA HORIZON Research and Innovation Actions
Call	Safe, Resilient Transport and Smart Mobility services for passengers and goods (HORIZON-CL5-2024-D6-01)
Objectives of the call	Project results are expected to contribute to all of the following expected outcomes: • Advanced collective awareness, decision making and triggering of actions for Connected, Cooperative and Automated Mobility (CCAM) applications, enabled by new concepts and tools built on advancements in Artificial Intelligence (AI), including Hybrid Intelligence (HI). • CCAM solutions evolving from reactive into predictive system state awareness, decision making and actuation, enhancing road safety. • Understanding of AI-related ethical issues and user needs. • Increased user acceptability and societal benefit of CCAM solutions, based on explainable, trustworthy and human-centric AI. Interactions with AI-based vehicles are understandable, human-like and reflect human psychological capabilities.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	05 September 2024
Maximum amount/ Call budget	Call budget: EUR 10 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl5-2024-d6-01-04

Nr 485/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

AR/VR-empowered digital twins for modelling complex phenomena in new RI application areas

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-RIA HORIZON Research and Innovation Actions
Call	Next generation of scientific instrumentation, tools, methods, and advanced digital solutions for RIs (2024) (HORIZON-INFRA-2024-TECH-01)
Objectives of the call	The aim of this topic is to deliver digital twin solutions which advance the state-of-art of European RIs and show transformative potential in RI operations. The solutions should pave way for new ways to conduct experiments by the RIs through AR/VR (augmented reality/virtual reality) empowered digital twins. Mixed reality (XR) technologies can also be considered. The focus is on newer application areas, such as healthcare, safety and security, to understand complex real-world systems, particularly in application areas constrained by specific physical limitations (like radiation, pressure or temperature).
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	12 March 2024
Maximum amount/ Call budget	Call budget: EUR 24 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-infra-2024-tech-01-04

Nr 486/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Centralised, reliable, cyber-secure & upgradable in-vehicle electronic control architectures for CCAM connected to the cloud-edge continuum (CCAM Partnership)

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-RIA HORIZON Research and Innovation Actions
Call	Safe, Resilient Transport and Smart Mobility services for passengers and goods (HORIZON-CL5-2024-D6-01)
Objectives of the call	• New, centralised, reliable, cyber-secure and upgradable in-vehicle electronic control architectures for CCAM (Connected, Cooperative and Automated Mobility). • Widespread deployment of level 4 automation in road vehicles by expanding the Operational Design Domains (ODDs) of the control system towards higher complexity or greater scale. • Safe operation of Connected and Automated Driving (CAD) functions through system agility, experience-based decision making and access to cloud intelligence. • Paradigm shift from human-based and component-supported vehicle control to a more integrated, resource efficient and reliable system for the control of CCAM systems. • Strengthened cooperation of European OEMs and suppliers to co-design a standard cyber secure electronic architecture layout with harmonised interfaces.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	05 September 2024
Maximum amount/ Call budget	Call budget: EUR 12 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl5-2024-d6-01-01

Nr 487/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Fundamentals of Software Engineering (RIA)

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-RIA HORIZON Research and Innovation Actions
Call	Digital and emerging technologies for competitiveness and fit for the Green Deal (HORIZON-CL4-2024-DIGITAL-EMERGING-01)
Objectives of the call	• Methods, mechanisms and tools that allow smart intelligent system specification, agile system and code development, advanced code analysis, fault prediction and location and self-repair by using emerging techniques, in particular based on AI and data technologies. This may include environments that allow to automatically derive requirements and produce conceptual and architectural models. Tools should support mastering complex requirements, design-by-contract programming at all levels of integration, semi-automatic creation of pre-conditions, post-conditions and invariants for software modules facilitating automated unit and integration testing. • Methods and tools for the development of dynamic and resilient software for systems running on multiple processing architectures including cross-compilation, run-time self-adaptation and multi-architecture executables.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	19 March 2024
Maximum amount/ Call budget	Call budget: EUR 13 500 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl4-2024-digital-emerging-01-22

Nr 488/2023

Fiche develop in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Collaborative intelligence – combining the best of machine and human (AI Data and Robotics Partnership) (RIA)

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-RIA HORIZON Research and Innovation Actions
Call	A human-centred and ethical development of digital and industrial technologies (HORIZON-CL4-2024-HUMAN-01)
Objectives of the call	• Demonstrate the value of human-machine collaboration and interaction by improved effectiveness, intuitiveness, efficiency, completeness, limits of knowledge indication and other objective or quantifiable subjective measures. • Demonstrate how collaborative decision-making improves over human decision-making and that the collaborative decisions cover all stages of reasoning (that they are based on an improved coverage of data and knowledge sources, on an improved analytic ability to reason from input to output, and on a well-communicated decision).
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	19 March 2024
Maximum amount/ Call budget	Call budget: EUR 20 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl4-2024-human-01-07

Nr 489/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Integrated risk-based border control that mitigates public security risk, reduces false positives and strengthens privacy

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-IA HORIZON Innovation Actions
Call	Border Management 2024 (HORIZON-CL3-2024-BM-01)
Objectives of the call	Projects' results are expected to contribute to some or all of the following outcomes: • Improve assisted border crossing control systems, coordinated between border, customs and security controls; • Allocate more efficiently border check resources, maintaining security while minimising time and hassle for crossings and false positives; • Allocate flexibly border check resources, when and where needed, depending on changing needs (for example seasonally, and/or in the case of roll-on-roll-off ferries); • Contribute to capabilities that strengthen the Schengen area, by providing security at its external borders that also reassure on maintaining the free movement within its borders.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	20 November 2024
Maximum amount/ Call budget	Call budget: EUR 5 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2024-bm-01-04

Nr 490/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Cost-effective sustainable technologies and crisis management strategies for RN large-scale protection of population and infrastructures after a nuclear blast or nuclear facility incident

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-RIA HORIZON Research and Innovation Actions
Call	Disaster-Resilient Society 2024 (HORIZON-CL3-2024-DRS-01)
Objectives of the call	• Improved understanding of the radioactive fallout and methodology regarding robust and rapid monitoring of dose rate and nuclide specific determination with purpose of facilitating safe evacuation after a nuclear or radiological event; • Improved tools and methods for risk assessment following a nuclear or radiological event and optimized actions after a disaster; • Identification of the relevant range of different protective measures, including medical countermeasures, needed after a RN disaster, and improved protection of population and infrastructures through better analysis of sensor data resulting in adequate protective actions; • Improved understanding of contamination and decontamination of population and infrastructure after a RN-incident; • Recommendations on integration of improved technologies and assessment methodologies in the RN crisis managements systems;
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	20 November 2024
Maximum amount/ Call budget	Call budget: EUR 6 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2024-drs-01-05

Nr 491/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Identify, inspect, neutralise Unexploded Ordnance (UXO) at sea

Financing entity	European Commission
Managing entity	-
Programme	Horizon Europe Framework Programme (HORIZON)
Type of action	HORIZON-RIA HORIZON Research and Innovation Actions
Call	Border Management 2023 (HORIZON-CL3-2023-BM-01)
Objectives of the call	Projects' results are expected to contribute to some or all of the following outcomes: • Increased capabilities to detect, classify, inspect, assess and neutralise UXO at sea; • Improved safety and security for maritime economic operators and for EU citizens.
Who can apply?	Any legal entity, regardless of its place of establishment, including legal entities from nonassociated third countries or international organisations is eligible to participate, provided that the conditions laid down in the Horizon Europe Regulation have been met, along with any other conditions laid down in the specific call topic.
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	23 November 2023
Maximum amount/ Call budget	Call budget: EUR 5 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2023-bm-01-02

Nr 492/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project, **Funding opportunities**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Long-range indirect fire support capabilities for precision and high efficiency strikes

Financing entity	European Commission
Managing entity	-
Programme	European Defence Fund
Type of action	EDF-DA EDF Development Actions
Call	Call for EDF development actions implemented via actual cost grants (EDF-2023-DA)
Objectives of the call	The objective of this study is to develop European solutions for 155mm (up to 52-calibre) and rocket artilleries adapted to the new threats by increasing the fire range compared to current systems while maintaining interoperability principle. The targeted solutions must be cost-driven based on the assumption of a symmetric high intensity battle.
Who can apply?	In order to be eligible, the applicants (beneficiaries and affiliated entities) must: • be legal entities (public or private bodies), • be established in one of the eligible countries, i.e.: EU Member States (including overseas countries and territories (OCTs)), non-EU countries (listed EEA countries, have their executive management structure established in eligible countries, must not be subject to control by a non-associated third country or nonassociated third-country entity).
How to apply?	Electronically via the Founding & Tenders Portal Electronic Submission System
Duration	-
Deadline	22 November 2023
Maximum amount/ Call budget	Call budget: EUR 714 500 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2023-da-ground-ifs

Nr 493/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Surveillance and Reconnaissance Techniques for Chemical and Biological Threats

Description	In Europe, there are still technological gaps in several aspects of the CBRN Security Cycle and specifically in the devices for rapid detection, identification and monitoring of low-volatile chemical warfare agents and non-volatile biological warfare agents, mainly in complex natural environments. Benchmark technologies, including IMS, GC-IMS, and Py-GC-IMS, can sample and identify the most volatile CWAs within seconds (IMS) or BWAs within minutes, even at low ppbV concentration levels, but cannot detect extremely low doses of low-volatile toxic fourth generation CWAs, nor can they differentiate biological fragments from harmless substances. To overcome these gaps, it is necessary to develop new highly selective and sensitive detectors with detection limits in the pptV range, operated at elevated temperatures (>200°C) to prevent condensation of low volatile constituents, high 2D resolving power and robust analytical methods.
Goal	TeChBioT aims for the development of a universal detection technology based on high-temperature ion mobility spectrometry with optional gas chromotographic pre-separation and pyrolysis for enabling fast detection and identification of nonvolatile biological and low-volatile chemical agents. The innovative technology is combined with Artificial Intelligence and Deep Learning models to reduce the dimensionality of the 2D spectral data and enable distinguishing of bacteria, fungi, viruses, low volatile chemical warfare agents, and toxic industrial compounds at pptV concentration levels based on their unique fingerprint within a complex environment.
Lead Partner	ECOLE ROYALE MILITAIRE - KONINKLIJKE MILITAIRE SCHOOL
Partners involved	GOTTFRIED WILHELM LEIBNIZ UNIVERSITAET HANNOVER, T4I ENGINEERING SINGLE MEMBER PRIVATE COMPANY, ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS, TALLINNA TEHNIKAÜLIKOOL, BUNDESMINISTERIUM DER VERTEIDIGUNG, EXUS SOFTWARE MONOPROSOPI ETAIRIA PERIORISMENIS EVTHINIS, INTERSCIENCE BV
Duration	01 December 2022 - 30 November 2025
Results	-
Funding	€ 4,328,983.75
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103176/EDF https://defence-industry-space.ec.europa.eu/system/files/2022-07/Factsheet_EDF21_TeChBioT.pdf

Nr 494/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Small Satellite for Geostationary Earth Orbit Space Situation Awareness

Description	NAUCRATES is the scientific name for the Pilot Fish. The scope of Naucrates is to design and manufacture the technological demonstrator of a satellite intended for optical intelligence of Geostationary Earth Orbit (GEO) resident objects. GEO allows a satellite to remain in orbit over a single point of the earth's surface. Seven uses for GEO have been set forth by the UN Committee on Peaceful Uses of Outer Space: communications, meteorology, earth resources and environment, navigation and aircraft control, astronomy and data relay. Hence, GEO needs special control and protection. US Air Force with the declassified Geosynchronous Space Situational Awareness Program, Russia, and China have these capabilities. Europe, with its fleet of GEO satellites, both military and commercial, should develop satellites designed to monitor at least its own satellites.
Goal	The project NAUCRATES aims at designing and demonstrating a microsatellite as an in orbit optical sensor with the capability to approach other objects in GEO till 10km to take centimetre resolution images. It will be positioned in a stable orbit outside GEO belt, will not create harm to other satellite nor disturb the transmissions. NAUCRATES will not be visible by ground radars, telescopes or SIGINT. The NAUCRATES payload is based on an optical telescope. The acquired images will be transmitted via infrared laser at 2 Gbit/s with a contact duration < 2 min on a ground spot signal of few hundred meters impossible to be eavesdropped. NAUCRATES satellite can be launched directly in GEO by Ariane 6 and could stay in orbit for a 3 to 5 years. NAUCRATES is the first GEO satellite with a mass lower than 100kg, the first stealth satellite and the first European satellite for SSA in GEO. This is the first SMEs team to offer a GEO satellite designed and manufactured in Europe.
Lead Partner	ON-AIR CONSULTING & SOLUTIONS SRL
Partners involved	IMT SRL, SPACE TECHNOLOGIES FOR INNOVATION S.R.L., OPTEC SPA, BRADFORD ENGINEERING BV, SYSTEMS DEVELOPMENT & SUPPORT SRL, INTEGRASYS SA, TEKEVER SPACE - SISTEMAS ESPACIAIS LDA, TTI NORTE SL, CELESTIA SATELLITE TEST ANDSIMULATION BV, HYPERION TECHNOLOGIES BV
Duration	01 December 2022 - 30 November 2025
Results	-
Funding	-
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101102517/EDF

Nr 495/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Augmented Capability for High End Soldiers

Description	ACHILE is aimed at bringing a breakthrough transformation for soldier systems, through an open architecture developed for the Preparatory Action Plan on Defence Research (PADR). It will seek to demonstrate enhanced interchangeable capabilities improving all areas of dismounted combat: survivability, sustainability, mobility, localization and navigation, perception and situational awareness, lethality/smart engagement and communication. ACHILE will develop specific capabilities in four main areas: Soldier Core and Soldier Extension to address capabilities at soldier level, and Team Core and Team Extension to address squad and networking capabilities, as well as robotics and weapon interaction at team level.
Goal	• Better protection for soldiers, with lighter equipment and improved ergonomics, a modular approach and optimized Size, Weight And Power (SWAP) capability up to the system level. • Enhanced soldier performance, in particular for visual and sound perception, and individual situational awareness. • Augmented team capabilities through network connectivity, shared situational awareness, and coordination with all other units on the battlefield.
Lead Partner	SAFRAN ELECTRONICS & DEFENSE
Partners involved	RHEINMETALL ELECTRONICS GMBH, INDRA SISTEMAS SA, LEONARDO - SOCIETA PER AZIONI, TALGEN CYBERSECURITY OU, THALES SIX GTS FRANCE SAS, THALES LAS FRANCE SAS, ELNO, MICROOLED SARL, SIMSOFT3D, EYELIGHTS, BLACKNED GMBH, GMV AEROSPACE AND DEFENCE SA, GOGOA MOBILITY ROBOTS SL, AMOPACK SL, LARIMART SPA, FABBRICA D'ARMI PIETRO BERETTA – SPA, STAM SRL, ISTITUTO AFFARI INTERNAZIONALI, EPIC BLUE, FN HERSTAL SA, WOJSKOWA AKADEMIA TECHNICZNA IM.JAROSLAWA DABROWSKIEGO, SKA POLSKA SPOLKA Z OGRANICZONA ODPOWIEDZIALNOSCIA, EXOFRAME SPOLKA Z OGRANICZONA ODPOWIEDZIALNOSCIA, ITTI SP ZOO, NFM Group AS, BSS aps
Duration	01 December 2022 - 31 January 2027
Results	-
Funding	€ 40 000 000
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103558/EDF https://www.safran-group.com/pressroom/achile-project-european-dismounted-soldier-system-community-ready-start-design-next-generation-2023-06-09

Nr 496/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

High Efficiency Read Out Circuits

Description	Many defence applications rely on Infrared (IR) optronics systems to detect, recognise, and identify objects or targets during night and day. These systems are composed of IR sensors able to detect electromagnetic radiation within a wavelength spectrum different from the visible one. At the heart of the IR sensor lies the Focal Plane Array, broken down into two functional layers, the detection layer and the Read-Out Integrated Circuit. The key features of a ROIC are to provide the electrical interface between each individual detector pixel and its associated readout circuit and to convert the signals provided by the pixel readout circuit into a digital equivalent that can be provided to the sensor output and acquired by the external driving electronics. Currently the mainstream sizes of IR sensors for defence applications are between VGA format and SXGA format and pixel pitch distance between 20 µm and 10 µm. The next generations of IR systems will require longer detection, recognition and identification ranges, large field of views, faster frame rates and higher performance.
Goal	The HEROIC ambition is to enable European IR sensor suppliers to sustainably design the next generation of EU ROICs for IR sensors for defence applications. HEROIC unites, from across EU, different complementary players in the supply chain, including key system manufacturers and IR technology providers. HEROIC represents a first phase in the securing of the availability of a common advanced fully EU ROIC supply chain compatible with various IR detector technologies and 2D/3D architectures by 2030.
Lead Partner	LYNRED
Partners involved	AIM INFRAROT-MODULE GMBH, XENICS NV, COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES, INTEGRATED DETECTOR ELECTRONICS AS, UNIVERSIDAD DE SEVILLA, INDRA SISTEMAS SA, KONGSBERG DEFENCE & AEROSPACE AS, PCO SA, MILTECH HELLAS BIOMICHANIA EMPORIOANTIPROSOPEIES ILEKTRONIKON OPTIKON KAI MICHANOLOGIKON EIDON AE
Duration	01 January 2023 - 31 December 2026
Results	-
Funding	€ 17,999,998.00
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101102939/EDF https://defence-industry-space.ec.europa.eu/system/files/2022-07/Factsheet_EDF21_HEROIC.pdf

Nr 497/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Hydrogen Battlefield Reconnaissance and Intelligence Drone

Description	UAVs are a mandatory asset for preparing and conducting military operations. Despite the gains they allow for conducting Intelligence, Surveillance and Reconnaissance missions, UAVs suffer from major shortcomings in terms of operational deployment. Currently, fixed wing tactical drones are either electric with limited range or powered with internal combustion engines that are noisy and needs intensive maintenance. They also rely on a cumbersome catapult launcher for take-off, have no flight clearance over populated areas and limited resistance to harsh battlefield. HYBRID aims at bringing to the EU defence market a battlefield ready, long endurance and easy to use fixed-wing drone with vertical take-off and landing capability.
Goal	HYBRID aims to develop an electric hydrogen fuel cell-powered drone with state-of-the-art avionics, ruggedized into all kinds of threats and environments, equipped with an innovative automated video detection algorithm to reduce the operator workload. The differentiating factor of HYBRID is to offer all these features in an easy to use, compact package. First, partners will define the system's overall architecture and derive the specifications of all sub-assemblies, subsystems, and components. Then, partners will implement Vertical Take-off and Landing capability, ruggedize the airframe, design high-end ruggedized electronics and object recognition features. In the end, the integration will be carried out to conduct a test campaign in real conditions with representative end-users.
Lead Partner	DELAIR
Partners involved	ALFATEC GROUP D.O.O., ISD LYSEIS OLOKRIROMENON SYSTIMATONANONYMOS ETAIREIA
Duration	01 December 2022 - 30 November 2025
Results	-
Funding	€ 3,163,713.94
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101102411/EDF https://defence-industry-space.ec.europa.eu/system/files/2022-07/Factsheet_EDF21_HYBRID.pdf

Nr 498/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Fluidic Actuators for Control of stEaLth aIrcraFT

Description	The FACELIFT project aims to improve strategic surveillance capability, survivability and operational resilience for future stealth aircraft, which will be more stealthy and more maneuverable than the current generation of military assets such as the European MALE-RPAS. This will be achieved using fluidic actuators (sweeping jets and synthetic jets) integrated in front of the wing control surfaces. These control surfaces will then be more efficient and can be downsized thus reducing the Radar Cross Section.
Goal	Two types of actuators will be considered: sweeping jets and synthetic jets. It is expected that the implementation of closed-loop controlled fluidic actuators will deliver a 50 % decrease of the Radar Cross Section originating from a control surface for the same maneuverability by area reduction. Considering stabilising surfaces, such as a fin, it is expected that the area may be halved, which on the aircraft level may contribute up to a 30 % reduction of the RCS. By using synthetic jet actuators, the IR signature will not be impacted due to its electric power source.
Lead Partner	CEDRAT TECHNOLOGIES SA
Partners involved	ESC DEFENCE S.R.O., NAVASTO GMBH, OFFICE NATIONAL D'ETUDES ET DE RECHERCHES AEROSPATIALES
Duration	01 December 2022 - 30 November 2025
Results	-
Funding	-
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101102557/EDF https://cedrat-technologies.com/wp-content/uploads/2023/06/facelift-project-presentation.pdf

Nr 499/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Space Response to Risk & Integration with Ground segment

Description	SPRING is a European SMEs-led project which will study the military specificities of a spacecraft automated reactivity in respect of a threat. It will integrate a communication chain between the ground segment and the flight segment, automated threat assessment on ground, and semi automated maneuvers calculated on-board. The project will demonstrate how to increase the safety and reactivity of military space systems through avoiding collision or close encounter with a hostile spacecraft. The project will result in the first ever integrated calculation & communication chain between ground and flight segments, able to send a countermeasure to a spacecraft in a very low short time following the detection of a threat. Following this countermeasure uplink, the spacecraft will react accordingly in a semi-autonomous to autonomous manner. Space-based recorded data, specific to military assets and requirements for identification, is sent to the ground segment for further automated threat assessment, further reaction scenarios recommendation and cataloguing in a specific Space Situational Awareness catalogue.
Goal	The overall objective is to develop an integrated solution for semi-automatised calculation and communication between ground detection, ground-based threat assessment and reaction scenarios recommendation, interfacing with military C2 and the flight segment for space-based object surveillance and autonomous planning.
Lead Partner	SHARE MY SPACE
Partners involved	SYBILLA TECHNOLOGIES SPOLKA Z OGRANICZONA ODPOWIEDZIALNOSCIA, NURJANA TECHNOLOGIES SRL, LMO, AIKO SRL,
Duration	01 December 2022 - 30 November 2024
Results	-
Funding	€ 3,675,873.69
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103509/EDF https://defence-industry-space.ec.europa.eu/system/files/2022-07/Factsheet_EDF21_SPRING.pdf

Nr 500/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

High Instantaneous Dynamic Range Direct RF sampling modular chiplet Architecture

Description	The project "High Instantaneous Dynamic Range Direct RF sampling modular chiplet Architecture" (HIDRA) offers to execute studies and design regarding Digital Signal Processing for Software Defined Radio.
Goal	The project will result in a modular chiplet architecture with carefully co-designed components leveraging best IC technologies for specific parts of the RF signal chain comprising direct RF sampling chiplet and high RF power handling chiplet. The project provides a viable path towards addressing one of the European technology shortfalls in the key area of semiconductor data converters for defense applications. It will strengthen the security of supply and contribute to European non-dependence by leveraging strength of current European leadership in advanced node FD SOI fabrication processes coupled with European GaN on SiC capabilities and know-how.
Lead Partner	BEYOND SEMICONDUCTOR, RAZISKAVE IN RAZVOJ, D.O.O.
Partners involved	BALTIJOS PAZANGIU TECHNOLOGIJU INSTITUTAS, UNIVERZA V LJUBLJANI, UNIVERSITE DE BORDEAUX, CONTINIUM TECHNOLOGIES S.R.O., ADVICO MICROELECTRONICS GMBH
Duration	01 December 2022 - 31 July 2026
Results	-
Funding	€ 3,996,992.42
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103423/EDF https://defence-industry-space.ec.europa.eu/system/files/2022-09/Factsheet_EDF21_HIDRA.pdf

Nr 501/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Live Operational Data Enhancement for Situational Awareness Through Augmented Reality

Description	The research is focussed on innovations related to the following three characteristics: human-centric, seamlessly interoperable, enabling operations under all conditions. In the initial (study) phase of the project, a comprehensive overview of the state of relevant technological advances related to edge AI and AR will be established, relevant operational scenarios and mission profiles (with participation of the 4 MoDs) will be defined and insights related to soldier system architectural frameworks will be updated. Research work will include fusion of image from multiple sensors, automated (AI-based) detection of activity and stance of the soldier (used to make the soldier-machine interface adaptive) and multi-modal AR interfaces operating across weapons scope and helmet.
Goal	The LODESTAR project aims to define additional recommendations (compatible with GOSSRA and STANREC 4845 and building on top of these), based on studies and research related to AI and AR. Results will be demonstrated in a TRL4-5 demonstration systems realised in the final phase of the project.
Lead Partner	EMBEDDED ACOUSTICS B.V.
Partners involved	BALTIJOS PAZANGIU TECHNOLOGIJU INSTITUTAS, UAB ADOS-TECH, NEX VISION, E&Q ENGINEERING SOLUTIONS AND INNOVATION SL
Duration	01 December 2022 - 31 May 2025
Results	-
Funding	-
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101102526/EDF

Nr 502/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Smart, Heterogeneous Technological Platform Extending the Power and Frequency Limits of Flexible Nanoelectronics

Description	The project "Smart, Heterogeneous Technological Platform Extending the Power and Frequency Limits of Flexible Nanoelectronics" (POWERFLEX) proposes a disruptive solution for high power and frequency conformal antennae based on novel flexible GaN power amplifier, Carbonnano-tube based low noise amplifier and flexible RFMEM Stechnologiesand their 2D monolithic integration.
Goal	A new idea of cooling the amplifier with a flexible organic based thermal platform will be implemented. POWERFLEX will deliver one Ka band (flexible) demonstrator delivering 40dBm power that will be validated in the military laboratories of THALES. POWERFLEX in essence will inaugurate a new filed in flexible electronics, namely that of power flexible (nano) electronics and will boost the competitiveness of the European SATCOM ecosystem.
Lead Partner	THALES
Partners involved	IDRYMA TECHNOLOGIAS KAI EREVNAS, BERLINER NANOTEST UND DESIGN GMBH, CIRCUITS INTEGRATED HELLAS IKE, UPPSALA UNIVERSITET, ETHNIKO KAI KAPODISTRIAKO PANEPISTIMIO ATHINON, INSTITUTUL NATIONAL DE CERCETAREDEZVOLTARE PENTRU MICROTEHNOLOGIE, THALES SIX GTS FRANCE SAS, PRISMA ILEKTRONIKA ABEE, TAIPRO ENGINEERING SA,
Duration	01 December 2022 - 30 November 2025
Results	-
Funding	€ 3,458,087.24
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101102565/EDF https://defence-industry-space.ec.europa.eu/system/files/2022-07/Factsheet_EDF21_POWERFLEX.pdf

Nr 503/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

European Non-Line-of-Sight Optical Imaging

Description	The main technical challenge "European Non-Line-of-Sight Optical Imaging" (ENLIGHTEN) project is to develop new NLOS algorithms and technology such as a SPAD camera and laser illuminator that work in the short-wave-infrared (SWIR) regime.
Goal	ENLIGHTEN aims at developing disruptive technologies for next-generation electro-optical (EO) sensing devices which enable vision of scenes hidden behind obstacles. With this future sensing approach, the proposal pushes the development of advanced concepts, promising technologies and innovations to the benefit of operational effectiveness. With this future sensing approach, ENLIGHTEN pushes the development of advanced concepts, promising technologies and innovations to the benefit of operational effectiveness. Moreover, the project supports the EU strategic autonomy and its freedom of action. Further, the project aims at stimulating cross-border cooperation of legal entities and fostering a better exploitation of the industrial potential of innovation, research and technological development. ENLIGHTEN can significantly boost the performance of future capabilities.
Lead Partner	UNIVERSIDAD DE ZARAGOZA
Partners involved	INSTITUT FRANCO-ALLEMAND DE RECHERCHES DE SAINT LOUIS, UNIVERZA V LJUBLJANI, POLITECNICO DI MILANO, FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV, MICRO PHOTON DEVICES SRL
Duration	01 December 2022 - 30 November 2026
Results	-
Funding	€ 8,424,382.23
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103242/EDF https://edrin.org/fileadmin/media/Factsheet_EDF21_ENLIGHTEN.pdf

Nr 504/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Sea/Air Interphasic Wing-in-Ground Effect Autonomous Drones

Description	The project "Sea/Air Interphasic Wing-in-Ground Effect Autonomous Drones" (SEAWINGS) will develop a new class of military surveillance drones to operate in the sea/air interface giving rise to a new type of unmanned craft, Unmanned Wing-in-Ground Vehicles, capable of very high payloads, inexpensive, long-range that do not require infrastructure or launch vehicle for departure and landing.
Goal	Specific objectives are: • Implementing an architecture for the SEAWINGS platform to operate autonomously; • Adapting and deliver the technological components for operational field circumstances; • Upgrading the operational interface, supervision system, launch and recovery system for field trials; • Conducting and evaluate a series of partial field trials according to increasing levels of difficulty.
Lead Partner	LA PALMA RESEARCH CENTRE SL
Partners involved	UNIVERSIDAD POLITECNICA DE MADRID, INESC TEC - INSTITUTO DE ENGENHARIADE SISTEMAS E COMPUTADORES, TECNOLOGIA E CIENCIA, TRISOLARIS ADVANCED TECHNOLOGIES LDA, ZANASI ALESSANDRO SRL, PORVALOR - ATIVOS DE ENGENHARIA LDA
Duration	01 December 2022 - 31 May 2026
Results	-
Funding	€ 3,927,342.66
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101102763/EDF https://defence-industry-space.ec.europa.eu/system/files/2022-09/Factsheet_EDF21_SEAWINGS.pdf

Nr 505/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Using fiber optical cables for maritime situational awareness

Description	The project "Using fiber optical cables for maritime situational awareness" (FIBERSENSE) will focus on and advance the Distributed Acoustic Sensing (DAS) technology. DAS exploits the laser - induced Rayleigh backscattering in the Fiber Optic Cable (FOC) to detect incident acoustic waves.
Goal	Feasibility studies will be performed, including in an isolated-controlled environment for underwater testing, and in real operational environments, also for extended testing periods. The expected impact is increased functional life time and reduction in costs of use.
Lead Partner	SATWAYS-OLOKLIROMENES LYSEIS ASFALEIAS KAI AMYNAS-IDIOTIKI EPICHEIRISI PAROCHIS YPIRESION ASFALEIAS (IEPYA)-ETAIREIA PERIORISMENIS EFTHYNIS
Partners involved	AP SENSING GMBH, INOV INSTITUTO DE ENGENHARIA DE SISTEMAS E COMPUTADORES INOVACAO, WEHRTECHNISCHE DIENSTSLLE FUR SCHIFFE MARINEWAFFEN MARITIME TECNOLOGIE UND FORSCHNG, ETHNIKO ASTEROSKOPEIO ATHINON
Duration	01 December 2022 - 30 November 2025
Results	-
Funding	€ 3,386,861.61
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101110375/EDF https://defence-industry-space.ec.europa.eu/system/files/2023-01/Factsheet_EDF21_FIBERSENSE.pdf

Nr 506/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Additive Manufacturing of Lightweight Laser Target Designator

Description	The application of unmanned aircraft systems (UAS) has become a key capability in today's operational environment, both at the national level and abroad. Small- and mini-class UAS are compact, agile and easy to deploy platforms that have been deployed in a wide range of scenarios, consistently contributing to intelligence, surveillance and reconnaissance (ISR) missions, and considerably reducing the threat to human life in high-risk operations. The most critical factor that limits their application is determined by its payload carrying capacity. Small class UAS can transport only a few kilos, which makes them unfit for the heavy electro-optic systems necessary for target designation missions. Recent developments in material science, additive manufacturing and laser technology have created the necessary conditions for the development of a new generation of laser target designator systems (LTD).
Goal	The project proposes the development of a miniature LTD optimised for integration into a mini-UAV unit. State-of-the-art diodepumped solid-state laser technology and athermal optical design will be used to obtain a low SWaP-C system with optical output fully compliant with NATO STANAG 3733, enabling accurate long-range designation and targeting. Further reduction of the LTD's size and weight will be achieved by innovative mechanical design of the laser household and its optical system supports. These complex and lightweight structures will be manufactured by selective laser melting of lightweight metal alloys. These downsized LTD devices would comply with the stringent payload size requirements of small class UAV without any decrease in their performance. This would allow small- and mini-class UAS to be able to perform target designation activities and extend their range of effectiveness.
Lead Partner	AKTYVUS PHOTONICS UAB
Partners involved	GLOBAL DESIGN TECHNOLOGY, VALSTYBINIS MOKSLINIU TYRIMU INSTITUTAS FIZINIU IR TECHNOLOGIJOS MOKSLU CENTRAS, OPEN ENGINEERING SA, ALTUS LSA COMMERCIAL AND MANUFACTURING SA
Duration	01 December 2022 - 31 January 2026
Results	-
Funding	€ 2,868,733.37 (European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101102480/EDF https://defence-industry-space.ec.europa.eu/system/files/2023-01/Factsheet_EDF21_AMLTD.pdf

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Secure Microcontroller with Embedded Quantum Random Number Generator

Description	The project "Secure Microcontroller with Embedded Quantum Random Number Generator" SMiEQ will define and prototype a secure microcontroller with embedded QRNG aiming at the protection of weapon systems, (un)manned aerial vehicle, fixed and rotary wings, (un)manned aircrafts and any other systems critical systems against cyber-attacks.
Goal	The result of these studies will be the design of a microcontroller ready to be used to secure European defense systems in the era of quantum computing which will represent a threat to these systems
Lead Partner	BULL SAS
Partners involved	FONDAZIONE BRUNO KESSLER, TIEMPO SAS
Duration	01 December 2022 - 31 May 2026
Results	-
Funding	European Defence Fund
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103001/EDF

Nr 508/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Convoy Operations with Manned-unMAnNeD Systems

Description	COMMANDS addresses the requirement of military unmanned ground vehicles to operate not only in controlled paved surfaces, but also in unstructured environments, facing degraded or denied satellite signal and communications scenarios where the development of Computer Based Processing Technologies, Machine Learning and Artificial Intelligence provide game changing Intelligent Capabilities. The Technology Demonstrator Programme includes both a laboratory demonstrator and a real scenario Mobile Demonstrator centered around the used case of a Last Kilometre Re-supply Convoy with Force Protection. The capability services architecture are common to manned and unmanned platforms. enabling seamless, standard transition from manned to unmanned.
Goal	The COMMANDS project aims to develop Through Life Capabilities (TLC) for agile, intelligent and cooperative Manned and Unmanned Land Systems. These Capabilities will be based on a variety of state-of-the-art UGV Technologies solutions that will provide seamless functional services across integrated modular open architectures. The answer to the UGVT call is based on a solid Systems Engineering process supported by a Technology Demonstrator and a Business Case, that will ensure early de-risking as well as potential early exploitation of technologies directly addressing a roadmap of self-reliant EU Defence TLC sustainable development. The results will not only enable to upgrade current ground vehicles of the EU inventory for specific missions, but also to be integrated in future vehicles in development.
Lead Partner	SENER AEROESPACIAL SOCIEDAD ANONIMA
Partners involved	SANTA BARBARA SISTEMS SA, INSTITUTO NACIONAL DE TECNICA AEROESPACIAL ESTEBAN TERRADAS, INDRA SISTEMAS SA, POLITECNICO DI MILANO, LINK CAMPUS UNIVERSITY, MASA GROUP, LABORATOIRE NATIONAL DE METROLOGIE ET D'ESSAIS, Clavister AB, IKNOWHOW SA, INTRACOM DEFENSE AE, BALTIJOS PAZANGIU TECHNOLOGIJU INSTITUTAS, SCERTAS GMBH, SKYLD SECURITY AND DEFENCE LIMITED, EIGHT BELLS LTD, VETRONICS RESEARCH CENTRE EU LTD, SIGNALGENERIX LIMITED, IVECO DEFENCE VEHICLES SPA, LEONARDO - SOCIETA PER AZIONI, VOJENSKY VYZKUMNY USTAV SP, WOJSKOWA AKADEMIA TECHNICZNA IM.JAROSLAWA DABROWSKIEGO
Duration	01 December 2022 - 30 November 2025
Results	-
Funding	European Defence Fund
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101102635/EDF

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

EDF-2021-EPW

Description	The main objective of the project "European Protected Waveform" (EPW) is to present the military end-user with an innovative end-to-end secure solution for seamless satellite communications at maximum information assurance. The European Protected Waveform is built around four corner stones: efficient, secure, affordable and interoperable satellite communications and will be accessible to small, mid-sized and large European nations seeking to embrace today's and future challenges related to increased throughput demand over satellite, dispersed operations, mobility and new security threats.
Goal	The project will study and design a multi-layered security and resiliency solution built around the corner stones of efficient, secure, affordable and interoperable satellite, to embrace today's and future challenges related to increased through put demand over satellite, dispersed operations, mobility and new security threats.
Lead Partner	ST ENGINEERING I DIRECT EUROPE CY
Partners involved	AIRBUS DEFENCE AND SPACE GMBH, AMPHINICY DOO ZA RACUNALNE AKTIVNOSTI I ZASTUPANJE, ANTWERP SPACE N.V., TTI NORTE SL, ELITAL - ELETTRONICA ITALIANA-SOCIETA' A RESPONSABILITA' LIMITATA, EUTELSAT, GISS SPOLKA Z OGRANICZONA ODPOWIEDZIALNOSCIA, INDRA SISTEMAS SA, LEONARDO - SOCIETA PER AZIONI, LUXGOVSAT S.A., LASTING SOFTWARE SRL, NEOSAT GMBH, STICHTING KONINKLIJK NEDERLANDS LUCHT - EN RUIMTEVAARTCENTRUM, OHB DIGITAL CONNECT GMBH, QUADSAT APS, ECOLE ROYALE MILITAIRE - KONINKLIJKE MILITAIRE SCHOOL, THALES ALENIA SPACE ITALIA SPA, THALES SIX GTS FRANCE SAS
Duration	01 December 2022 - 28 February 2026
Results	-
Funding	€ 25,000,000.00 (European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103510/EDF https://defence-industry-space.ec.europa.eu/system/files/2022-07/Factsheet_EDF21_EPW.pdf

Nr 510/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Modular ARchitecture Solution for EU States

Description	MARSEUS project is a second step of an overall roadmap in order to mature and develop a European BLOS capability including its various components under a full European design authority. MARSEUS will enhance the BLOS capability initiated in the LynkEUs project and will study architecture's components and functions related to an extended range BLOS capability and an extended BLOS capacity.
Goal	The project "Modular ARchitecture Solution for EU States" (MARSEUS) aims at developing a collaborative close combat architecture enhancing existing missile systems with a Beyond Line Of Sight (BLOS) capability. The project builds on the ongoing EDIDP 2019 LynkEUs project, thus continuing the work begun during this precursor project.
Lead Partner	MBDA FRANCE
Partners involved	NOVADEM, BULL SAS, DELAIR, ARQUUS, ECOLE ROYALE MILITAIRE - KONINKLIJKE MILITAIRE SCHOOL, XENICS NV, JOHN COCKERILL DEFENSE, FN HERSTAL SA, ADDITESS ADVANCED INTEGRATED TECHNOLOGY SOLUTIONS & SERVICES LTD, SIGNALGENERIX LIMITED, SAAB DYNAMICS AKTIEBOLAG, BAE SYSTEMS HAGGLUNDS, EXENSOR TECHNOLOGY AKTIEBOLAG
Duration	01 December 2022 - 30 November 2025
Results	-
Funding	€ 25,000,000.00 (European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103595/EDF https://defence-industry-space.ec.europa.eu/system/files/2023-01/Factsheet_EDF21_MARSEUS.pdf

Nr 511/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

PROACTIVE AUTOMATIC IMAGERY INTELLIGENCE POWERED BY ARTIFICIAL INTELLIGENCE EXPLOITING EUROPEAN SPACE ASSETS

Description	This proposal, therefore, will design a system to fully automatize the IMINT workflow, consisting of: Automatic Acquisition, Automatic Pre-processing, (Key Challenge) Automatic Extraction, Automatic report generation, Automatic Dashboard management. Two technologies using Artificial Intelligence lie at the core of the solution that IntSen2 proposes: • Super-resolution: Improving the resolution of imagery by a factor of 4 allows imagery from Sentinel satellites to provide value in security scenarios; • Automatic Extraction: Applying AI based extraction techniques to super-resolved Sentinel imagery can unlock the use of all operational potential of Sentinel for security scenarios.
Goal	IntSen2 aims at researching a disruptive change, using Artificial Intelligence to develop a concept of application for an IMINT service, from a reactive service design to a proactive service design. And it does so by basing the research and proposed solutions exclusively on European assets in order to support EU operational autonomy.
Lead Partner	TRACASA INSTRUMENTAL SL
Partners involved	EUROPEAN UNION SATELLITE CENTRE, ZABALA INNOVATION CONSULTING SA, EVENFLOW, RINA CONSULTING SPA, PLANETEK HELLAS ETAIREIA PERIORISMENIS EFTHYNIS YPIRESIES CHARTOGRAFISIS MESO DORYFOROU, UNIVERSITA DEGLI STUDI DI NAPOLI FEDERICO II, JOANNEUM RESEARCH FORSCHUNGSGESELLSCHAFT MBH, CENTRUM BADAN KOSMICZNYCH POLSKIEJ AKADEMII NAUK
Duration	01 December 2022 - 30 November 2024
Results	-
Funding	European Defence Fund
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103622/EDF

Nr 512/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

New European WarHEAd Technologies

Description	The New European WarHEAd Technologies (NEWHEAT) project aims to find solutions to defeat most recent and foreseeable threats that will emerge in the near future to the armed forces of EU Member States. New warhead technologies are a must-have for the armed forces of EU Member States to keep their lead and defeat these threats.
Goal	NEWHEAT aims to improve the performance of conventional shaped charge by integrating new high explosive, new liner materials and new geometries. To go beyond the State-of-the-Art and address future challenges, NEWHEAT will also focus on the development of new concepts and demonstrators for warheads: • Explosively Formed Projectiles, • Multi-Liner Explosively Formed Projectiles, • Slow Stretching Jet Shaped Charges.
Lead Partner	TDW GESELLSCHAFT FUR VERTEIDIGUNGSTECHNISCHE WIRKSYSTEME MIT BESCHRANKTE RHAFTUNG
Partners involved	FORSVARETS FORSKNINGINSTITUTT, TOTALFORSVARETS FORSKNINGSINSTITUT, OY FORCIT AB, FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV, INSTALAZA S.A., NEXTER MUNITIONS, WOJSKOWY INSTYTUT TECHNICZNY UZBROJENIA
Duration	01 December 2022 - 30 November 2025
Results	-
Funding	€ 9,988,212.18 (European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101102442/EDF https://defence-industry-space.ec.europa.eu/system/files/2022-07/Factsheet_EDF21_NEWHEAT.pdf

Nr 513/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

5G COMmunications for Peacekeeping And Defence

Description	The project is bringing the world's leading 5G vendors and Europe's strongest defence system integrators together, supported by mobile network operators, research institutes and several niche-technology companies. In a joint effort, the consortium will carry out feasibility studies addressing important use cases, relevant for both peacekeeping and defence applications. Based on study results, a reference architecture for a 5G based robust and resilient multi-dimensional communications system will be designed.
Goal	The objective with the 5G COMPAD project is to evaluate and propose how modern commercial mobile communications technology can support sustained information superiority in the defence domains at scale. 5G offers superior performance, new and improved functionality and life cycle cost advantages over existing systems.
Lead Partner	SAAB AKTIEBOLAG
Partners involved	ERICSSON AB, RHEINMETALL ELECTRONICS GMBH, BITTIUM WIRELESS OY, NOKIA SOLUTIONS AND NETWORKS OY, THALES SIX GTS FRANCE SAS, LEONARDO - SOCIETA PER AZIONI, INSTER TECNOLOGIA Y COMUNICACIONESSA, EIGHT BELLS HELLAS I.K.E., INTRACOM DEFENSE AE, CAFA TECH OU, TELENOR ASA, SINTEF AS, FORSVARETS FORSKNINGINSTITUTT, LATVIJAS MOBILAIS TELEFONS SIA, AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH, Synkzone AB, BHE BONN HUNGARY ELEKTRONIKAI KORLATOLT FELELOSSEGU TARSASAG, APR TECHNOLOGIES AB, NOKIA SOLUTIONS AND NETWORKS KFT
Duration	01 December 2022 - 31 January 2027
Results	-
Funding	€ 26,998,532.29 (European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103519/EDF https://defence-industry-space.ec.europa.eu/system/files/2022-07/Factsheet_EDF21_5G%20COMPAD.pdf

Nr 514/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Knowledge Extraction, Machine Learning and other AI approaches for secure, robust, frugal and explainable solutions in Defence Applications

Description	The project "Knowledge Extraction, Machine Learning and other AIapproaches for secure, robust, frugal, resilient and explainable solutions in Defence Applications" (KOIOS) will be developed around four main outputs (Simulation framework with performance computing capabilities and reduced complexity; Identification and development of use cases; Definition of ametrics specifically designed for measuring frugality, robustness, resilience; and Development of experiments built on a common protocol ensuring their reproducibility) for enhanced AIusagein defence applications.
Goal	The main objective of our project, KOIOS, is to develop new AI-based methods that are trustworthy (under human control and explainable), robust (resilient to attacks) and frugal in the use of resources (data, computing capabilities, energy,…) addressing tasks in a more efficient manner than the current state-of-the-art ML/DL methods while maintaining similar performance, and improving resilience (for adversarial attacks), consistent behaviour and limiting the cognitive and technical efforts when adapting to new data or dynamic contexts.
Lead Partner	CT INGENIEROS AERONAUTICOS DE AUTOMOCION E INDUSTRIALES SL
Partners involved	BARCELONA SUPERCOMPUTING CENTER CENTRO NACIONAL DE SUPERCOMPUTACION, TOTALFORSVARETS FORSKNINGSINSTITUT, UNIVERSITAET DER BUNDESWEHR MUENCHEN, NTT DATA SPAIN, SL, OFFICE NATIONAL D'ETUDES ET DE RECHERCHES AEROSPATIALES, LABORATOIRE NATIONAL DE METROLOGIE ET D'ESSAIS, MITIGA SOLUTIONS SL, APPLIED INTELLIGENCE ANALYTICS LIMITED, TECHNISCHE UNIVERSITEIT EINDHOVEN, STICHTING MARITIEM RESEARCH INSTITUUT NEDERLAND, IDRYMA TECHNOLOGIAS KAI EREVNAS, UNIVERSITA' DEGLI STUDI DI BERGAMO, VOCAPIA RESEARCH
Duration	01 December 2022 - 30 November 2025
Results	-
Funding	European Defence Fund
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103770/EDF https://edrin.org/fileadmin/media/Factsheet_EDF21_KOIOS.pdf

Nr 515/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Frugal and Robust AI for Defence Advanced Intelligence

Description	The project "Frugal and Robust AI for Defence Advanced Intelligence" (FaRADAI) focusses on frugal learning, i.e. the ability of a system to adapt and learn from its' environment, including from user supervision, for areas on able cost and without intervention from expert developers.
Goal	Within the FaRADAI project, current advances in AI technologies will be thoroughly researched in parallel with a detailed study of the main challenges imposed by a defence system. Aiming at significant breakthroughs in AI, the models will accelerate their wider application and deployment in defence systems increasing their impact and the overall performance.
Lead Partner	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS
Partners involved	BIANOR SERVICES EOOD, BALTIJOS PAZANGIU TECHNOLOGIJU INSTITUTAS, C&V CONSULTING, COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES, CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI, DEFSECINTEL SOLUTIONS OU, NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS", FLYSIGHT SRL, FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN LEONARDO - SOCIETA PER AZIONIFORSCHUNG EV, HENSOLDT OPTRONICS GMBH, INDRA SISTEMAS SA, LEONARDO - SOCIETA PER AZIONI, MBDA ITALIA SPA, OKTAL SYNTHETIC ENVIRONMENT, RHEINMETALL ELECTRONICS GMBH, RIGAS TEHNISKA UNIVERSITATE, SAFRAN ELECTRONICS & DEFENSE, STAM SRL, SZAMITASTECHNIKAI ES AUTOMATIZALASI KUTATOINTEZET, FUNDACION TECNALIA RESEARCH & INNOVATION, THALES, THALES SIX GTS FRANCE SAS, LINK CAMPUS UNIVERSITY, UNIVERSIDAD POLITECNICA DE MADRID, NAVAL GROUP, INSTITUT PO OTBRANA, EXUS SOFTWARE MONOPROSOPI ETAIRIA PERIORISMENIS EVTHINIS, SATWAYS-OLOKLIROMENES LYSEIS ASFALEIAS KAI AMYNAS-IDIOTIKI EPICHEIRISI PAROCHIS YPIRESION ASFALEIAS (IEPYA)-ETAIREIA PERIORISMENIS EFTHYNIS, MARINTRAFIK OPEREISONS MONOPROSOPI ANONYMI ETAIREIA PLIROFORIKIS, NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO, E-GEOS SPA, SKA POLSKA SPOLKA Z OGRANICZONA ODPOWIEDZIALNO, INFILI TECHNOLOGIES SOCIETE ANONYME, THALES ESPANA SISTEMAS SA
Duration	01 December 2022 - 31 May 2026
Results	-
Funding	€ 18,498,239.16 (European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103386/EDF https://defence-industry-space.ec.europa.eu/system/files/2022-07/Factsheet_EDF21_FaRADAI_0.pdf

Nr 516/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

AI Framework for Improving Cyber Defence Operations

Description	The project ”AI Framework for Improving Cyber Defence Operations” (AInception) will develop novel AI-based tools and techniques for detection and response: from detecting adversarial behaviour from logs and network traffic; to understanding, contextualizing and explaining the detected threat; to generating risk and impact aware response action; all the way to automating the execution and evaluation of the response action on the underlying infrastructure. AI will play a central role for all these steps in the AInception tool pipeline. These tools will be combined into a proof-of-concept end to-end detection and response prototype, evaluated in operational scenarios with end users.
Goal	The project aims at developing Artificial Intelligence-based intrusion detection tools and techniques that out perform current military systems for selected scenarios and techniques that can abstract, aggregate, enrich and contextualise alerts into a more manageable set of abstracted meta alerts.
Lead Partner	SPACE HELLAS ANONYMI ETAIREIA SYSTIMATA KAI YPIRESIES TILEPIKOINONIONPLIROFORIKIS ASFALEIAS - IDIOTIKI EPICHEIRISI PAROCHIS YPERISION ASFA
Partners involved	FORSVARETS FORSKNINGINSTITUTT, THALES SIX GTS FRANCE SAS, NAVAL GROUP, UBITECH LIMITED, EIGHT BELLS LTD, INFILI TECHNOLOGIES SOCIETE ANONYME, TOTALFORSVARETS FORSKNINGSINSTITUT, NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO, KUNGLIGA TEKNISKA HOEGSKOLAN, NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS", AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH, MINISTRY OF NATIONAL DEFENCE, GREECE, INSTITUT PO OTBRANA, COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES, CY4GATE SPA, MNEMONIC AS, THALES HELLAS MONOPROSOPI ANONYMI ETAIREIA PARAGOGIS EMPORIAS KAI YPIRESION ILEKTRONIKOU EXOPLISMOU
Duration	01 December 2022 - 30 November 2025
Results	-
Funding	€ 8,147,875.50 (European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103385/EDF https://edrin.org/fileadmin/media/Factsheet_EDF21_Ainception.pdf

Nr 517/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Novel 3D heterogeneous integration for future miniaturized power RF Transceiver front ends

Description	The project "Novel 3D heterogeneous integration for future miniaturized power RF Transceiver frontends" (POWERPACK) proposes to develop disruptive technologies for RF MEMS for high frequency and high-power operation
Goal	The project will develop disruptive technologies for miniaturised RFchips for high frequency and high-power operation, and will focus on miniaturisation and 3D integration. The outcome will be a reduction in transmission losses, and will result in two demonstrators. These demonstrators will operate in the X-Band and in the Ka-Band. The devices will allow for integration in platforms where the components will need to ever be smaller and lighter.
Lead Partner	THALES
Partners involved	TAIPRO ENGINEERING SA, CIDETE INGENIEROS SOCIEDAD LIMITADA, CIRCUITS INTEGRATED HELLAS IKE, BERLINER NANOTEST UND DESIGN GMBH, MICROWAVE CHARACTERIZATION CENTER, IDRYMA TECHNOLOGIAS KAI EREVNAS, INSTITUTUL NATIONAL DE CERCETAREDEZVOLTARE PENTRU MICROTEHNOLOGIE, FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV, ARISTOTELIO PANEPISTIMIO THESSALONIKIS
Duration	01 December 2022 - 30 November 2025
Results	-
Funding	€ 3,494,531.61 (European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101102564/EDF https://defence-industry-space.ec.europa.eu/system/files/2022-07/Factsheet_EDF21_POWERPACK.pdf

Nr 518/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

EUROPEAN DIGITAL NAVAL FOUNDATION

Description	The project "European Digital Naval Foundation" (EDINAF) will enable the integration of a joint naval operational cloud as a component into the broader military multidomain operations cloud.
Goal	EDINAF will work on an IT infrastructure and associated data interface standards (edge and cloud computing). It will support the design and the creation of next generation smart vessels and gather the European supply chain around a common standard applicable to equipment manufacturing and to future naval operations.
Lead Partner	NAVANTIA S.A.
Partners involved	SHIPYARDS AND MARITIME EQUIPMENT ASSOCIATION OF EUROPE, DAMEN SCHELDE NAVAL SHIPBUILDING BV, SAAB KOCKUMS AKTIEBOLAG, NAVAL GROUP, FINCANTIERI SPA, KONGSBERG DEFENCE & AEROSPACE AS, THYSSENKRUPP MARINE SYSTEMS GMBH, INDRA SISTEMAS SA, AERTEC SOLUTIONS SL, UNIVERSIDADE DA CORUNA, NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO, STICHTING MARITIEM RESEARCH INSTITUUT NEDERLAND, THALES NEDERLAND BV, RH MARINE NETHERLANDS BV, MINISTRY OF DEFENSE, UNIVERSITE DE LORRAINE, MBDA FRANCE, B-COM, LEONARDO - SOCIETA PER AZIONI, UNIVERSITA DEGLI STUDI DI GENOVA, SINTEF AS, SINTEF OCEAN AS, JOTNE CONNECT AS, LIGHT STRUCTURES AS, RENK GMBH, RHEINMETALL ELECTRONICS GMBH, QRELATION MANAGEMENT TEAM GMBH
Duration	01 December 2022 - 30 November 2025
Results	-
Funding	€ 29,000,000.00 (European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103273/EDF https://edrin.org/fileadmin/media/Factsheet_EDF21_EDINAF.pdf

Nr 519/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Miniaturized Board-mountable Optical Transceiver for high data rate Military Satellite Communications

Description	Mini-BOT aims to establish the first European supply chain of hi-rel OTRXs removing dependency barriers and unlocking the full potential of military fiber optics to the European A&D and space industry. Mini-BOT targets significant advances with respect to the state-of-the-art by engaging high-end technologies in which Europe has and continues to invest.
Goal	Mini-BOT OTRX design targets challenging the state-of-the-art as follows: • 128 Gb/s (4x32 Gb/s) aggregate data rates deploying transceiver electronics with >58% better energy efficiency and opto-electronics with >60% bandwidth, • deployment of miniaturized metalens optics with one order of magnitude smaller size than conventional diffractive optics, • module footprint as low as 1.6 grams and 190 mm2 representing >86% more capacity per unit mass and 139% more capacity per unit area.
Lead Partner	LEO SPACE PHOTONICS R&D MONOPROSOPIIKE
Partners involved	VIGO PHOTONICS SPOLKA AKCYJNA, NAPA TECHNOLOGIES, CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE CNRS, POLITECHNIKA LODZKA
Duration	01 December 2022 - 30 November 2025
Results	-
Funding	(European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101102948/EDF

Nr 520/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Advanced, Disruptive and Emerging QUAntum technologies for DEfense

Description	The project "Advanced, Disruptive and Emerging QU Antum technologies for DEfense" (ADEQUADE) intends to provide breakthrough in three Quantum Sensing (QS) domains and the intended results will pave the way for the development of capabilities with significant technological, operational and strategic advantages over existing defence products or technologies in different warfare capabilities: positioning, radio frequency, optronics.
Goal	ADEQUADE aims at providing a breakthrough in different quantum-sensing domain swhich will develop capabilities with significant technological, operational and strategic advantages over existing defence products or technologies in different warfare areas.
Lead Partner	THALES
Partners involved	CONSIGLIO NAZIONALE DELLE RICERCHE, CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE CNRS, DIEHL DEFENCE GMBH & CO. KG, DANMARKS TEKNISKE UNIVERSITET, ELETTRONICA SPA, ECOLE NORMALE SUPERIEURE PARIS-SACLAY, FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV, FLYSIGHT SRL, G.E.M. ELETTRONICA SRL, FUNDACIO INSTITUT DE CIENCIES FOTONIQUES, INDRA SISTEMAS SA, ISTITUTO NAZIONALE DI RICERCA METROLOGICA, LEONARDO - SOCIETA PER AZIONI, CHILAS B.V., LATVIJAS UNIVERSITATE, MBDA ITALIA SPA, EXAIL, OFFICE NATIONAL D'ETUDES ET DE RECHERCHES AEROSPATIALES, POLITECNICO DI MILANO, QUIX QUANTUM BV, RHEINMETALL ELECTRONICS GMBH, SENER AEROESPACIAL SOCIEDAD ANONIMA, SUPRACON AG, SORBONNE UNIVERSITE, TELESPAZIO SPA, NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO, UNIVERSITA DEGLI STUDI DI BARI ALDO MORO, UNIVERZITA PALACKEHO V OLOMOUCI, UNIVERSITY OF STUTTGART, SAFRAN ELECTRONICS & DEFENSE
Duration	01 December 2022 - 30 November 2025
Results	-
Funding	€ 27,433,831.28 (European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103417/EDF https://edrin.org/fileadmin/media/Factsheet_EDF21_ADEQUADE.pdf

Nr 521/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

HIGH FREQUENCY OVER THE HORIZON SENSORS' COGNITIVE NETWORK

Description	The project "High Frequency Over The Horizon Sensors' Cognitive Network" (iFURTHER) aims to address air and sea long range detection (over the horizon) by developing new technologies to be integrated in a network of HF infrastructures operating in a collaborative way. At the end, the project will contribute to develop a persistent and very wide-area EU defence capability, to monitor air and sea domains by delivering some concrete and scalable solutions to consider.
Goal	• Detection and tracking of air and sea targets at long range over the horizon, far beyond current existing systems, by utilization of sky-wave and surface-wave signal reflections; • Filling of the gaps and extension of current air and sea EU radar surveillance coverage, by implementing a multi static sensors' configuration being supported by ad hoc networking protocols; • Implementation of cognitive radar management schemes to optimize the operational parameters in real time and in accordance with the environmental conditions; • Implementation of advanced signal processing techniques to improve over-the-horizon detection and tracking performance as well as target localization capabilities
Lead Partner	ELLINIKI AEROPORIKI VIOMICHANIA ANONYMI ETAIREIA
Partners involved	OFFICE NATIONAL D'ETUDES ET DE RECHERCHES AEROSPATIALES, ETHNIKO ASTEROSKOPEIO ATHINON, IMATIK-EFARMOGES YPSILIS TEXNOLOGIAS ETAIREIA PERIORISMENIS EFTHINIS, CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI, ISTITUTO NAZIONALE DI GEOFISICA E VULCANOLOGIA, POLITECHNIKA WARSZAWSKA, FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV, HELZEL MESSTECHNIK GMBH, TECHNISCH-MATHEMATISCHE STUDIENGESELLSCHAFT MIT BESCHRANKTER HAFTUNG, INDRA SISTEMAS SA, UNIVERSIDAD DE ALCALA, BHE BONN HUNGARY ELEKTRONIKAI KORLATOLT FELELOSSEGU TARSASAG, SIGNALGENERIX LIMITED, PATRIA AVIATION OY, ERA AS, MINISTRY OF NATIONAL DEFENCE, GREECE, L - UP SAS
Duration	01 December 2022 - 30 November 2025
Results	-
Funding	€ 10,955,937.10 (European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103607/EDF https://defence-industry-space.ec.europa.eu/system/files/2022-07/Factsheet_EDF21_iFURTHER_1.pdf

Nr 522/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Highly Automated Swarm of Affordable ISR Long Endurance UAVs for force protection

Description	The project "Highly Automated Swarm of Affordable ISR Long Endurance UAVs for force protection" (ALTISS) will be based on innovative solutions for communication and flight management, enhanced image processing algorithms for light UAV and automated event detection, and enhanced SIGINT (Signal Intelligence) sensors to detect and localise radio emitters and merge info with image processing to improve the identification of targets. It is an innovative solution that will improve force protection while decreasing collateral damages and logistic footprint.
Goal	The objective is to increase air observation coverage capacity through an affordable permanent detection of crossing events on a linear surface 10 km x 500 km wide when the others rare and expensive air observation assets are unavailable, either dedicated to more critical mission or too expensive to be acquired by governments.
Lead Partner	MAGELLIUM SAS
Partners involved	M3 SYSTEMS BELGIUM, SAGAX INFORMATIKAI, SZERVEZO ES TANACSADO KORLATOLT FELELOSSEGU TARSASAG, RADIONOR COMMUNICATIONS AS
Duration	01 December 2022 - 30 November 2025
Results	-
Funding	€ 3,202,501.08 (European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101102587/EDF https://edrin.org/fileadmin/media/Factsheet_EDF21_ALTISS.pdf

Nr 523/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

RF INTERFERENCE REMOVAL FOR MILITARY SERVICES BASED ON SPACES LINK

Description	The project "RF Interference Removal for Military Services based on Spaces Link" (RFSHIELD) will develop a European-made solution to protect the Sat Comservices from intentionaland non-intentional interferences, increasing the availability and performance of COMSATCOM / MILSATCOM services for military users.
Goal	The main objective of RFSHIELD project is to increase the availability and performance of COMSATCOM/MILSATCOM services for military users by developing a European-made solution to protect the SatCom services from intentional and non-intentional interferences. It is the first European solution, that aims to do it in a waveform agnostic way while it is interoperable with the network equipment.
Lead Partner	INTEGRASYS SA
Partners involved	AICOX SOLUCIONES SA, ECLIPTIC DEFENCE AND SPACE LTD, INGESPACE, MEDIA BROADCAST SATELLITE GMBH
Duration	01 December 2022 - 31 May 2025
Results	-
Funding	€ 3,420,390.01 (European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101102640/EDF https://defence-industry-space.ec.europa.eu/system/files/2022-07/Factsheet_EDF21_RFSHIELD.pdf

Nr 524/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Advanced Galileo PRS resilience for EU Defence

Description	The project "Advanced Galileo PRS resilience for EU Defence" (Navguard) will develop ground and space-based systems to detect illegitimate activities in GNSS frequency bands and geolocate the sources of malicious activities, including an in-orbit demonstration of a PRS space-based augmentation system. An Information management subsystem will also be developed together with a user interface to establish a situational awareness picture.
Goal	The Navguard project ambitions to develop a European NAVWAR capability relying on GNSS spectrum surveillance systems, and to strengthen the PRS resilience, complementing ongoing EDIDP GEODE activities.
Lead Partner	FDC SARL
Partners involved	OHB DIGITAL SOLUTIONS GMBH, ANTWERP SPACE N.V., THALES ALENIA SPACE FRANCE SAS, SAFRAN TRUSTED 4D SAS, SAFRAN ELECTRONICS & DEFENSE, THALES AVS FRANCE SAS, THALES SIX GTS FRANCE SAS, DIEHL DEFENCE GMBH & CO. KG, FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV, INDUSTRIEANLAGEN BETRIEBSGESELLSCHAFT MBH, OHB SYSTEM AG, BEYOND GRAVITY GERMANY GMBH, ELETTRONICA SPA, LEONARDO - SOCIETA PER AZIONI, QASCOM SRL, THALES ALENIA SPACE ITALIA SPA, TELESPAZIO SPA, GMV AEROSPACE AND DEFENCE SA, INDRA SISTEMAS SA, TECNOBIT SL, HISDESAT SERVICIOS ESTRATEGICOS SA, TOTALFORSVARETS FORSKNINGSINSTITUT, BEYOND GRAVITY SWEDEN AB, SAAB DYNAMICS AKTIEBOLAG, AEROSPACELAB
Duration	01 December 2022 - 30 November 2026
Results	-
Funding	€ 24,372,921.37 (European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103596/EDF https://defence-industry-space.ec.europa.eu/system/files/2023-01/Factsheet_EDF21_Navguard.pdf

Nr 525/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

European Defence Operational Collaborative Cloud

Description	The project "European Defence Operational Collaborative Cloud" (EDOCC) will create a virtual platform that will increase the interoperability, efficiency and resiliency of military operation. This will strengthen collaborative services on the battlefield. The project will study, designand conceptually validate the virtual platform and develop the first version of a services catalogue while identifying appropriate standards and technologies for highperformance and interoperability.
Goal	The objective is to provide EU and Member States a virtual platform based on Cloud technologies that will increase the interoperability, efficiency and resiliency of military operations.
Lead Partner	AIRBUS DEFENCE AND SPACE GMBH
Partners involved	INDRA SISTEMAS SA, LEONARDO - SOCIETA PER AZIONI, RHEINMETALL ELECTRONICS GMBH, SAAB AKTIEBOLAG, ATOS IT SOLUTIONS AND SERVICES SRL, MBDA DEUTSCHLAND GMBH, GTS DEUTSCHLAND GMBH, THALES ITALIA SPA, THALES SIX GTS FRANCE SAS, THALES ESPANA SISTEMAS SA, NAVANTIA S.A., GMV AEROSPACE AND DEFENCE SA, CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI, TELESPAZIO SPA, E 4 COMPUTER ENGINEERING SPA, SIGHUP SRL, BLACKNED GMBH, MYNARIC LASERCOM GMBH, PROVE&RUN, EXENCE SPOLKA AKCYJNA, DEFSECINTEL SOLUTIONS OU, SISTRADE - SOFTWARE CONSULTING SA, WINGS ICT SOLUTIONS TECHNOLOGIES PLIROFORIKIS KAI EPIKOINONION ANONYMI ETAIREIA, AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH, GUARDTIME OU
Duration	01 December 2022 - 30 November 2025
Results	-
Funding	€ 40,000,000.00 (European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103651/EDF https://defence-industry-space.ec.europa.eu/system/files/2023-01/Factsheet_EDF21_EDOCC.pdf

Nr 526/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

real-time Monitoring and Sampling of CB menaces for improved dynamic mapping of threats, vulnerabilities and response capacities

Description	"Real-time Monitoring and Sampling of CB menaces for improved dynamic mapping of threats, vulnerabilities and response capacities" is a research project focused on real-time monitoring of CBRN events paired with innovative sampling capabilities, to enhance dynamic mapping of threats, vulnerabilities and response capacities, inter alia addressing CBRN forensics priorities.
Goal	The project will provide new sensing capabilities. This aims to reinforce CBRN DIM platforms to include low-cost Chemical and Biological monitoring technologies making use of unmanned systems for chemical and biological monitoring and sampling missions
Lead Partner	FONDAZIONE SAFE
Partners involved	AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH, BRUHN NEWTECH AS, AGENZIA NAZIONALE PER LE NUOVE TECNOLOGIE, L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE, CAFA TECH OU, CONSORZIO CREO-CENTRO RICERCHE ELETTRO OTTICHE, RE-LION GROUP B.V.
Duration	01 January 2023 - 31 December 2025
Results	-
Funding	€ 4,401,671.90 (European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103010/EDF https://defence-industry-space.ec.europa.eu/system/files/2022-09/Factsheet_EDF21_MOSAIC_updated.pdf

Nr 527/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Hybrid Energy Grid and Propulsion System

Description	HEGAPS project, stands for: Hybrid Energy Grid And Propulsion System research: Project objective is to create a CPS, cyber physical system to test different options and technologies into an integrated naval grid.
Goal	The specific objective of the project is to create a digital twin environment able to coordinate different assets in different locations by means of digital simulation of multiagent systems (CPS system). This allows Europe to generate a digital complete evaluation scenario that links all these facts into the design or modification of naval vessels with a cyber physical configuration that will validate the complete model. The scenario can then be used as engineering tool for development and validation for existing and new concept of on onboard energy assets.
Lead Partner	SEAPLACE SL
Partners involved	EDAIR TECHNOLOGIES SL, SUPRASYS SL, STADT AS, ATLANTIC ORGANIZATION FOR SECURITY, FUNDACION CENTRO DE TECNOLOGIAS AERONAUTICAS
Duration	01 December 2022 - 30 November 2024
Results	-
Funding	(European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101102515/EDF

Nr 528/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Enhanced Pilot Interfaces & Interactions for fighter Cockpit

Description	The project “Enhanced Pilot Interfaces & Interactions for fighter Cockpit” (EPIIC) will focus on new air power capabilities and seek to ensure the Air dominance of the European defence forces.
Goal	EPIIC aims at tackling the huge technological challenges of the future air warfare and the collaborative combat by identifying, assessing and developing highly innovative technologies and disruptive interactive modalities to be integrated into future fighter cockpits. EPIIC will study and develop some key fighter cockpit–related technologies such as, adaptive HMI, Innovative Virtual Assistant interaction, Large Area Display, Innovative and sovereign Eyes-Out technologies (Helmet Mounted Display and Canopy projection), disruptive Crew monitoring systems and new multi modal interactions.
Lead Partner	THALES AVS FRANCE SAS
Partners involved	INDRA SISTEMAS SA, DASSAULT AVIATION, AIRBUS DEFENCE AND SPACE GMBH, AIRBUS DEFENCE AND SPACE SA, LEONARDO - SOCIETA PER AZIONI, SAAB AKTIEBOLAG, AALBORG UNIVERSITET, DIEHL AEROSPACE GMBH, DEUTSCHES ZENTRUM FUR LUFT - UND RAUMFAHRT EV, ESG ELEKTRONIKSYSTEM- UND LOGISTIK GMBH, GMVIS SKYSOFT SA, HAT.TEC GMBH, INSTITUTUL NATIONAL DE CERCETARE-DEZVOLTARE AEROSPATIALA "ELIE CARAFOLI"- INCAS BUCURESTI, PANEPISTIMIO PATRON, STICHTING KONINKLIJK NEDERLANDS LUCHT - EN RUIMTEVAARTCENTRUM, ROCKWELL COLLINS DEUTSCHLAND GMBH, TECNOBIT SL, TERMA AS, SVEUCILISTE U ZAGREBU FAKULTET ELEKTROTEHNIKE I RACUNARSTVA, INSTA ILS OY, ALMADESIGN CONCEITO E DESENVOLVIMENTO DE DESIGN LDA, EMPORDEF TECNOLOGIAS DE INFORMACAO SA, NEXT2U SRL, TOTALFORSVARETS FORSKNINGSINSTITUT
Duration	01 December 2022 - 31 December 2025
Results	-
Funding	€ 74,999,974.60 (European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103592/EDF https://defence-industry-space.ec.europa.eu/system/files/2023-01/Factsheet_EDF21_EPIIC.pdf

Nr 529/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Platform to Platform Free Space Optical link

Description	The project "Platform to Platform Free Space Optical link" (P2P-FSO) aims at the provision of a free space optical point-to-point communication system.
Goal	P2P-FSO will develop a free space optical point-to-point communication system between military platforms, overcoming challenges regarding high data rate transfer and communication range, depending on terrain and weather conditions. The light source will be a high-power short-wave infrared laser(SWIR).
Lead Partner	NEX VISION
Partners involved	TWOPTICS SYSTEMS DESIGN SL, LAMBDA-X SA, HELLENIC INSTRUMENTS IKE, AMPHINICY LUXEMBOURG SARL
Duration	01 December 2022 - 31 August 2026
Results	-
Funding	€ 3,466,128.63 (European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101102758/EDF https://defence-industry-space.ec.europa.eu/system/files/2022-07/Factsheet_EDF21_P2P-FSO.pdf

Nr 530/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Secure Digital Military Mobility System

Description	The project Secure Digital Military Mobility System (SDMMS), will develop a secure, ICT-based solution that will facilitate direct and secure exchange of information between nations requesting and approving any military movement.
Goal	The SDDMS will be implemented in a federated architecture over multiple instances where each nation can host its own instance allowing for customised configurations, security and data management requirements. Interoperability is a key aspect of the system and will be designed in a manner that allows extensibility and interfacing with other systems at EU, NATO or national level. In the foreseen implementation the SDMMS systems addresses all Functional Requirements of the call and all Initial Common Requirements (ICR) developed by the contributing Ministries of Defence (cMs). As a jointly-developed system for the whole EU, SDMMS contributes oto the Union's strategic autonomy and the reduction of fragmentation between military systems of MS, introducing significant savings as the system can be used as-is without the need of further software development at national level.
Lead Partner	CYBERNETICA AS
Partners involved	NETCOMPANY-INTRASOFT SA, JOTNE CONNECT AS, INDUSTRIEANLAGEN BETRIEBSGESELLSCHAFT MBH, BALTIJOS PAZANGIU TECHNOLOGIJU INSTITUTAS, ITTI SP ZOO, MINISTERUL APARARII NATIONALE, SIA CYBER CIRCLE, OLTIS GROUP AS, INTERCONSULT BULGARIA OOD, INSTITUT PO OTBRANA
Duration	01 December 2022 - 31 May 2025
Results	-
Funding	(European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103172/EDF

Nr 531/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Quantum-based simultaneous high-accuracy resilient navigator and vector strapdown kinematic gravimeter

Description	The project Quantum-based simultaneous high-accuracy resilient navigator and vector strapdown kinematic gravimeter (Q-SiNG) is a step in the development of navigation and timing technologies of guaranteed availability, continuity, and accuracy.
Goal	The goal of Q-SiNG is to build a demonstrator of a quantum-based simultaneous high-accuracy resilient navigator and vector strapdown kinematic gravimeter (Q-SiNG). This PNT engine shall reach a technology readiness level (TRL) 4 thus paving the way for TRL 5. Q-SiNG will be validated in the environments of marine and submarine navigation and gravimetry.
Lead Partner	GEONUMERICS SL
Partners involved	CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE CNRS, CIVITANAVI SYSTEMS SPA, GEOMATICS RESEARCH & DEVELOPMENT SRL, IQUA ROBOTICS SOCIEDAD LIMITADA
Duration	01 December 2022 - 31 December 2025
Results	-
Funding	(European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101102424/EDF

Nr 532/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

AI-based LAnguage technology development framework for Defence ApplicatioNs

Description	The project "Ai-based LAnguage technology development framework for Defence ApplicatioNs" (ALADAN) will develop an AI-based language solutions for defence applications.
Goal	ALADAN will design and develop a disruptive framework of development for Artificial Intelligence (AI) based language solutions for defence applications (i.e. spoken language identification, speech recognition, spoken term search, and text and speech translation), that will rely mainly on the use of non-confidential data for training, to target indomain data, using only a small amount of application-specific data for validation.
Lead Partner	VOCAPIA RESEARCH
Partners involved	LINGEA SRO, IANUS CONSULTING LTD, CROWDEE GMBH
Duration	01 December 2022 - 31 May 2026
Results	-
Funding	€ 3,143,675.82 (European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101102545/EDF https://defence-industry-space.ec.europa.eu/system/files/2022-07/Factsheet_EDF21_ALADAN_0.pdf

Nr 533/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project**	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

ABITS - Advanced Biometrics In Training and Simulation

Description	The ABITS development project will create an indoor tactical training solution with integrated data-driven performance indicators. This training-simulation loop will gather data from physiological sensors, assess trainee well-being through performance quantification, and provide analytics. It will capture and quantify a trainee's psychophysical state, such as attention, stress, and cognitive load, using non-invasive physiological sensors integrated within the training and simulation environment.
Goal	ABITS aims to enhance military simulation and training with quantitative measurements of trainees' psychophysical states based on real-time monitoring from non-invasive physiological sensors. This means that a trainee is not just evaluated on their weapon handling and tactical performance, but also on their psychophysical state during training. ABITS can later evolve into an operational toolset for real-time monitoring and guidance of soldiers, such as gunners, UAV/UGV operators in battle situations.
Lead Partner	GUARDIARIS, RACUNALNISKE APLIKACIJE IN SIMULACIJE D.O.O
Partners involved	SMARTEX SR, VIEWPOINTSYSTEM GMBH
Duration	01 December 2022 - 30 November 2024
Results	-
Funding	(European Defence Fund)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101103036/EDF https://www.abits-edf.eu/

Nr 534/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Training Cybersecurity Skills through Advanced Higher Education Joint Programmes

Description	The project is originated by a consortium originally formed within the European University Alliance ARQUS, with the addition of five SMEs and a Research Centre, all of them covering four different European countries and with a high level of expertise in the field of cybersecurity.
Goal	It aims to train professionals in this field through the following initiatives: (a) a joint European Master in cybersecurity with a mobility path along the four universities; (b) a MOOC in cybersecurity aiming at training a minimum of 800 students from non-ICT sectors in each edition; (c) a scholarship programme to attract highly qualified students; (d) a programme of agreements and incentives to attract faculty, companies and research centres and generate synergies; and (e) the acquisition of key technological infrastructure for support of the programmes. The two training activities (Master and MOOC) have been developed taking into account the main frameworks and recommendations for the development of professional training plans in the field of cybersecurity, such as NICE (National Initiative for Cybersecurity Education) from NIST in the USA or the Joint Task Force (JTF) on cybersecurity, involving ACM, IEEE and other reference organizations.
Lead Partner	UNIVERSIDAD DE GRANADA
Partners involved	UNIVERSIDADE DO MINHO, UNIVERSITA DEGLI STUDI DI PADOVA, VILNIAUS UNIVERSITETAS, SECURIQ SISTEMAS SL, DIGITALSIGN - CERTIFICADORA DIGITAL SA, EUROTUX INFORMATICA S.A., AMPED SRL, QASCOM SRL, FUNDACION IMDEA NETWORKS
Duration	01 October 2023 - 30 September 2027
Results	-
Funding	(Digital Europe Programme)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/43152860/101123445/DIGITAL

Nr 535/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

SPecialised Education programmes in CybersecuriTy and RObotics

Description	SPecialised Education programmes in CybersecuriTy and Robotics (SPECTRO) will focus on the design and delivery of two double-degree master's programmes (ISCED Level 7, 120 ECTS) in two key digital technology areas for the future of Europe: 1) Cybersecurity and 2) Robotics. The two specialised master's programmes, which will also include a minor in Innovation and Entrepreneurship, will be designed and delivered by a consortium consisting of 12 higher education institutions from 7 different countries, 2 innovative SMEs, 1 leading research centre in Information Systems and EIT Digital, a pan-European organisation with in-depth knowledge and experience in the digital skills domain. The master's programmes developed by SPECTRO partners will address the labour market needs, foster strong interactions and mobility between academia and business, strengthen knowledge triangle integration, promote entrepreneurship, and considerably boost the growth of the existing EIT Digital ecosystem, one of the largest digital ecosystems in Europe. In addition to the two master's programme, SPECTRO partners will also develop and deploy a series of self-standing learning modules on topics related to Cybersecurity and Robotics. These modules will lead to four different certifications, which will be released by participating higher education institutions and EIT Digital.
Goal	SPECTRO will expand the specialised education offer in Europe and will contribute to reducing the current shortage of digital specialists in Europe, by providing training to more than 1000 European citizens in Cybersecurity and Robotics.
Lead Partner	EIT DIGITAL
Partners involved	EOTVOS LORAND TUDOMANYEGYETEM, UNIVERSITA DEGLI STUDI DI TRENTO, UNIVERSITEIT TWENTE, UNIVERSITE DE RENNES, TURUN YLIOPISTO, EURECOM GIE, UNIVERSITATEA BABES BOLYAI, KUNGLIGA TEKNISKA HOEGSKOLAN, AALTO KORKEAKOULUSAATIO SR, ALMA MATER STUDIORUM - UNIVERSITA DI BOLOGNA, UNIVERSITE COTE D'AZUR, BUDAPESTI MUSZAKI ES GAZDASAGTUDOMANYI EGYETEM, CYSCALE SYSTEMS SRL, GIM OY
Duration	01 September 2023 - 31 August 2027
Results	-
Funding	(Digital Europe Programme)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/43152860/101123118/DIGITAL

Nr 536/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

DIGITAL4Security – European Masters Programme in Cybersecurity Management & Data Sovereignty

Description	DIGITAL4Security is an innovative and market-led European Masters Programme in Cybersecurity Management & Data Sovereignty that will equip European SMEs and Companies across multiple sectors with the cybersecurity management, regulatory and technical skills they need to prevent and respond to existing and emerging cybersecurity threats, helping to safeguard European industries from cyber-attack.
Goal	The objective is to reskill and upskill graduates, professionals, managers, and business leaders to become 'Cyber Confident' and empowered with the cybersecurity management expertise they need to strengthen their cybersecurity infrastructure and implement robust incident prevention and management procedures. The global objective of this project is to design and implement a highly innovative, effective and sustainable European Cyber-security Masters Programme that will provide a continuous supply of qualified cybersecurity management experts, helping to address the growing cybersecurity skills gap that is endangering the stability of many European industries and public sector institutions.
Lead Partner	UNIVERSITATEA POLITEHNICA DIN BUCURESTI
Partners involved	SCHUMAN ASSOCIATES SCRL, ATAYA & PARTNERS, POLITECNICO DI MILANO, POLSKI KLASTER CYBERBEZPIECZENSTWA CYBERMADEINPOLAND SP. Z O. O., CONTRADER SRL, DIGITAL TECHNOLOGY SKILLS LIMITED, INDEPENDENT PICTURES LIMITED, MATRIX INTERNET APPLICATIONS LIMITED, PROFIL KLETT D.O.O., SERVICENOW IRELAND LIMITED, UNIVERSITA DEGLI STUDI DI BRESCIA, UNIVERSITY OF DIGITAL SCIENCE GGMBH, SKILLNET IRELAND COMPANY LIMITED BY GUARANTEE, IT@CORK ASSOCIATION LIMITED LBG, ADECCO FORMAZIONE SRL, UNIVERSITAT KOBLENZ, VYSOKE UCENI TECHNICKE V BRNE, MUNSTER TECHNOLOGICAL UNIVERSITY, EUROPEAN DIGITAL SME ALLIANCE, DIGITALEUROPE AISBL*, MYKOLO ROMERIO UNIVERSITETAS, SVEUCILISTE U RIJECI, NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTUT BADAWCZY, UNIVERSIDAD INTERNACIONAL DE LA RIOJA SA, NATIONAL COLLEGE OF IRELAND, TERAWE TECHNOLOGIES LIMITED, CY CERGY PARIS UNIVERSITE, BANCO SANTANDER SA, G & N SILENSEC LTD, RED OPEN S.R.L., NOKIA NETWORKS FRANCE, VYTAUTO DIDZIOJO UNIVERSITETAS
Duration	01 October 2023 - 30 September 2027
Results	-
Funding	(Digital Europe Programme)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/43152860/101123430/DIGITAL

Nr 537/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional **project**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

A personalised, customised, work-based training framework for enhanced CYbeR-security skills across indUstrial Sectors

Description	The CYRUS project proposes a novel training system to create an innovation DNA on cybersecurity for TM organisations. A complete set of skills and measures to be vigilant to identify and respond to cyber-attacks will be delivered within the CYRUS framework, which exploits innovative methods for training implementation and delivery. Virtualisation, dedicated cyber-range simulations in operational settings, and work-based learning will allow timely and efficient course delivery, overcome the current hindrance, and raise interest in the awareness program and good practices. The target group of the proposed training sessions are employees at all levels: new entrants building the required competences (skilling), professionals and managers improving and upgrading their expertise (upskilling and reskilling) updating on existing and emerging sector skills.
Goal	Cybersecurity training is fundamental to help employees protect themselves and their companies against cyberattacks and threats. Cybersecurity training empowers employees with the expertise to identify cyber threats and determine the right actions to mitigate them.
Lead Partner	DEEP BLUE SRL
Partners involved	CEFRIEL SOCIETA CONSORTILE A RESPONSABILITA LIMITATA, STICHTING VU, G & N SILENSEC LTD, STOWARZYSZENIE POLSKA PLATFORMA BEZPIECZENSTWA WEWNETRZNEGO, EIT MANUFACTURING CENTRAL GGMBH, ITALIENISCHE HANDELSKAMMER FUR DEUTSCHLAND, UNION INTERNATIONALE DES CHEMINS DE FER, EUROPEAN FEDERATION FOR WELDING JOINING AND CUTTING, UNIVERSITATEA SPIRU HARET, VIESOJI ISTAIGA LIETUVOS INOVACIJU CENTRAS
Duration	01 January 2023 - 31 December 2025
Results	-
Funding	(Digital Europe Programme)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/43152860/101100733/DIGITAL

Nr 538/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Training SMEs for the Digital Decade

Description	Training SMEs for the Digital Decade (SME4DD) will deliver short-term training programmes in three strategic digital technologies for Europe: • Artificial Intelligence, • Blockchain, • Cybersecurity. The short-term training programmes will be designed based on the needs of companies - especially SMEs - and will increase the number of men and women able to design, develop and deploy digital solutions in the economy and across sectors.
Goal	SME4DD will contribute to reduce the existing gap in advanced digital skills in Europe and increase Europe's competitiveness.
Lead Partner	EIT DIGITAL
Partners involved	DIGITALIS JOLET NONPROFIT KORLATOLT FELELOSSEGU TARSASAG, UNIONE CONFCOMMERCIO-IMPRESE PER L' ITALIA MILANO, BUDAPESTI MUSZAKI ES GAZDASAGTUDOMANYI EGYETEM, INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE, TALENT GARDEN ITALIA SRL, KORMANYZATI INFORMATIKAI FEJLESZTESI UGYNOKSEG, HYPER ISLAND PROGRAM AB
Duration	01 January 2023 - 31 December 2025
Results	-
Funding	(Digital Europe Programme)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/43152860/101100768/DIGITAL

Nr 539/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional **project**	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Tech Time 2 Skill : fostering the acquisition of the most in-demand advanced digital skills in AI and Cybersecurity by the European labour force

Description	The Tech Time 2 Skill consortium is a partnership of 7 stakeholders led by BeCode, bringing together key training providers, professional or business associations, and business stakeholders in Spain, France and Belgium. The consortium will work to develop, pilot and deploy 6 high-quality digital training programmes that will meet the SME's needs, giving the opportunity to SME leaders and high skilled workers, as well as job seekers, to be able to design, develop and deploy digital solutions in the economy and across sectors ; while strengthening the competitiveness of European SMEs ; thus contributing to the overall competitiveness of European market in a sustainable and balanced manner between all economic actors of the territory.
Goal	Tech Time 2 Skill is a forward-looking project targeting the acquisition of the most in-demand advanced digital skills in AI and Cybersecurity by the European labour force in order to foster EU's digital talents pools and support the digital transformation of European SMEs in a sustainable manner.
Lead Partner	BECODE
Partners involved	SIMPLON.CO, ASOCIACION FACTORIA F5, PIMEC PETITA I MITJANA EMPRESA DE C ATALUNYA, AGORIA ASBL, AGENCE DU NUMERIQUE
Duration	01 January 2023 - 31 December 2025
Results	-
Funding	(Digital Europe Programme)
www	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/43152860/101100691/DIGITAL

Nr 540/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers,information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

M.Sc. in Cyber Security

Description	The IU International University of Applied Sciences Master's programme in Cyber Security, allows to acquire skills need to protect data and ensure top security measures for systems used by companies worldwide.
Organizer	IU International University of Applied Sciences
Cooperation with	-
Duration	24 months
Thematic Scope	Corporate Governance of IT, Compliance, and Law, Advanced Mathematics, Cyber Security and Data Protection, Advanced Research Methods, Seminar: Advanced Cyber Security, Cryptology, Cyber Risk Assessment and Management, IT Systems: Software, IT Systems: Hardware, Cyber Systems and Network Forensics, Secure Networking, Theoretical Computer Science for IT Security, Project: Current Challenges of Cyber Security
Costs	EUR 497 / per month
No of ECTS credits	120 ECTS
E-learning	A mix of online self-study and on-campus learning.
Tools	-
Job opportunities	After completing your Master's degree in Cyber Security, participants will be a highly sought-after expert who is best qualified for responding efficiently to cyber incidents, as well as for forensic methods of identification and defence. They will have the necessary hard and soft skills required to take responsibility over central security architectures, as well as for confidently advising companies and teams on how to optimise cyber security. They may also be responsible for digital transformations of teams and companies based on 'security by design', and work with external agencies to detect and deter criminal activities. Example job opportunities: • IT Security Architect, • Security Manager, • Cyber Forensics Analyst.
Additional info	-
www	https://www.iu.org/master/cyber-security/?campus=true&clickref=1101lxIecPcs&utm_source=private-network&utm_medium=koop&utm_campaign=partner1100l110537&utm_content=SEO

Nr 541/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers,information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Master of Science in Artificial Intelligence & Cybersecurity

Description	The International Master Degree program in Artificial Intelligence & Cybersecurity aims to develop a system of education and academic exchange, in a spirit of cooperation at European level. The Course is offered in an inter-university international collaboration with the Alpen-Adria University of Klagenfurt (Austria), where some courses will be held. It allows students to obtain a double degree: "Diplom-Ingenieur" from the AlpenAdria University of Klagenfurt and "Laurea Magistrale" from the University of Udine. Students will experiment different approaches to teaching: from traditional foundational courses to practical ones based on projects and reports. The program allows the students to take advantage of the best skills of the two universities in the area of computer science, with particular emphasis on the theoretical and practical applications of Artificial Intelligence and Cybersecurity.
Organizer	Università degli Studi di Udine
Cooperation with	Alpen-Adria University of Klagenfurt
Duration	2 years
Thematic Scope	automated reasoning, complexity and information theory, deep learning, verification and validation techniques in ai and cybersecurity, foundation of cybersecurity and ethics, advanced algorithms, advanced data science, advanced database systems for big data, auditory and tactile interactions, computer network security, computer vision, distributed systems, formal methods for security, foundations of neural networks, generative ai, information retrieval, interactive 3d graphics, quantum computing and communication, recommender systems, video game programming
Costs	-
No of ECTS credits	120
E-learning	Some courses can be attended remotely.
Tools	-
Job opportunities	The Program prepares students to be able to work autonomously as artificial intelligence specialist and cybersecurity specialist. The Program also prepares students for the professions analyst and software designer or analyst, designer and system administrator.
Additional info	-
www	https://www.dmif.uniud.it/en/master/artificial-intelligence-cybersecurity/

Nr 542/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers,information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

CYBER RISK STRATEGY AND GOVERNANCE

Description	Two of Italy's universities, Bocconi and Politecnico di Milano, have joint forces to prepare a new category of professionals in the field of cyber risk. The two-year program, entirely taught in English, is based on a complementary blend of their strengths: Politecnico provides top-flight technological training, while Bocconi shares its expertise on the strategic and economic fronts. It brings together several key knowledge areas to govern cyber risk. Firstly, it offers technical competencies in the fields of computer science and technology, crucial to a deep understanding of the cyber world. Then it reviews managerial, legal and economic principles to place cyber risk into context. Students also practice the soft skills required to communicate cyber challenges.
Organizer	Politecnico di Milano
Cooperation with	Bocconi University
Duration	2 YEARS
Thematic Scope	Introduction to cyber risk; Software methodologies and architectures for security; Cybersecurity technologies, procedures and policies; Artificial intelligence for security; Technology governance; Social engineering; Strategy and governance for cyber risk; Cyber risk and data protection law; Methods and data analytics for risk assessment; Institutional scenarios of cyber risk; Ethical aspects of security and privacy; Soft skills; Data protection, Business and cyber intelligence, Blockchain and cryptoassets, Machine learning in cyber risks, Computer forensics, Fintech models
Costs	-
No of ECTS credits	-
E-learning	-
Tools	-
Job opportunities	This MSc program is built to prepare students to enter the job market in firms, financial institutions, other institutions in public/private sectors as well as consulting companies, with two main profiles: as Cyber Risk Managers graduates will support tasks related to cyber risk management at organizational level, as Data protection and security managers graduates will support tasks related to data protection, privacy management and compliance in order to govern risks on data.
Additional info	-
www	https://www.polimi.it/en/international-prospective-students/laurea-magistrale-programmes-equivalent-to-master-of-science/programme-catalogue/cyber-risk-strategy-and-governance/?utm_source=Keystone&utm_campaign=Keystone&utm_medium=ReadMoreSchoolWebsiteCTA

Nr 543/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers,information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Master's Degree in Cybersecurity

Description	The Cybersecurity master degree offers both the technological and organizational knowledge necessary to define, supervise and coordinate the system and information security of complex IT infrastructures, to organize the protection against cyber attacks, to implement computer incident management processes, to manage recovery in case of successful attack, to develop secure software through advanced methodologies, and finally to deal with the security-related aspects of information systems within corporate risk-management policies and regulations.
Organizer	Sapienza University of Rome
Cooperation with	-
Duration	2-year
Thematic Scope	Cryptography, Distributed Systems, Network Infrastructures, Statistics, Cyber and Computer Law, Ethical Hacking, Malware Analysis and Incident Forencsis, Security Governance, and more
Costs	-
No of ECTS credits	120 ECTS
E-learning	-
Tools	-
Job opportunities	• Security Officers (supervise and coordinate security policies, in particular those related to companies' information management systems, communication, normative aspects and identification of security standards). • Cybersecurity Officers (they are technology experts working inside an organisation of protection from cyberattacks in the different phases of prevention, detection, mitigation and recovery. Their specialisation also include knowledge of active security techniques so as to be ready to appropriately operate in mitigation). • Information Officers (they are in charge of the analysis and re-engineering of existing business processes, by ensuring appropriate security policies, identifying and developing the use of new tools, re-designing corporate physical infrastructures and network access and optimise the corporate know- how).
Additional info	-
www	https://cybersecurity.uniroma1.it/overview

Nr 544/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

30th ACM Conference on Computer and Communications Security (ACM CCS 2023)

Description	The ACM Conference on Computer and Communications Security (CCS) is the flagship annual conference of the Special Interest Group on Security, Audit and Control (SIGSAC) of the Association for Computing Machinery (ACM).
Goal	The conference brings together information security researchers, practitioners, developers, and users from all over the world to explore cutting-edge ideas and results.
Organizer	Technical University of Denmark
Co-organizers/ Patrons	-
Topics	• Cybersecurity • Computer security • Data security • Communications security • Network security • Information security • Cryptography • Mobile security
Date	26-30 November 2023
Costs	5.400,00 kr. - 6.800,00 kr.
www	https://www.sigsac.org/ccs/CCS2023/

Nr 545/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Gartner Security & Risk Management Summit

Description	The Gartner Security & Risk Management Summit is a cybersecurity conference that focuses on enterprise security solutions and risk management strategies. The conference takes place in different locations around the world each year, such as London, Dubai, and Singapore. Attendees of the conference include security professionals, business leaders, and IT experts, who come together to learn about the latest trends and developments in enterprise security.
Goal	Gartner Security & Risk Management Summit helps security and risk management leaders and practitioners to continuously improve the flexibility and responsiveness of security risk management techniques and technology to achieve mission-critical objectives.
Organizer	Gartner
Co-organizers/ Patrons	-
Topics	• Cybersecurity Leadership • Cyber and IT Risk Management • Infrastructure Security • Application and Data Security • Cybersecurity Operations • Technical Insights for Security Practitioners • The CISO Circle • Diversity, Equity and Inclusion • Artificial Intelligence
Date	26 – 28 September 2023
Costs	-
www	https://www.gartner.com/en/conferences/emea/security-risk-management-uk

Nr 546/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

International Conference on the EU Cyber Security and Resilience Acts 2024

Description	the International Conference on the EU Cyber Security and Resilience Acts will bring together product developers and the standards community from 27 countries to prepare for the coming evolution of risk-based frameworks that will address market fragmentation across borders.
Goal	Conference topics will be of interest to the entire standards community, including Certification Bodies, Evaluation Laboratories, Researchers, Evaluators, Policy Makers, Product Developers, Sellers and Buyers interested in the specification, development, evaluation, and certification of IT security in Europe, North America and Asia.
Organizer	Cnxtd (“Connected”) Event Media Corp
Co-organizers/ Patrons	-
Topics	Topics include 5G Standards, IoT Schemes, Artificial Intelligence, Industrial Automation Control Systems (IACS), ETSI EN 303645, CEN/CENELEC JTC13 WG3, EUCC, Union Rolling Work Programme (URWP), NIS Directive, Cloud Standards, Lightweight Standards, IACS, SESIP, Secure Development Lifecycle (SDL), and Global Platform.
Date	11-13 March 2024
Costs	3-Day Conference All Access Registration: €840.00
www	https://eucyberact.org/

Nr 547/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

IOT Solutions World Congress 2024

Description	The Security of Things World Congress is an annual conference that focuses on the internet of things and security.
Goal	The IOTSWC 2024 aims is to give an access to the latest insights and best practices from thought leaders across the industry, as well as exclusive previews of cutting-edge technologies and game-changing innovations.
Organizer	Fira Barcelona
Co-organizers/ Patrons	-
Topics	• Industry IoT • Artificial Intelligence • Renewable Energy • Cloud Computing • Cybersecurity • Big Data • Augmented Reality • Robotic Process Automation • 5G Technologies • Edge Computing • Digital Twin
Date	May 21 - 23, 2024
Costs	€ 200 - € 1,095
www	https://www.iotsworldcongress.com/

Nr 548/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Critical Infrastructure Protection & Resilience Europe

Description	Critical Infrastructure Protection and Resilience Europe brings together leading stakeholders from industry, operators, agencies and governments to collaborate on securing Europe.
Goal	The conference will look at developing on the theme of previous events in helping to create better understanding of the issues and the threats, to help facilitate the work to develop frameworks, good risk management, strategic planning and implementation.
Organizer	IACIPP
Co-organizers/ Patrons	-
Topics	• Power & Energy Sector Symposium • Government, Defence & Space Sector Symposium • Communications Sector Symposium • CBRNE Sector Symposium • Transport Sector Symposium • Information Technology (CIIP) Sector Symposium • Emerging Threats against CI • Crisis Management, Coordination & Communication • The Insider Threat • Risk Mitigation and Management • Technologies to Detect and Protect • Business Continuity Management
Date	03- 05 October 2023
Costs	€ 395 - € 595
www	https://www.cipre-expo.com/

Nr 549/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

26th European Conference on Artificial Intelligence ECAI 2023

Description	ECAI 2023 will feature a full programme of technical papers, as well as many AI-related events of interest for researchers, students and industry professionals. This includes workshops and tutorials, as well as sister conferences for starting researchers (STAIRS) and prestigious applications of AI (PAIS). The conference is supported by the European Association for Artificial Intelligence (EurAI) and the Polish Artificial Intelligence Society (PSSI).
Goal	The aim is to provide a forum for academic and industrial researchers and practitioners to share experiences and insights on the applicability, development and deployment of artificial intelligence.
Organizer	European Association for Artificial Intelligence (EurAI) and the Polish Artificial Intelligence Society (PSSI)
Co-organizers/ Patrons	Jagiellonian University in Kraków, AGH University of Science and Technology, Krakow Technology Park
Topics	• Multi-Agent Systems (MAS) • Game theory and social choice. (GT) • Constraint satisfaction and optimization (CS) • Games and Virtual Environments (GAME) • Human Aspects in AI (HAI) • Data Mining and Data Science (DMS) • Knowledge Representation, Reasoning and semantics (KRR) • Machine Learning (ML) • Multidisciplinary Topics and Applications (MULT) • Speech, Natural Language Processing and Understanding (NLP) • Search, Planning and Scheduling (PLAN) • Robotics (ROB) • Safe, Explainable, and Trustworthy AI (XAI). Includes ethical AI. • Uncertainty in AI (UAI) • Vision (VIS) • AI for Social Good (AISG)
Date	September 30, 2023 - October 5, 2023
Costs	EUR 350 – EUR 1280
www	https://ecai2023.eu/

Nr 550/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

12th International Conference on Prestigious Applications of Intelligent Systems, PAIS 2023

Description	The 12th International Conference on Prestigious Applications of Intelligent Systems, PAIS 2023, will take place on October 3rd in Krakow, Poland, as a sister conference to ECAI 2023, the 26th European Conference on Artificial Intelligence. PAIS is the largest showcase of real applications using AI technology worldwide and is the ideal place to meet developers of successful applications, discuss limitations of current algorithms, needs for future applications and algorithms, as well as novel methods in data collection and machine learning.
Goal	The aim is to provide a forum for academic and industrial researchers and practitioners to share experiences and insights on the applicability, development and deployment of intelligent systems.
Organizer	European Association for Artificial Intelligence (EurAI) and the Polish Artificial Intelligence Society (PSSI)
Co-organizers/ Patrons	Jagiellonian University in Kraków, AGH University of Science and Technology, Krakow Technology Park
Topics	• Evaluation: Responsible AI, impact on humans (AI and HMI, AI and UX) • Technology: Computational and Energy costs and complexity, AI and ML algorithms, search, scheduling, planning, constraints and satisfiability • Methodology: Data collection, storage, and management, Method to acquire information (vision, sensing, AI-human interaction), distributed intelligence, information theory and uncertainty in AI • Application: Data analysis and insights, knowledge representation and reasoning, natural language and semantics processing, autonomous agents' systems
Date	3 October 2023
Costs	EUR 350 – EUR 900
www	https://ecai2023.eu/ECAI2023-3

Nr 551/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

The 10th European Starting AI Researchers' Symposium (STAIRS)

Description	The 10th European Starting AI Researchers' Symposium (STAIRS) is an international meeting that specifically aims to bring together starting researchers (late PhD students or postdocs). STAIRS is meant to provide with the chance to discuss and explore research interests as well as European career objectives and options.
Goal	STAIRS offers a unique and valuable opportunity for young researchers to receive feedback on their recent findings and start up new research collaborations. Specifically, STAIRS' objectives are: • to offer a setting for discussion and feedback on participants' current research, • to provide guidance on future research directions, • to develop a supportive community of scholars and a spirit of collaborative research, • to contribute to the conference goals through interaction with other researchers and participation in ECAI/PAIS/STAIRS conference events.
Organizer	European Association for Artificial Intelligence (EurAI) and the Polish Artificial Intelligence Society (PSSI)
Co-organizers/ Patrons	Jagiellonian University in Kraków, AGH University of Science and Technology, Krakow Technology Park
Topics	• Autonomous Agents & Multi-agent Systems • Case-Based Reasoning • Cognitive Modelling & Cognitive Architectures • Computational Creativity • Constraints, Satisfiability, and Search • Deep Reinforcement Learning • Information Retrieval • Knowledge Representation, Reasoning, and Logic • Machine Learning & Data Mining • Model-Based Reasoning • Natural Language Processing • Planning and Scheduling • Robotics, Perception, Vision and Sensing
Date	1 October 2023
Costs	EUR 300 – EUR 350
www	https://ecai2023.eu/STAIRS2023Call

Nr 552/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

13th International Conference on Artificial Intelligence, Soft Computing and Applications (AIAA 2023)

Description	13th International Conference on Artificial Intelligence, Soft Computing and Applications (AIAA 2023) will provide an excellent international forum for sharing knowledge and results in theory, methodology and applications of Artificial Intelligence, Soft Computing. The Conference looks for significant contributions to all major fields of the Artificial Intelligence, Soft Computing in theoretical and practical aspects.
Goal	The aim of the Conference is to provide a platform to the researchers and practitioners from both academia as well as industry to meet and share cutting-edge development in the field.
Organizer	-
Co-organizers/ Patrons	-
Topics	AI Algorithms, Artificial Intelligence, Artificial Intelligence Tools & Applications, Automatic Control, Bioinformatics, Biomedical Engineering, CAD Design & Testing, Computational, Theories of Learning, Data Mining and Machine Learning Tools, Data Visualization, E-commerce, E-medicine, Evolutionary Computing, Fuzzy Logic, Fuzzy Systems, Heuristic and AI Planning Strategies and Tools, Hybrid Intelligent Systems, Image Processing, Information Retrieval, Intelligent System Architectures, Knowledge Representation, Knowledge-based Systems, Machine Learning, Mechatronics, Morphic Computing, Multimedia & Cognitive Informatics, Nano & Micro-systems, Natural Language Processing, Neural Networks, Parallel Processing, Pattern Recognition, Pervasive Computing and Ambient Intelligence, Probabilistic Reasoning, Programming Languages, Reactive Distributed AI, Reasoning and Evolution, Recent Trends and Developments, Robotics, Rough Sets, Semantic Web,, Techniques and Technologies, Signal or Image Processing, Soft Computing and Applications, Soft Computing Theory and Applications, Software & Hardware Architectures, Software Agents, Symbolic Machine Learning, Telecommunications, Vision Recognition, Wavelet, Web Intelligence Applications & Search
Date	November 25 - 26, 2023
Costs	-
www	https://www.cndc2023.org/aiaa/index

Nr 553/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

23rd International Conference on Construction Applications of Virtual Reality (CONVR2023)

Description	The overarching theme for CONVR2023 is "Managing the digital transformation of construction industry". In addition, the topics of the conference include VR/AR, BIM and digital twins, IoT, artificial intelligence, construction automation and sustainability. In addition, this year program will include workshops with leading international research teams and industry partners and groups.
Goal	The aim of the conference is to share your innovative research and interact with global researchers who will demonstrate the latest advances for the digitalization and optimisation of the built environment.
Organizer	University of Firenze
Co-organizers/ Patrons	-
Topics	• Virtual Reality (VR) and Augmented Reality (AR) • Reality capture and Photogrammetry • H-BIM for heritage management • Simulation and Automation techniques • Computer Vision and Image Processing • Linked Data and Semantic Web for Knowledge Management • Smart Contracts, Distributed Ledger Technologies and Blockchain • Data Science, Machine Learning, and Data-Driven Approaches • Health & Safety • Green and smart buildings • Occupant-centric building design and operation • Building Information Modeling (BIM) • Digital Twins • Internet of Everything • Mobile and wearable computing • Construction site management
Date	November 13-16, 2023
Costs	EUR 350 – EUR 350
www	http://convr2023.com/

Nr 554/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

15th International Conference on Computational Collective Intelligence

Description	ICCCI 2023 is an international scientific conference for research in the field of Computational Collective Intelligence. The proceedings of ICCCI 2023 will be published by Springer in series Lecture Notes in Artificial Intelligence LNCS/LNAI.
Goal	The aim of this conference is to provide an internationally respected forum for scientific research in the computer-based methods of collective intelligence and their applications.
Organizer	Eötvös Loránd University (Hungary), Wrocław University of Science and Technology (Poland)
Co-organizers/ Patrons	IEEE SMC Technical Committee on Computational Collective Intelligence and European Research Center for Information Systems (ERCIS) and International University-VNU-HCM, Vietnam
Topics	The scope of ICCCI 2023 includes all topics related with processing data and knowledge from autonomous sources, especially in: collective processing, knowledge integration, data integration, group decision making, multi-criteria decision making, consensus computing, and social networks.
Date	September 27-29, 2023
Costs	€ 500 - € 600
www	https://iccci.pwr.edu.pl/2023/

Nr 555/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

IEEE 21st International Symposium on Intelligent Systems and Informatics (SISY 2023)

Description	The IEEE 21st International Symposium on Intelligent Systems and Informatics (SISY 2023) to be held on September 21-23, 2023 in Pula, Croatia. Conference proceedings that meet IEEE quality review standards may be eligible for inclusion in the IEEE Xplore Digital Library.
Goal	The aim of SISY 2023 symposium is to offer researchers an opportunity to extend the existing scientific relationships all over the world in the field of Intelligent Systems.
Organizer	IEEE (Institute of Electrical and Electronics Engineers)
Co-organizers/ Patrons	-
Topics	• Computational Intelligence • Intelligent Robotics • Intelligent Mechatronics • Intelligent Manufacturing Systems • Informatics • Applied Mathematics
Date	September 21-23, 2023
Costs	EUR 400 - EUR 450
www	http://conf.uni-obuda.hu/sisy2023/index.html

Nr 556/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

42nd AIAA/IEEE Digital Avionics Systems Conference (DASC)

Description	42nd AIAA/IEEE Digital Avionics Systems Conference (DASC) is the R&D conference in the field of digital avionics offered by two distinguished professional societies, the American Institute of Aeronautics and Astronautics (AIAA) and the Institute of Electrical and Electronics Engineers (IEEE).
Goal	DASC 2023 will bring approximately 300 avionics practitioners together to interact and network with colleagues, learn of the latest avionics technology innovations, and meet the vendors of avionics and avionics systems that supply products and solutions to technical needs.
Organizer	American Institute of Aeronautics and Astronautics (AIAA), Institute of Electrical and Electronics Engineers (IEEE)
Co-organizers/ Patrons	-
Topics	• Flight Operational Efficiency for Reduced Carbon Emissions • Airspace Integration of Autonomous Vehicles • Cognitive Assistants • Machine Learning in Practice • Flight Deck of the Future • Security & Information Assurance • Single pilot and reduced crew operations • Security/Assurance • Certification • Trust in automation
Date	October 1-5, 2023
Costs	$420 - $1050
www	https://2023.dasconline.org/

Nr 557/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Science Robotics

Description	Science Robotics provides a much-needed forum for the latest technological advances and for the critical social, ethical and policy issues surrounding robotics. Bearing the quality hallmark of the Science family of journals, Science Robotics caters to both researchers and general stakeholders. It is multidisciplinary, covering the traditional disciplines of robotics, as well as emerging trends such as advanced materials and bio-inspired designs; it covers all scales, from very large systems to micro/nano robots; its scope is broad, addressing both theoretical advances and practical applications; and it promotes reproducibility, facilitated by online supplementary materials and design/code repositories.
Goal / Target audience	Science Robotics publishes original, peer-reviewed, science- or engineering-based research articles that advance the field of robotics. The journal also features editor-commissioned Reviews.
Publisher	American Association for the Advancement of Science
Topics/ Content	Sub-topics include: actuators, advanced materials, artificial Intelligence, autonomous vehicles, bio-inspired design, exoskeletons, fabrication, field robotics, human-robot interaction, humanoids, industrial robotics, kinematics, machine learning, material science, medical technology, motion planning and control, micro- and nano-robotics, multi-robot control, sensors, service robotics, social and ethical issues, soft robotics, and space, planetary and undersea exploration.
ISSN	2470-9476
www	https://www.science.org/journal/scirobotics

Nr 558/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Nature Machine Intelligence

Description	Nature Machine Intelligence publishes high-quality original research and reviews in a wide range of topics in machine learning, robotics and AI. It also explores and discusses the significant impact that these fields have on other scientific disciplines as well as many aspects of society and industry.
Goal / Target audience	Nature Machine Intelligence provides a platform to discuss these wide implications — encouraging a cross-disciplinary dialogue — with Comments, News Features, News & Views articles and also Correspondence.
Publisher	Springer Nature Switzerland AG
Topics/ Content	Disciplines covered in the journal: AI, robotics, AI and cognitive science, human-robot interaction, machine learning, deep learning, reinforcement learning, robot learning, artificial neural networks, symbolic reasoning, computer vision, natural language processing, genetic and evolutionary computing, neuro-inspired computing, humanoid robots, swarm robotics, bio-inspired robotics, soft robotics, multi-agent systems and so on.
ISSN	2522-5839
www	https://www.nature.com/natmachintell/

Nr 559/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

International Journal of Computer Vision

Description	International Journal of Computer Vision (IJCV) the science and engineering of the rapidly growing field of computer vision.
Goal/Target audience	Regular articles present major technical advances of broad general interest. Survey articles offer critical reviews of the state of the art and/or tutorial presentations of pertinent topics. The journal also features book reviews, position papers, editorials by leading scientific figures, as well as additional on-line material, such as still images, video sequences, data sets, and software.
Publisher	Springer Netherlands
Topics/ Content	• Mathematical, physical and computational aspects of computer vision: image formation, processing, analysis, and interpretation; machine learning techniques; statistical approaches; sensors. • Applications: image-based rendering, computer graphics, robotics, photo interpretation, image retrieval, video analysis and annotation, multi-media, and more. • Connections with human perception: computational and architectural aspects of human vision.
ISSN	09205691, 15731405
www	https://www.springer.com/journal/11263

Nr 560/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Neural Networks

Description	Neural Networks provides a forum for developing and nurturing an international community of scholars and practitioners who are interested in all aspects of neural networks, including deep learning and related approaches to artificial intelligence and machine learning. Neural Networks welcomes submissions that contribute to the full range of neural networks research, from cognitive modeling and computational neuroscience, through deep neural networks and mathematical analyses, to engineering and technological applications of systems that significantly use neural network concepts and learning techniques.
Goal / Target audience	The journal publishes articles, letters, and reviews, as well as letters to the editor, editorials, current events, and software surveys.
Publisher	Elsevier Ltd.
Topics/ Content	Articles are published in one of four sections: learning systems, cognitive and neural science, mathematical and computational analysis, engineering and applications.
ISSN	08936080, 18792782
www	https://www.sciencedirect.com/journal/neural-networks

Nr 561/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Artificial Intelligence Review

Description	The Review publishes state-of-the-art research reports and critical evaluations of applications, techniques and algorithms from these fields. Artificial Intelligence Review also presents refereed survey and tutorial articles, as well as reviews and commentary on significant developments from these disciplines.
Goal / Target audience	Artificial Intelligence Review serves as a forum for the work of researchers and application developers from Artificial Intelligence, Cognitive Science and related disciplines.
Publisher	Springer Netherlands
Topics/ Content	• Artificial Intelligence • Cognitive Science
ISSN	02692821, 15737462
www	https://www.springer.com/journal/10462

Nr 562/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Knowledge-Based Systems

Description	Knowledge-based Systems is an international and interdisciplinary journal in the field of artificial intelligence.
Goal / Target audience	The journal publish original, innovative and creative research results in the field of artificial intelligence, and is designed to focus on research in knowledge-based and other artificial intelligence techniques-based systems with the following objectives and capabilities: to support human prediction and decision-making through data science and computation techniques; to provide a balanced coverage of both theory and practical study in the field; and to encourage new development and implementation of knowledge-based intelligence models, methods, systems, and software tools, with applications in business, government, education, engineering and healthcare.
Publisher	Elsevier
Topics/ Content	This journal's current leading topics are but not limited to: • Machine learning theory, methodology and algorithms, • Data science theory, methodologies and techniques, • Knowledge presentation and engineering, • Recommender systems and E-service personalization, • Intelligent decision support systems, prediction systems and warning systems, • Computational Intelligence systems, • Data-driven optimization, • Cognitive interaction and brain–computer interface, • Knowledge-based computer vision techniques.
ISSN	09507051
www	https://www.sciencedirect.com/journal/knowledge-based-systems

Nr 563/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Pattern Recognition

Description	The journal Pattern Recognition was established some 50 years ago, as the field emerged in the early years of computer science.
Goal/Target audience	The journal accepts papers making original contributions to the theory, methodology and application of pattern recognition in any area, provided that the context of the work is both clearly explained and grounded in the pattern recognition literature.
Publisher	Elsevier Ltd.
Topics/ Content	pattern recognition
ISSN	00313203
www	https://www.sciencedirect.com/journal/pattern-recognition

Nr 564/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference/ **Contest**	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Drone Contest

Description	The Leonardo Drone Contest is an Open Innovation challenge designed and launched by Leonardo in collaboration with six Italian universities, to encourage the development of Artificial Intelligence applied to Uncrewed Systems.
Goal	The aim of the project is to encourage the creation of an innovation 'ecosystem' that involves and brings together the capabilities of large companies, universities, small and medium enterprises, and national spin-offs and start-ups. In particular, Leonardo is supporting the activities of six PhD students (one per university) from the Politecnico of Turin and Milan and from the Universities of Bologna, Sant'Anna of Pisa, Rome Tor Vergata and Federico II of Naples. For three years, these students have been engaged in developing an autonomous drone guidance system, sharing both university and Leonardo resources and knowledge. For the trial and competition, the six PhD students each had their own multidisciplinary team, made up of students from different courses and levels in the engineering area, where each member enriched their experience through teamwork and by achieving the contest's objectives.
Organizer	Leonardo S.p.A.
Co-organizers/ Patrons	-
Topics	Launched in 2019, the Leonardo Drone Contest has taken place over a three-year period and consisted of two annual events, a scientific symposium, and a competition. The first two competitions in 2020 and 2021 saw the six universities' teams challenge each other in increasingly competitive rounds on the 'airfield' of Leonardo's Turin site. It was a true 'drone game', with the level complexity increasing each year. The 2022 competition took place on 6 and 7 October and marks the conclusion of this experimental cycle
Date	6 - 7 October 2022
Costs	-
www	https://www.leonardo.com/en/innovation-technology/open-innovation/drone-contest

Nr 565/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

World Congress on Robotics, AI & Computer Science (USF Mobile Robots Conference)

Description	The theme of the conference is: Learning and Demonstrating the Surging Interest in Machine Learning and Mobile Robotics. The event comprises keynote speech, many oral presentations, poster presentations, interactive sessions, exhibitions, plenary sessions, with its high quality, it provides an exceptional value for industry researchers and all participants. S
Goal	USF Mobile Robots aims to strengthen the participants action and an impact on national, regional and international scales through a multidisciplinary program that features the latest successful. This assemblage offers the field to worldwide analysts, educators, specialists, researchers, scientific skills, understudies, business representatives and vernal analysts over the world to voice their assessment disclosures all over the globe.
Organizer	United Scientific Forum
Co-organizers/ Patrons	-
Topics	The conference covers all important aspects of Machine Learning topics such as but not limited to Accuracy, Algorithm, Artificial Neural Networks, Bias Error, Clustering, Deep Learning, Dimension, Hidden Layers, etc.
Date	February 28-29, 2024
Costs	$210 - $840
www	https://unitedscientificforum.com/robotics/

Nr 566/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

2nd International Experts Summit on Artificial Intelligence and Robotic Technology (IESAIRT 2024)

Description	IESAIRT2024 provides a platform of international standards where you can discuss and share knowledge on Artificial Intelligence and Robotic Technology to bring a unique forum for exchanging the information regarding the latest developments, finding solutions and enriching the knowledge. In addition to Presentations, Workshops, and Discussions, the conference also offers a unique venue for renewing professional relationships, and providing plenty of networking opportunities during the summit.
Goal	The aim of the IESAIRT2024 is to share innovative and great results in Artificial Intelligence and Robotic Technology.
Organizer	Meghaz Meetings
Co-organizers/ Patrons	-
Topics	Machine learning, Cognitive Intelligence, Multi-robot systems, Social Intelligence, Intelligent interactive technology, Human-robot interaction, Human-machine interface/integration, Teleoperation/ telerobotics/ haptics, Behavioral Intelligence, Neuroscience based control, Genetic Intelligence, Artificial Intelligence, Computational intelligence, Nanorobots, Swarm robotics, Glossary of robotics, Environmental interaction and navigation, Bionics and Biomimetics, Intelligent Mechatronics and Robotics, Robotics in Agriculture and Forestry, Robotics in Pharmacy and Health Care, Robotics in Construction, Robotics in Hazardous Fields, Frontiers in Robotics and AI, Robotic Mapping Autonomous Robot, Cognitive Robotics, Soft Robotics and Mobile Robot, Evolutionary Robotics and Robotic aspects
Date	August 07-09, 2024
Costs	$289 - $699
www	https://www.meghazmeetings.com/iesairt-2024/

Nr 567/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

International Forum on Applied Science and Engineering (ASEFORUM2024)

Description	The main agenda of this conference is to bring together world-leading academics, practitioners, industry leaders, policymakers, and business professionals from the fields of Applied Science and Engineering to develop practical solutions for current challenges in these fields. The conference series has featured plenary talks, keynote talks, special sessions, poster presentations, workshops, and contributed papers each year.
Goal	The aim of ASEFORUM2024 is to be a premier international forum to highlight novel developments, share new ideas, research results, and development experiences, and provide networking opportunities with peers to help establish connections for early career scientists to meet a diverse mix of researchers, decision-makers to strengthen existing connections and forge new ones.
Organizer	Continuum Forums
Co-organizers/ Patrons	-
Topics	Applied Physics, Applied Biosciences and Bioengineering, Applied Dentistry and Oral Sciences Biomedical Engineering, Applied Microbiology, Applied Neuroscience and Neural Engineering, Materials Science and Engineering, Chemical and Molecular Sciences, Nanotechnology and Applied Nanosciences, Robotics and Automation, Aerospace Science and Engineering, Surface, Sciences and Technology, Environmental Sciences, Green Sustainable Science and Technology, Earth Sciences and Geography, Energy Science and Technology, Optics and Lasers, Acoustics and Vibrations, Quantum Science and Technology, Applied Thermal Engineering, Fluid Science and Technology, Computing and Artificial Intelligence, Mechanical Engineering, Civil Engineering, Electrical, Electronics and Communications Engineering, Applied Industrial Technologies, Food Science and Technology, Marine Science and Engineering, Transportation and Future Mobility, Agricultural Science and Technology, Additive Manufacturing Technologies
Date	March 04-06, 2024
Costs	$299 - $899
www	https://www.continuumforums.com/2024/aseforum?utm_source=BenchmarkEmail&utm_campaign=ASEFORUM2024_08-30&utm_medium=email

Nr 568/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

2nd International Conference on Aerospace and Aeronautical Engineering

Description	Aerospace and Aeronautical Engineering-2024 makes a complete platform of engineering concerned with the design, development, production of aircraft, spacecraft. The field has traditionally focused on problems related to atmospheric and space flight, with two major and overlapping branches. And is concerned with the manufacture, testing and maintenance of flight-capable machines.
Goal	The aimis to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Aerospace and Aeronautical Engineering.
Organizer	Pangea Global Events
Co-organizers/ Patrons	-
Topics	Space Science, Astrophysics, Flight Simulation, Aeroacoustics, Ground Handling Process, Spacecraft Operation, Aircraft Noise, Control and Climate Effects, Energetics and Propulsion, Testing and Performance, Ground Handling Process, Robotics and Intelligent Systems, Air Transport Systems, Scientific Sessions, Aerospace Communications, Deep Space Exploration, Propulsion and Combustion, Unmanned Air Vehicles, Air Traffic Management, Avionics and Mission Technologies, Crew Training System, Transmission and, Landing Systems, Signal and Image Processing, Thermal Management, Aviation Safety and Regulation
Date	March 21-23, 2024
Costs	$399 - $999
www	https://www.pagesconferences.com/2024/aerospace-engineering-technology?utm_source=BenchmarkEmail&utm_campaign=Aerospace-2024_08-31&utm_medium=email

Nr 569/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Global Summit on Sensors and Sensing Technology (SENTECH2023)

Description	The SENTECH2023 will be a 3 days event that means to gather the key players of the Sensors and Sensing Technology community and related sectors. This event is launched with the aims to become an established event, attracting global participants, intent on sharing, exchanging and exploring new avenues of Sensors and Sensing Technology - related scientific and commercial developments. A wide-ranging scientific program consisting of plenary lectures, keynote lectures, Invited lectures, parallel sessions, as well as poster sessions for young scientists covering all topics in Sensors and Sensing Technology will be scheduled. This conference provides a wonderful opportunity for you to enhance your knowledge about the newest interdisciplinary approaches in Sensors and Sensing Technology.
Goal	SENTECH2023 aims to bring together the renowned researchers, scientists and scholars to exchange ideas, to present sophisticated research works and to discuss hot topics in the field and share their experiences on all aspects of Sensors and Sensing Technology.
Organizer	The Scientistt
Co-organizers/ Patrons	-
Topics	Mechanical Sensors, Physical Sensors, Optical Sensors, Electromagnetic Sensors, Photonic Sensors, Biosensors, Sensor Applications, Infrared Sensors, Devices and Thermography, Polymer Materials for Sensors, Micro and Nanosensors, Chemical Sensors, Remote Sensors and Telemetry, Sensor Interfacing and Signal Conditioning, Nanomaterials and Electronics, Technology for Sensors, Sensing and Imaging, Multi Sensor Fusion, Sensing for Robotics and Automation, Wearable Sensors, Devices and Electronics, Semiconductor Materials for Sensors, Humidity Sensors, Signal Processing, Deep Learning in Sensor Systems, Sensor Networks, Actuators and Sensor Power Systems, Machine/Deep Learning and Artificial Intelligence in Sensing and Imaging, Smart/Intelligent Sensors, MEMS and NEMS, 3D Sensing
Date	November 16-18, 2023
Costs	$299 - $999
www	https://www.thescientistt.com/2023/sensors-technology?utm_source=BenchmarkEmail&utm_campaign=SENTECH2023_09-05&utm_medium=email

Nr 570/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

12th Computing Conference 2024

Description	Computing Conference (formerly called Science and Information (SAI) Conference) is a research conference held in London, UK since 2013. The conference series has featured keynote talks, special sessions, poster presentation, tutorials, workshops, and contributed papers each year.
Goal	The goal of the conference is to be a premier venue for researchers and industry practitioners to share new ideas, research results and their enriching experiences in various fields. It is one of the best respected conferences in the area of computer science.
Organizer	The Science and Information (SAI) Organization
Co-organizers/ Patrons	-
Topics	• Computing • Computer Vision • Technology Trends • Ambient Intelligence • Artificial Intelligence • Data Science • Security • e-Learning
Date	11-12 July 2024
Costs	GBP £300 - GBP £650
www	https://saiconference.com/computing

Nr 571/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Energy and AI

Description	Energy and AI provides a fast and authoritative open access platform to disseminate the latest research progress in the cross-disciplinary area of energy and artificial intelligence (AI). The journal focuses on innovative applications of AI that address the critical challenges in energy systems, energy materials, energy chemistry, energy utilization & conversion, and energy & society, as well as other important pressing issues in energy research. The journal also considers papers on the development of bespoke AI technologies and methodologies for advancing energy, decarbonization and sustainable development, such as data-driven approaches, optimization algorithms and AI ethics.
Goal / Target audience	Energy and AI aims to become a leading journal for cutting-edge research at the interface between energy and AI. Papers purely focusing on a single aspect of energy or AI are not suitable for the journal.
Publisher	Elsevier BV
Topics/ Content	• Automation of science discovery related to energy materials and chemistry • Digital twinning or big data analytics of complex energy processes/systems • Data-driven design of energy materials, devices and systems • Internet-of-things and cyber-physical energy systems • AI for human factors in energy related activities • Virtual reality applied to energy and environment • Autonomous systems for energy efficiency maximalization • Hardware for data collections in energy systems • Data Science for energy applications • Hybrid data-driven and physical modelling for energy related problems • Intelligent control of energy systems • AI, energy and society • AI safety, reliability and ethics within energy applications • AI for life-cycle assessment or energy and decarbonization roadmaps • Energy robotics
ISSN	26665468
www	https://www.sciencedirect.com/journal/energy-and-ai

Nr 572/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Expert Systems with Applications

Description	Expert Systems With Applications is a refereed international journal whose focus is on exchanging information relating to expert and intelligent systems applied in industry, government, and universities worldwide.
Goal/Target audience	The thrust of the journal is to publish papers dealing with the design, development, testing, implementation, and/or management of expert and intelligent systems, and also to provide practical guidelines in the development and management of these systems.
Publisher	Elsevier Ltd.
Topics/ Content	The journal will publish papers in expert and intelligent systems technology and application in the areas of, but not limited to: finance, accounting, engineering, marketing, auditing, law, procurement and contracting, project management, risk assessment, information management, information retrieval, crisis management, stock trading, strategic management, network management, telecommunications, space education, intelligent front ends, intelligent database management systems, medicine, chemistry, human resources management, human capital, business, production management, archaeology, economics, energy, and defense. Papers in multi-agent systems, knowledge management, neural networks, knowledge discovery, data and text mining, multimedia mining, and genetic algorithms will also be published in the journal.
ISSN	09574174
www	https://www.sciencedirect.com/journal/expert-systems-with-applications

Nr 573/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Physics of Life Reviews

Description	Physics of Life Reviews is an international journal appearing quarterly, that publishes review articles on physics of living systems, complex phenomena in biological systems, and related fields of artificial life, robotics, mathematical bio-semiotics, and artificial intelligent systems. This journal is a unifying force, going across the barriers between disciplines, addressing all living systems from molecules to populations and from genetics to mind and artificial systems modeling these phenomena.
Goal/Target audience	Physics of Life Reviews intends to keep the active researcher abreast of developments on a wide range of topics by publishing timely reviews, which are more than mere literature surveys but normally less than a full monograph. Although most of the reviews will be of a specialist nature, each review should contain enough introductory material to make the main points intelligible to a non-specialist and to inspire and facilitate interdisciplinary research.
Publisher	Elsevier
Topics/ Content	physics of living systems, complex phenomena in biological systems, and related fields of artificial life, robotics, mathematical bio-semiotics, and artificial intelligent systems
ISSN	18731457, 15710645
www	https://www.sciencedirect.com/journal/physics-of-life-reviews

Nr 574/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Engineering Applications of Artificial Intelligence

Description	Papers submitted to "Engineering Applications of Artificial Intelligence" should report some novel aspects of AI used for a real world engineering application and also validated using some public data sets for easy replicability of the research results.
Goal / Target audience	This journal provides an international forum for rapid publication of work describing the practical application of AI methods in all branches of engineering.
Publisher	Elsevier Ltd.
Topics/ Content	Focal points of the journal include, but are not limited to innovative applications of: • Internet–of–things and cyber-physical systems, • Intelligent transportation systems & smart vehicles, • Big data analytics, understanding complex networks, • Neural networks, fuzzy systems, neuro-fuzzy systems, • Deep learning and real world applications, • Self-organizing, emerging or bio-inspired system, • Global optimization, Meta-heuristics and their applications: Evolutionary Algorithms, swarm intelligence, nature and biologically inspired meta-heuristics, etc., • Architectures, algorithms and techniques for distributed AI systems, including multi-agent based control and holonic control, • Decision-support systems, • Aspects of reasoning: abductive, case-based, model-based, non-monotonic, incomplete, progressive and approximate reasoning, • Applications of chaos theory and fractals, • Real-time intelligent automation, and their associated supporting methodologies and techniques, including control theory and industrial informatics, • Knowledge processing, knowledge elicitation and acquisition, knowledge representation, knowledge compaction, knowledge bases, expert systems, • Perception, e.g. image processing, pattern recognition, vision systems, tactile systems, speech recognition and synthesis, • and more.
ISSN	09521976
www	https://www.sciencedirect.com/journal/engineering-applications-of-artificial-intelligence

Nr 575/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Machine Learning

Description	The journal publishes articles reporting substantive results on a wide range of learning methods applied to a variety of learning problems.
Goal/Target audience	The journal features papers that describe research on problems and methods, applications research, and issues of research methodology. Papers making claims about learning problems or methods provide solid support via empirical studies, theoretical analysis, or comparison to psychological phenomena. Applications papers show how to apply learning methods to solve important applications problems. Research methodology papers improve how machine learning research is conducted.
Publisher	Springer Netherlands
Topics/ Content	• Learning Problems: Classification, regression, recognition, and prediction; Problem solving and planning; Reasoning and inference; Data mining; Web mining; Scientific discovery; Information retrieval; Natural language processing; Design and diagnosis; Vision and speech perception; Robotics and control; Combinatorial optimization; Game playing; Industrial, financial, and scientific applications of all kinds. • Learning Methods: Supervised and unsupervised learning methods (including learning decision and regression trees, rules, connectionist networks, probabilistic networks and other statistical models, inductive logic programming, case-based methods, ensemble methods, clustering, etc.); Reinforcement learning; Evolution-based methods; Explanation-based learning; Analogical learning methods; Automated knowledge acquisition; Learning from instruction; Visualization of patterns in data; Learning in integrated architectures; Multistrategy learning; Multi-agent learning.
ISSN	15730565, 08856125
www	https://www.springer.com/journal/10994

Nr 576/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Neurocomputing

Description	Neurocomputing publishes articles describing recent fundamental contributions in the field of neurocomputing. Neurocomputing theory, practice and applications are the essential topics being covered.
Goal/Target audience	Neurocomputing covers practical aspects with contributions on advances in hardware and software development environments for neurocomputing, including, but not restricted to, simulation software environments, emulation hardware architectures, models of concurrent computation, neurocomputers, and neurochips (digital, analog, optical, and biodevices). Neurocomputing reports on applications in different fields, including, but not restricted to, signal processing, speech processing, image processing, computer vision, control, robotics, optimization, scheduling, resource allocation and financial forecasting.
Publisher	Elsevier
Topics/ Content	Neurocomputing welcomes theoretical contributions aimed at winning further understanding of neural networks and learning systems, including, but not restricted to, architectures, learning methods, analysis of network dynamics, theories of learning, self-organization, biological neural network modelling, sensorimotor transformations and interdisciplinary topics with artificial intelligence, artificial life, cognitive science, computational learning theory, fuzzy logic, genetic algorithms, information theory, machine learning, neurobiology and pattern recognition.
ISSN	09252312
www	https://www.sciencedirect.com/journal/neurocomputing

Nr 577/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Internet of Things (Netherlands)

Description	Internet of Things; Engineering Cyber Physical Human Systems is a comprehensive journal encouraging cross collaboration between researchers, engineers and practitioners in the field of IoT & Cyber Physical Human Systems.
Goal/Target audience	The journal offers a unique platform to exchange scientific information on the entire breadth of technology, science, and societal applications of the IoT.
Publisher	Elsevier BV
Topics/ Content	• Theory and fundamental research (research that addresses the core underlying scientific principles dealing with the analysis and algorithmics of "IoT ecosystem" as a multicomponent system with complex and dynamic dependences at large-scale) • Software development, technology and engineering (key enabling IoT technologies related to sensors, actuators and machine intelligence. Development and deployment IoT tools and platforms to ensure security, reliability and efficiency) • Applications of IoT (new Applications of connected products and/or connected business processes to create new business value and business models) • Societal aspects of IoT (research in cyber-human systems that reflect human understanding and interaction with the physical world and (semi) autonomous systems)
ISSN	25426605
www	https://www.sciencedirect.com/journal/internet-of-things

Nr 578/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

International Journal of Intelligent Systems

Description	International Journal of Intelligent Systems serves as a forum for individuals interested in tapping into the vast theories based on intelligent systems construction. With its peer-reviewed format, the journal publishes original research and review articles written by today's experts in the field.
Goal/Target audience	International Journal of Intelligent Systems serves as a forum for individuals interested in tapping into the vast theories based on intelligent systems construction.
Publisher	John Wiley and Sons Ltd
Topics/ Content	• Control methods • Distributed artificial intelligence • Knowledge representation and reasoning • Learning settings • Machine learning algorithms • Machine learning approaches • Machine learning paradigms • Natural language processing
ISSN	1098111X, 08848173
www	https://onlinelibrary.wiley.com/journal/1098111x https://www.hindawi.com/journals/ijis/

Nr 579/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Pattern Recognition Letters

Description	Pattern Recognition Letters aims at rapid publication of concise articles of a broad interest in pattern recognition.
Goal / Target audience	Subject areas include all the current fields of interest represented by the Technical Committees of the International Association of Pattern Recognition, and other developing themes involving learning and recognition.
Publisher	Elsevier
Topics/ Content	• Statistical, structural, syntactic pattern recognition; • Neural networks, machine learning, data mining; • Discrete geometry, algebraic, graph-based techniques for pattern recognition; • Signal analysis, image coding and processing, shape and texture analysis; • Computer vision, robotics, remote sensing; • Document processing, text and graphics recognition, digital libraries; • Speech recognition, music analysis, multimedia systems; • Natural language analysis, information retrieval; • Biometrics, biomedical pattern analysis and information systems; • Special hardware architectures, software packages for pattern recognition
ISSN	01678655
www	https://www.sciencedirect.com/journal/pattern-recognition-letters

Nr 580/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Minds and Machines

Description	Minds and Machines affords an international forum for the discussion and debate of important and controversial issues concerning significant developments within its areas of editorial focus. Among the features that make this journal distinctive within the field are these: • strong stands on controversial issues are especially encouraged, • important articles exceeding normal journal length may appear, • special issues devoted to specific topics are a regular feature, • critical responses to previously published pieces are invited, • review essays discussing current problem situations will appear.
Goal / Target audience	This journal is intended to foster a tradition of criticism within the AI and philosophical communities on problems and issues of common concern. Its scope explicitly encompasses philosophical aspects of computer science.
Publisher	Springer Netherlands
Topics/ Content	• Machines and Mentality • Knowledge and Its Representation • Epistemic Aspects of Computer Programming • Connectionist Conceptions • Artificial Intelligence and Epistemology • Computer Methodology • Computational Approaches to Philosophical Issues • Philosophy of Computer Science • Simulation and Modelling • Ethical Aspects of Artificial Intelligence
ISSN	09246495, 15728641
www	https://www.springer.com/journal/11023

Nr 581/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Fuzzy Sets and Systems

Description	Fuzzy Sets and Systems publishes high-quality research articles, surveys as well as case studies. The scope of the journal Fuzzy Sets and Systems has expanded so as to account for all facets of the field while emphasizing its specificity as bridging the gap between the flexibility of human representations and the precision and clarity of mathematical or computerized representations, be they numerical or symbolic.
Goal / Target audience	The journal welcomes original and significant contributions in the area of Fuzzy Sets whether on empirical or mathematical foundations, or their applications to any domain of information technology, and more generally to any field of investigation where fuzzy sets are relevant. Applied papers demonstrating the usefulness of fuzzy methodology in practical problems are particularly welcome.
Publisher	Elsevier
Topics/ Content	Topics related to fuzzy sets.
ISSN	01650114
www	https://www.sciencedirect.com/journal/fuzzy-sets-and-systems

Nr 582/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Neural Computing and Applications

Description	Neural Computing & Applications is an international journal which publishes original research and other information in the field of practical applications of neural computing and related techniques such as genetic algorithms, fuzzy logic and neuro-fuzzy systems.
Goal / Target audience	This journal provides an international forum for publication original research and other information in practical applications of neural computing and related techniques.
Publisher	Springer London
Topics/ Content	All items relevant to building practical systems are within its scope, including but not limited to: adaptive computing, algorithms, applicable neural networks theory, applied statistics, architectures, artificial intelligence, benchmarks, case histories of innovative applications, fuzzy logic, genetic algorithms,hardware implementations, hybrid intelligent systems, intelligent agents, intelligent control systems, intelligent diagnostics, intelligent forecasting, machine learning, neural networks, neuro-fuzzy systems, pattern recognition, performance measures, self-learning systems, software simulations, supervised and unsupervised learning methods, system engineering and integration
ISSN	09410643, 14333058
www	https://www.springer.com/journal/521

Nr 583/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Intelligent Systems with Applications

Description	Intelligent Systems with Applications (ISWA) is a peer reviewed open-access journal which focuses on the achievements of research and applications related to intelligent systems (IS).
Goal / Target audience	The journal audience comprises academia, industry, and practitioners.
Publisher	Elsevier BV
Topics/ Content	The journal aims to publish papers dealing with, but not limited to, the following research fields: • Knowledge Representation and Reasoning, • Machine Learning (ML) and Neural Computing, E • volutionary Computation, • Fuzzy Systems, • Intelligent Information Processing, • Intelligent Control and Robotics, • Multi-agent Systems and Programming. The journal welcomes submissions of IS-applications in various areas: Intelligent Cities, Industries, Consuming, Medical Treatment and Health, Agriculture, Business and Finance, Internet of Things (IoT). Research addressing IS-applications in other fields is also encouraged.
ISSN	26673053
www	https://www.sciencedirect.com/journal/intelligent-systems-with-applications

Nr 584/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Cognitive Systems Research

Description	Cognitive Systems Research is dedicated to the study of human-level cognition. As such, it welcomes papers which advance the understanding, design and applications of cognitive and intelligent systems, both natural and artificial. Cognitive Systems Research plays a special role in fostering and promoting the 'BICA Challenge' to create a real-life computational equivalent of the human mind by devoting two special issues to BICA AI (Brain-Inspired Cognitive Architectures for Artificial Intelligence) related topics each year.
Goal / Target audience	The journal brings together a broad community studying cognition in its many facets in vivo and in silico, across the developmental spectrum, focusing on individual capacities or on entire architectures. It aims to foster debate and integrate ideas, concepts, constructs, theories, models and techniques from across different disciplines and different perspectives on human-level cognition.
Publisher	Elsevier
Topics/ Content	• Cognitive Science (including Philosophy of Cognitive Science) • Artificial Intelligence/Computer Science • Cognitive Robotics • Developmental Science • Psychology, and Neuroscience • Neuromorphic Engineering
ISSN	13890417
www	https://www.sciencedirect.com/journal/cognitive-systems-research

Nr 585/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Granular Computing

Description	Granular Computing constitutes an extensive body of knowledge, which dwells upon individual formalisms of information granules (established within various settings including set theory, interval calculus, fuzzy sets, rough sets, shadowed sets, probabilistic granules) and unifies them to form a coherent methodological and developmental environment.
Goal / Target audience	The Journal of Granular Computing provides a rapid dissemination of timely and important results. The aim is to bring recent advances in the dynamically expanding area including its fundamentals, algorithmic developments, and applications. It supports the integration of theoretical and practical results leading to advanced applications. The journal establishes an international forum and aims to address the needs of the academic community as well as to appeal to practitioners and graduate students by publishing time-to-time review material and surveys. It serves as a platform fostering comparisons, extensions, and innovative applications.
Publisher	Springer Nature Switzerland AG
Topics/ Content	The journal covers a broad spectrum of subjects of Granular Computing embracing the theory, methodology, and applied side of the discipline including case studies. Theoretical and applied studies involving fuzzy sets, interval analysis, rough sets, shadowed sets, probabilistic sets well positioned in the synergistic setup of Granular Computing and making reference to the fundamentals of the area are welcome.
ISSN	23644974, 23644966
www	https://www.springer.com/journal/41066

Nr 586/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Quantum Machine Intelligence

Description	This single-blind peer-reviewed journal publishes original articles on cutting-edge experimental and theoretical research in all areas of quantum artificial intelligence. The Journal is unique in promoting a synthesis of machine learning, data science and computational intelligence research with quantum computing developments.
Goal / Target audience	Its primary goal is to foster the utilization of quantum computing for real-world problems so as to pave the way towards the next generation of artificial intelligence systems. The Journal also publishes innovative papers reporting on machine intelligence theories, methods and applications inspired by physics and nature, e.g. computational intelligence, fuzzy systems, evolutionary computation, machine and deep learning.
Publisher	Springer Science and Business Media Deutschland GmbH
Topics/ Content	Selected areas and topics of interest include, but are not limited to: • Quantum Machine Learning, • Quantum Computing for Artificial Intelligence, • Artificial Intelligence for Quantum Information Processing, • Quantum and Bio-inspired Computational Intelligence, • Quantum Annealing and Optimization.
ISSN	25244914, 25244906
www	https://www.springer.com/journal/42484

Nr 587/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Journal of Artificial Intelligence and Soft Computing Research

Description	Journal of Artificial Intelligence and Soft Computing Research is a dynamically developing international journal focused on the latest scientific results and methods in traditional artificial intelligence, neural networks and soft computing techniques.
Goal / Target audience	The goal of the journal is to bring together scientists representing traditional artificial intelligence, neural networks and soft computing techniques and various research communities.
Publisher	De Gruyter Open Ltd.
Topics/ Content	AI in Modelling and Simulation, AI in Scheduling and Optimization, Automated Reasoning and Inference, Bioinformatics, Cognitive Aspects of AI, Computer Vision and Speech Understanding, Data Mining, Distributed Intelligent Processing, Evolutionary Design, Expert Systems, Fuzzy Modelling and Control, Hardware Implementations, Heuristic Search, Hybrid Models, Information Retrieval, Intelligent Database Systems, Knowledge Engineering, Mechatronics, Multi-agent Systems, Natural Language Processing, Neural Network Theory and Architectures, Neuro-informatics and Bio-inspired Models, Pattern Recognition, Robotics and Related Fields, Rough Sets Theory: Foundations and Applications, Supervised and Unsupervised Learning, Swarm Intelligence and Systems, Web Intelligence Applications & Search, Various Applications.
ISSN	24496499, 20832567
www	http://jaiscr.online/

Nr 588/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Journal of Intelligent and Robotic Systems: Theory and Applications

Description	The Journal of Intelligent and Robotic Systems (JINT) publishes original, peer-reviewed, invited, survey and review papers. JINT lays the foundation for a common framework for publication of ideas, derivation and testing of techniques that combine theory, science, engineering, and mathematics, leading to future innovations and novel technologies.
Goal / Target audience	The journal aims at bridging the gap between theory and practice, and intends to stimulate interaction between faculty, researchers, engineers and practitioners from academia, industry and government focusing on theoretical and applied research in all areas of intelligent systems and robotics.
Publisher	Springer Netherlands
Topics/ Content	The journal promote and disseminate scientific knowledge and information in the fields of system of systems, generalized system theory, distributed intelligent systems, bioengineering, robotics and automation, human-robot interaction, human-machine interfaces and interaction, robot ethics, social and service robotics, medical robotics, mechatronics, unmanned systems, multi-robot teams and networked swarms, machine intelligence, learning, system autonomy and autonomous systems, design for autonomy, cyber physical systems, and other related areas in which cutting edge technologies have been developed and applied to model, design, build and test complex engineering and autonomous systems.
ISSN	15730409, 09210296
www	https://www.springer.com/journal/10846

Nr 589/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Progress in Artificial Intelligence

Description	This journal publishes top-level research results in all aspects of artificial intelligence.
Goal / Target audience	This journal provides an international forum for publication original research and other information in all aspects of artificial intelligence.
Publisher	Springer Nature
Topics/ Content	• Data mining • Soft computing and computational intelligence • Knowledge • Complexity • Logic • Planning • Reasoning and search • Agents and multiagent systems • Artificial vision and robotics • Natural language and Web intelligence
ISSN	21926360, 21926352
www	https://www.springer.com/journal/13748

Nr 590/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Drones

Description	Drones is an international, peer-reviewed, open access journal published monthly online.
Goal / Target audience	The journal focuses on design and applications of drones, including unmanned aerial vehicle (UAV), Unmanned Aircraft Systems (UAS), and Remotely Piloted Aircraft Systems (RPAS), etc. Likewise, contributions based on unmanned water/underwater drones and unmanned ground vehicles are also welcomed.
Publisher	MDPI AG
Topics/ Content	• Design: onboard sensor design, airframe and structural design, power supply, geometric and radiometric sensors, sensor fusion, calibration of imageries, controlling system, signal/image processing, nano drones or nanotechnology • Development: performance, control system, mission planning, security systems, autonomy, navigation and position/orientation, autonomous take-off and landing, artificial intelligent, machine learning, simultaneous localization and mapping, controlled and non-controlled airspace, meteorology, GNSS outages, regulations, and economic impact • Applications: environments, agriculture, forestry, geosciences, urban area, logistics, disaster assistance, security and surveillance, architecture, monitoring, change detection, health, marine science, education
ISSN	2504446X
www	https://www.mdpi.com/journal/drones

Nr 591/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

International Journal of Fuzzy Systems

Description	The International Journal of Fuzzy Systems (IJFS) is an official journal of Taiwan Fuzzy Systems Association (TFSA) and is published semi-quarterly.
Goal / Target audience	IJFS will consider high quality papers that deal with the theory, design, and application of fuzzy systems, soft computing systems, grey systems, and extension theory systems ranging from hardware to software. Survey and expository submissions are also welcome.
Publisher	Springer International Publishing AG
Topics/ Content	Topics consist fuzzy systems, soft computing systems, grey systems, and extension theory systems ranging from hardware to software.
ISSN	15622479, 21993211
www	https://www.springer.com/journal/40815

Nr 592/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

IET Cyber-Physical Systems: Theory and Applications

Description	The research of IET Cyber-Physical Systems: Theory and Applications addresses the close interactions and feedback loop between cyber components such as sensing systems and dynamic physical components such as energy and mechanical systems.
Goal / Target audience	This journal aims to present the state-of-the-art interdisciplinary research addressing the above challenges from a system perspective that includes both cyber and physical aspects, with clear innovative contributions to theory and application.
Publisher	John Wiley & Sons Inc.
Topics/ Content	• Design, synthesis and verification of CPS • Big data modeling and analytics for CPS • Cross-layer modeling and optimization for CPS • Design automation for CPS • Embedded system design for CPS • CPS fault detection and recovery • CPS security and privacy • Sustainability and environmental issues in CPS • Social CPS computing • Industrial CPS and smart manufacturing • Applications of CPS in various domains such as smart energy systems, automotive and transportation systems, smart healthcare, surveillance systems and robotics
ISSN	23983396
www	https://ietresearch.onlinelibrary.wiley.com/journal/23983396

Nr 593/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

IEEE Transactions on Pattern Analysis and Machine Intelligence

Description	The IEEE Transactions on Pattern Analysis and Machine Intelligence publishes articles on all traditional areas of computer vision and image understanding, all traditional areas of pattern analysis and recognition, and selected areas of machine intelligence, with a particular emphasis on machine learning for pattern analysis. Areas such as techniques for visual search, document and handwriting analysis, medical image analysis, video and image sequence analysis, content-based retrieval of image and video, face and gesture recognition and relevant specialized hardware and/or software architectures are also covered.
Goal / Target audience	This publication considers original works that enhance the existing body of knowledge.
Publisher	IEEE Computer Society
Topics/ Content	• Bioengineering • Computing and Processing
ISSN	01628828
www	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=34

Nr 594/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Signal Processing

Description	Signal Processing incorporates all aspects of the theory and practice of signal processing. It features original research work covering novel signal processing tools as well as tutorial and review articles with a focus on the signal processing issues.
Goal / Target audience	It is intended for a rapid dissemination of knowledge to engineers and scientists working in the research, development or practical application of signal processing.
Publisher	Elsevier
Topics/ Content	Subject areas covered by the journal include: Signal Theory; Stochastic Processes; Detection and Estimation; Spectral Analysis; Filtering; Signal Processing Systems; Software Developments; Image Processing; Pattern Recognition; Optical Signal Processing; Digital Signal Processing; Multi-dimensional Signal Processing; Communication Signal Processing; Biomedical Signal Processing; Geophysical and Astrophysical Signal Processing; Earth Resources Signal Processing; Acoustic and Vibration Signal Processing; Data Processing; Remote Sensing; Signal Processing Technology; Radar Signal Processing; Sonar Signal Processing; Industrial Applications; New Applications.
ISSN	01651684
www	https://www.sciencedirect.com/journal/signal-processing

Nr 595/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Image and Vision Computing

Description	The journal publishes work that proposes new image interpretation and computer vision methodology or addresses the application of such methods to real world scenes.
Goal / Target audience	It seeks to strengthen a deeper understanding in the discipline by encouraging the quantitative comparison and performance evaluation of the proposed methodology.
Publisher	Elsevier Ltd.
Topics/ Content	The coverage includes: image interpretation, scene modelling, object recognition and tracking, shape analysis, monitoring and surveillance, active vision and robotic systems, SLAM, biologically-inspired computer vision, motion analysis, stereo vision, document image understanding, character and handwritten text recognition, face and gesture recognition, biometrics, vision-based human-computer interaction, human activity and behavior understanding, data fusion from multiple sensor inputs, image databases.
ISSN	02628856
www	https://www.sciencedirect.com/journal/image-and-vision-computing

Nr 596/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Signal Processing: Image Communication

Description	Signal Processing: Image Communication is an international journal for the development of the theory and practice of image communication.
Goal / Target audience	The primary objectives of the journal are the following: • To present a forum for the advancement of theory and practice of image communication. • To stimulate cross-fertilization between areas similar in nature which have traditionally been separated, for example, various aspects of visual communications and information systems. • To contribute to a rapid information exchange between the industrial and academic environments.
Publisher	Elsevier
Topics/ Content	Subjects of interest include image/video coding, 3D video representations and compression, 3D graphics and animation compression, HDTV and 3DTV systems, video adaptation, video over IP, peer-to-peer video networking, interactive visual communication, multi-user video conferencing, wireless video broadcasting and communication, visual surveillance, 2D and 3D image/video quality measures, pre/post processing, video restoration and super-resolution, multi-camera video analysis, motion analysis, content-based image/video indexing and retrieval, face and gesture processing, video synthesis, 2D and 3D image/video acquisition and display technologies, architectures for image/video processing and communication.
ISSN	09235965
www	https://www.sciencedirect.com/journal/signal-processing-image-communication

Nr 597/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Pattern Analysis and Applications

Description	The journal publishes high quality articles in areas of fundamental research in intelligent pattern analysis and applications in computer science and engineering.
Goal / Target audience	It aims to provide a forum for original research which describes novel pattern analysis techniques and industrial applications of the current technology.
Publisher	Springer London
Topics/ Content	The journal solicits articles that detail new technology and methods for pattern recognition and analysis in applied domains including, but not limited to, computer vision and image processing, speech analysis, robotics, multimedia, document analysis, character recognition, knowledge engineering for pattern recognition, fractal analysis, and intelligent control. The journal publishes articles on the use of advanced pattern recognition and analysis methods including statistical techniques, neural networks, genetic algorithms, fuzzy pattern recognition, machine learning, and hardware implementations which are either relevant to the development of pattern analysis as a research area or detail novel pattern analysis applications. Papers proposing new classifier systems or their development, pattern analysis systems for real-time applications, fuzzy and temporal pattern recognition and uncertainty management in applied pattern recognition are particularly solicited.
ISSN	1433755X, 14337541
www	https://www.springer.com/journal/10044

Nr 598/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Machine Vision and Applications

Description	Sponsored by the International Association for Pattern Recognition, this journal publishes high-quality, technical contributions in machine vision research and development. Machine Vision and Applications features coverage of all applications and engineering aspects of image-related computing, including original contributions dealing with scientific, commercial, industrial, military, and biomedical applications of machine vision.
Goal / Target audience	The journal places particular emphasis on the engineering and technology aspects of image processing and computer vision.
Publisher	Springer Verlag
Topics/ Content	It includes coverage of the following aspects of machine vision applications: algorithms, architectures, VLSI implementations, AI techniques and expert systems for machine vision, front-END sensing, multidimensional and multisensor machine vision, real-time techniques, image databases, virtual reality and visualization.
ISSN	14321769, 09328092
www	https://www.springer.com/journal/138

Nr 599/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Visual Computer

Description	The Visual Computer publishes articles on all research fields of capturing, recognizing, modelling, analysing and generating shapes and images.
Goal / Target audience	Original contributions, describing advances in the theory in the above mentioned fields as well as practical results and original applications, are invited.
Publisher	Springer Verlag
Topics/ Content	• Computer Animation and Simulation • Computational Geometry • Computational Photography • Computer Vision for Computer Graphics • Data Compression for Graphics • Geometric Modelling and Processing • HCI and Computer Graphics • Human Modelling • Image Based Rendering • Image Processing • Machine Learning for Graphics • Physically Based Modelling • Scientific Visualization • Shape Modelling • Shape Analysis • Sketch-based Modelling • Texturing • Virtual and Augmented Reality • Visual Analytics • Volume Rendering
ISSN	14322315, 01782789
www	https://www.springer.com/journal/371

Nr 600/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Computers and Graphics

Description	Computers & Graphics is dedicated to disseminate information on research and applications of computer graphics (CG) techniques. The journal encourages articles on: • Research and applications of interactive computer graphics. We are particularly interested in novel interaction techniques and applications of CG to problem domains. • State-of-the-art papers on late-breaking, cutting-edge research on CG. • Information on innovative uses of graphics principles and technologies. • Tutorial papers on both teaching CG principles and innovative uses of CG in education.
Goal / Target audience	Computers & Graphics provides a medium to communicate information concerning interactive CG and CG applications.
Publisher	Elsevier Ltd.
Topics/ Content	The journal focuses on interactive computer graphics, visualization and novel input modalities including virtual environments, and, within this scope, on graphical models, data structures, languages, picture manipulation algorithms and related software.
ISSN	00978493
www	https://www.sciencedirect.com/journal/computers-and-graphics

Nr 601/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Cyber-Physical Systems

Description	Cyber-Physical Systems is an international interdisciplinary journal dedicated to publishing the highest quality research in the rapidly-growing field of cyber-physical systems/ Internet-of-Things. Publications cover theory, algorithms, simulations, architectures, implementations, services and applications of state-of-the-art research in this field.
Goal / Target audience	Publications cover theory, algorithms, simulations, architectures, implementations, services and applications of state-of-the-art research in the field of cyber-physical systems/ Internet-of-Things.
Publisher	Taylor and Francis Ltd.
Topics/ Content	• sensor, vehicular, robot, camera, aerial and social smartphone networks • wireless networking technologies and autonomous ad hoc networks • internet of things and machine-to-machine communications • networked infrastructure management with applications such as smart power grids and transportation systems • network enabled computation, coordination, and actuation • scalability of complex networks • control theory with a clear cyber-physical tone such as networked control, distributed optimization, and distributed learning • autonomy with applications in mobile sensor networks, internet connected cars, etc. • modelling of tightly integrated physical processes, software, computation platforms, and networks • data management and processing (e.g. big data, cloud computing) • location and tracking based services • smart cameras and computer vision based context management • web of things • embedded systems applications (pervasive computing, real-time control technologies) • resource-constrained systems (low power, energizing, device miniaturization) • standards and middleware • incentive, security, trust, and privacy issues in CPS • smart living technologies such as smart city, smart home and office, wearable devices, learning devices, etc. • social M2M networks, social impact of CPS, creative aspects
ISSN	23335785
www	https://www.tandfonline.com/toc/tcyb20/current

Nr 602/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Computer Science

Description	The Computer Science Journal is a quarterly published by the AGH University of Science and Technology, Krakow Poland since 1999.
Goal / Target audience	The journal publishes original papers concerning theoretical and applied computer science problems. Main areas of interest of the journal are: theoretical aspects of computer science, soft computing, HPC, cloud and distributed processing and simulation, multimedia systems and computer graphics, natural language processing.
Publisher	AGH University of Science and Technology
Topics/ Content	• theoretical aspects of computer science, • pattern recognition and processing, • evolutionary algorithms, • neural networks, • database systems, • knowledge engineering, • automatic reasoning, • computer networks management, • distributed and grid systems, • multi-agent systems, • multimedia systems and computer graphics, • natural language processing, • soft-computing, • embedded systems, • adaptive algorithms, • simulation
ISSN	23007036, 15082806
www	https://journals.agh.edu.pl/csci

Nr 603/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Machine Graphics and Vision

Description	Machine GRAPHICS & VISION is a refereed international journal, published quarterly by the Institute of Information Technology of the Warsaw University of Life Sciences – SGGW, in cooperation with the Association for Image Processing, Poland – TPO.
Goal / Target audience	Machine GRAPHICS & VISION provides a scientific exchange forum and an authoritative source of information in the field of, in general, pictorial information exchange between computers and their environment, including applications of visual and graphical computer systems.
Publisher	Institute of Information Technology, Warsaw University of Life Sciences - SGGW
Topics/ Content	The journal concentrates on theoretical and computational models underlying computer generated, analysed, or otherwise processed imagery, in particular: • image processing, • scene analysis, modeling, and understanding, • machine vision, • pattern recognition, • image synthesis, including three-dimensional imaging and solid modeling, • computer-aided graphic arts and animation, • mathematical approaches to image processing, analysis, and synthesis, • computational geometry, • image models and transforms, • visualization and graphical data presentation, • diagrammatic knowledge representation and reasoning, • monocular and stereo vision, • modeling of human visual perception, • software and hardware image processing, • innovative uses of various graphic and vision devices and systems.
ISSN	2720250X, 12300535
www	https://mgv.sggw.edu.pl/

Nr 604/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	**Cybersecurity**

Title:

IEEE Transactions on Information Forensics and Security

Description	The IEEE Transactions on Information Forensics and Security covers the sciences, technologies, and applications relating to information forensics, information security, biometrics, surveillance and systems applications that incorporate these features.
Goal / Target audience	The journal considers original works that enhance the existing body of knowledge.
Publisher	Institute of Electrical and Electronics Engineers Inc.
Topics/ Content	• Communication, Networking and Broadcast Technologies • Computing and Processing • Signal Processing and Analysis
ISSN	1556-6021, 1556-6013
www	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206

Nr 605/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	**Cybersecurity**

Title:

IET Information Security

Description	IET Information Security is a Gold Open Access journal that publishes original research papers in the areas of information security and cryptography.
Goal / Target audience	The journal audience comprises academia, industry, and practitioners.
Publisher	Institution of Engineering and Technology, Hindawi
Topics/ Content	Access Control and Database Security, Ad-Hoc Network Aspects, Anonymity and E-Voting Authentication, Block Ciphers and Hash Functions, Blockchain, Bitcoin (technical aspects only), Broadcast Encryption and Traitor Tracing, Combinatorial Aspects, Covert Channels and Information Flow, Critical Infrastructures, Cryptanalysis, Dependability, Digital Banking Digital Currencies, Digital Rights Management, Digital Signature Schemes, Digital Steganography, DNS Security, Economic Aspects of Information Security, Elliptic Curve Cryptography and Number Theory, Embedded Systems Aspects, Embedded Systems Security and Forensics, Financial Cryptography, Firewall Security, Formal Methods and Security Verification, Hardware Security, Human Aspects, Information Warfare and Survivability, Intrusion Detection, Java and XML Security, Key Distribution, Key Management, Malware, Multi-Party Computation and Threshold Cryptography, Network Security, Peer-to-peer Security, PKIs, Public-Key and Hybrid Encryption, Quantum Cryptography, Risks of using Computers, Robust Networks, Secret Sharing, Secure Electronic Commerce, Software Obfuscation, Stream Ciphers, Trust Models, Watermarking and Fingerprinting
ISSN	1751-8717, 1751-8709
www	https://ietresearch.onlinelibrary.wiley.com/journal/17518717 https://www.hindawi.com/journals/ietis/

Nr 606/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

2nd Global Meet on Aerospace and Aeronautical Engineering (GMAERO2024)

Description	GMAERO2024 is an annual meeting organized with the intend of being a platform for Aerospace and Aeronautical Engineering experts, Researchers, academicians as well as industrial experts from all over the world to present their research results and development activities in Aerospace and Aeronautical Engineering.
Goal	The meeting brings together World Class participants and young researchers looking for opportunities for exchanges that cross the traditional discipline boundaries and allows them to resolve multidisciplinary challenging problems that only a venue of this nature can offer.
Organizer	Prime Meetings
Co-organizers/ Patrons	-
Topics	• Aerodynamics and Aviation Management • Aerospace and Aeronautical Science & Engineering • Aerospace Design, Testing and Performance • Aerospace Systems and Technology • Air Navigation and Air Traffic Management Systems • Air Transportation and Management Engineering • Aircraft Control and Information Engineering • Blast and Ballistic Loading • Crew Training Systems • Emerging Avionics Technology • Guidance, Navigation and Control • Robotics and Rotorcraft • Rocket Theory and Design • Safety and Security • Satellite Communications • Spacecraft and Space Propulsion • and more
Date	August 05-07, 2024
Costs	$299 – $899
www	https://primemeetings.org/2024/aerospace-aeronautical-engineering?utm_source=BenchmarkEmail&utm_campaign=GMAERO2024_10-13&utm_medium=email

No 607/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

2nd International Summit on Aerospace and Mechanical Engineering (ISAME2024)

Description	During the 2nd International Summit on Aerospace and Mechanical Engineering (ISAME2024) leaders in Aerospace and Mechanical engineering will share the latest developments and emerging challenges in these fields. As part of the three-day conference, participants will have a variety of networking opportunities and opportunities to participate in plenary talks, keynotes, interactive sessions, academic discussions, oral and poster presentations, technical workshops, and social events.
Goal	The conference, organized by SPECTRUM conferences, will provide a forum for researchers working on all aspects of additive manufacturing. A wonderful opportunity will be presented at the conference to introduce new participants to this field as well as to spotlight innovative tools and approaches.
Organizer	SPECTRUM conferences
Co-organizers/ Patrons	-
Topics	• Aerospace Engineering and Technology • Aircraft Control and Information Engineering • Transportation and Management Engineering • Embedded Systems in Aerospace and Defense • Aircraft Survivability Equipment • Artificial Intelligence for Aerospace • Unmanned Aerial Vehicle (UAV) • Robotics and Intelligent Systems • Aerospace Communications • Unmanned Air Vehicles • Avionics and Mission Technologies • Crew Training System • Transmission and Landing Systems • Signal and Image Processing • Flight Mechanics and Control • Emerging Avionics Technology • and more
Date	July 22-24, 2024
Costs	$299 – $899
www	https://www.spectrumconferences.com/2024/isame

No 608/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

9th International Congress on Information and Communication Technology

Description	9th International Congress on Information and Communication Technology in concurrent with ICT Excellence Awards (ICICT 2024) will be held at London, United Kingdom | 19 - 22 February 2024. ICICT 2024 will target state-of-the-art as well as emerging topics pertaining to ICT and its Supported e-Agriculture and Rural Development Technologies, e-Education and Computing Technologies, e-Mining and Inclusive Technologies for implementation for Engineering and Managerial Applications through ICT.
Goal	The objective of this International conference is to provide opportunities for the Researchers, Academicians, Industry persons and students to interact and exchange ideas, experience and expertise in the current trend and strategies for Information and Communication Technologies. Besides this, participants will also be enlightened about vast avenues, current and emerging technological developments in the field of ICT in this era and its applications will be thoroughly explored and discussed.
Organizer	Global Knowledge Research Foundation & G R Scholastic LLP
Co-organizers/ Patrons	-
Topics	• Communications • Infrastructure and Computation • Engineering Applications • E-Governance and Government • Technology Computation • Intelligent Systems • Electronic Systems & Circuits • Signal and Image Processing • Health Informatics
Date	19 - 22 February 2024
Costs	GBP £350 – GBP £1400
www	https://icict.co.uk/

No 609/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course Postgraduate studies	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	Cybersecurity

Title:

Air and Missile Defence Technology

Description	The Air and Missile Defence Technology Conference will provide a unique insight into GBAD, SHORAD, Counter-UAS, and international cooperation on air and missile defence.
Goal	The two-day conference will provide attendees the opportunity to engage with senior officials and technical experts to enhance their network and understanding of the Air and Missile defence prioritie.
Organizer	SAE Media Group
Co-organizers/ Patrons	-
Topics	Conference topics include Ground Based Air Defence (GRAD), Short-Range Air Defence (SHORAD), Unmanned Aircraft Systems (UAS), as well as international cooperation on air and missile defence.
Date	November 15-16, 2023
Costs	£899 – £1999
www	https://www.smgconferences.com/defence/uk/conference/Air-Missile-Defence?o=db&dl=br&p1=5970

No 610/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

e-Prime – Advances in Electrical Engineering, Electronics and Energy

Description	Elsevier's e-Prime – Advances in Electrical Engineering, Electronics and Energy is a new open-access, rapid turn-around, journal which publishes multidisciplinary papers from all areas of applied electronics, electrical engineering and energy. Focus is on high-quality research that is relevant and accessible to a global audience of scientists, practitioners, policy-makers and NGO's.
Goal / Target audience	Elsevier's e-Prime publishes research papers covering all aspects of electronics, electrical engineering and energy, ranging from systems engineering to power generation, semiconductors to infrastructure as well as other specializations that overlap e.g. hardware engineering, power electronics, nanotechnology, solar power and signal processing. Papers covering applications of AI, IOT, sensors, and the implementation of other technologies to the field are welcome.
Publisher	Elsevier
Topics/ Content	The wide spectrum of subjects includes all areas of electronics, electrical engineering, and energy, including: • Energy conversion, sustainable energy, power and energy systems • Electrical power applications, power systems and delivery • Signal Processing, lightwave technology, image processing • Wireless communication and smart grid • Systems mechatronics, software engineering, relatability, pattern analysis • Computer networks, and integrated systems • Semiconductors, nano-technologies, optoelectronics, photovoltaics and other electronic components • Power electronics and their applications • Control systems technology, Control engineering • Consumer, industrial, automotive, aerospace, and medical electronics • Circuits and systems • All energy applications ranging including solar, wind, water and nuclear • Quality, reliability and safety analysis • Applications of AI to electronics and energy development and implementation
ISSN	2772-6711
www	https://www.sciencedirect.com/journal/e-prime-advances-in-electrical-engineering-electronics-and-energy

Nr 611/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	**Cybersecurity**

Title:

Forensic Science International: Digital Investigation

Description	Forensic Science International: Digital Investigation covers a broad array of subjects related to crime and security throughout the computerized world. The primary pillar of this publication is digital evidence and multimedia, with the core qualities of provenance, integrity and authenticity. This publication promotes advances in investigating cybercrimes, cyberattacks and traditional crimes involving digital evidence, using scientific practices in digital investigations, and reducing the use of technology for criminal purposes.
Goal / Target audience	This widely referenced publication promotes innovations and advances in utilizing digital evidence and multimedia for legal purposes, including criminal justice, incident response, cybercrime analysis, cyber-risk management, civil and regulatory matters, and privacy protection. Relevant research areas include forensic science, computer science, data science, artificial intelligence, and smart technology. The journal is used by investigative agencies and forensic laboratories, computer security teams, practitioners, researchers, developers, and lawyers from industry, law enforcement, government, academia, and the military to share their knowledge and experiences.
Publisher	Elsevier Ltd.
Topics/ Content	Topics include, but are not limited to: • Research and development: Novel research and development in forensic science, computer science, data science, and artificial intelligence applied to digital evidence and multimedia. New methods to deal with challenges in digital investigations, including , exploiting specific technologies, and into preparing for and responding to computer security incidents. • Cyber-criminal investigation: develop new methods of online investigation and analysis of financially motivated cyber-crime such as banking Trojans, phishing, ransomware and other forms of cyber-fraud. In addition, researching future criminal activity involving peer-to-peer payments and crypto currencies. • Hardware Forensics: develop new methods of extracting and analyzing evidence from electronic hardware. • Cyber-risk management: Improved ways of using digital evidence to address security breaches involving information systems, methods to find zero day attacks and to perform cyber threat intelligence. The techniques and findings of digital investigations are essential in drawing post-incident conclusions, which are vital feedback components of the security policy development process, and managing risk appetite.
ISSN	2666-2825, 2666-2817
www	https://www.sciencedirect.com/journal/forensic-science-international-digital-investigation

Nr 612/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	**Cybersecurity**

Title:

Journal of Information and Intelligence

Description	Journal of Information and Intelligence is committed to publishing rigorously peer-reviewed, high-quality, original results and authoritative reviews of both fundamental and applied research in the area of information and intelligence.
Goal / Target audience	The journal aims at providing a unique interdisciplinary platform to promote disciplinary developments and academic exchange. It faces global researchers in related fields, from academia, industries and governments.
Publisher	Elsevier
Topics/ Content	Special areas of interest include but are not limited to: • AI-driven communication and networking • Computer networks and distributed computing • Computer vision, image processing, and pattern recognition • Information and intelligence-related chip design • Intelligent air and space exploration • Intelligent information sensing and signal processing • Internet of Things • Big data • Block chain • Machine learning theory and technology • Security, privacy, and trust for communication, network, data, etc.
ISSN	2949-7159
www	https://www.sciencedirect.com/journal/journal-of-information-and-intelligence

Nr 613/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Machine Learning with Applications

Description	Machine Learning with Applications (MLWA) is a peer reviewed, open access journal focused on research related to machine learning. The journal encompasses all aspects of research and development in ML, including but not limited to data mining, computer vision, natural language processing (NLP), intelligent systems, neural networks, AI-based software engineering, bioinformatics and their applications in the areas of engineering, medicine, biology, education, business and social sciences. It covers a broad spectrum of applications in the community, from industry, government, and academia.
Goal / Target audience	The journal audience comprises academia, industry, and practitioners.
Publisher	Elsevier
Topics/ Content	• Management Science and Operations Research • Artificial Intelligence • Computer Science Applications
ISSN	2666-8270
www	https://www.sciencedirect.com/journal/machine-learning-with-applications

Nr 614/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Natural Language Processing Journal

Description	The Natural Language Processing Journal aims to advance modern understanding and practice of trustworthy, interpretable, explainable human-centered and hybrid Artificial Intelligence as it relates to all aspects of human language.
Goal / Target audience	The NLP journal affords a world-wide platform for academics and practitioners to present their latest theoretical, practical, and methodological research concerning the development and application of trustworthy AI to analyze, process, or model human language across various multimodal contexts, domains, and intelligent systems, including hybrid AI, Human AI interaction and Social systems. The NLP journal welcomes original research papers, review papers, position papers, tutorial and best practice papers.
Publisher	Elsevier
Topics/ Content	Artificial Intelligence
ISSN	2949-7191
www	https://www.sciencedirect.com/journal/natural-language-processing-journal

Nr 615/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	**Journal**	Cybersecurity

Title:

Visual Informatics

Description	Visual Informatics is a peer-reviewed online journal published on the platform of Elsevier. It is dedicated to the development and application of theories, algorithms and technologies associated with visual data acquisition, analysis, synthesis, perception, enhancement and applications.
Goal / Target audience	The journal accepts surveys, original research articles, invited papers, special issues and excellent papers recommended by some related conferences.
Publisher	Elsevier
Topics/ Content	Suggested topics include but are not limited to: • Visual data acquisition and modelling • Visualization and visual analysis • Expressive rendering • Augmented reality • Natural interface based on visual perception
ISSN	2543-2656, 2468-502X
www	https://www.sciencedirect.com/journal/visual-informatics

Nr 616/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR : command, control, communications, computers, information/intelligence, surveillance
	Policy	**Journal**	Cybersecurity

Title:

Advances in Military Technology

Description	The international journal of Advances in Military Technology is a peer reviewed journal that provides insight into theoretical considerations and practical innovations in military and security technology.
Goal / Target audience	The journal covers a broad spectrum of interests including research, development, design, manufacturing, control, utilization, reliability, sustainability, and the effectiveness of new technologies for military and security requirements. AiMT builds a bridge between theoretical perspectives and practical considerations that are of active interest to the academic, scientific, business and policy communities.
Publisher	University of Defence
Topics/ Content	• Investigation of new materials and technologies to be used in military, defence and security equipment; • Research, development, reliability, effectiveness, control and exploitation of modern weapon systems; protective, security and service systems, means and tools; • Building-up the control and command systems of land and air forces; • Research and implementation of the advanced information, communication, simulation and control technologies in the military; • Other topics contributing to the development of military, defence and security theory and practice.
ISSN	1802-2308
www	https://www.aimt.cz/index.php/aimt

Nr 617/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	**C4ISTAR : command, control, communications, computers, information/intelligence, surveillance**
	Policy	**Journal**	Cybersecurity

Title:

ISPRS Open Journal of Photogrammetry and Remote Sensing

Description	The ISPRS Open Journal of Photogrammetry and Remote Sensing (IOJPRS) is an official journal of the International Society for Photogrammetry and Remote Sensing (ISPRS). The Journal provides a channel of communication for scientists and professionals in all countries working in the many disciplines that employ photogrammetry, remote sensing, spatial information systems, computer vision, and related fields. The Journal is designed to serve as a source reference and archive of advancements in these disciplines.
Goal / Target audience	The IOJPRS objective is to publish high quality, peer-reviewed, preferably previously unpublished papers of a scientific/research, technological development or application/practical nature.
Publisher	Elsevier
Topics/ Content	• Sensors (Airborne and spaceborne multispectral and hyperspectral imaging systems, Airborne and terrestrial cameras, Airborne, terrestrial and mobile laser scanning, Range imaging, Active and passive imaging sensor characterisation, Sensor calibration and standardisation, Geosensor networks, Internet of Things) • Methods and procedures (Spatial data handling technologies, Integrated sensor calibration and orientation, Surface and object reconstruction, modelling and interpretation, GIS data modelling, representation and structures, Database systems, Mapping from imagery, Visualisation, animation and virtual reality, Physical measurements and spectral signatures, Point cloud processing, Extraction of geometric and semantic information from SAR, SAR Interferometry, Image classification algorithms, Image segmentation and GEOBIA, Image time series analysis, Hyperspectral data analysis, Big image data analysis, Crowd sourcing, Feature extraction) • Applications and products (3D urban GIS, Close-range imaging and metrology, Architectural & archaeological photogrammetry, Determination of forest metrics, Medical image analysis and biometry, Resource and environmental modelling, Global monitoring and assessment, Thematic applications, DTM and orthoimage generation, Location based services)
ISSN	2667-3932
www	https://www.sciencedirect.com/journal/isprs-open-journal-of-photogrammetry-and-remote-sensing

Nr 618/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

MSc Cybersecurity

Description	This programme is designed to prepare IT professionals for a managerial or technical career in cybersecurity. It will be of value to people working in project/product/systems management, or as software developers or software engineers, as well as those in incident response, tech support or networking, who are looking to move into cybersecurity. It will help companies, government and state institutions, defence forces and others to upskill their staff to fill new roles in cyber security so that they can protect their organisations, their customers and the public.
Organizer	University College Dublin
Cooperation with	-
Duration	2 years
Thematic Scope	• Information Security • Risk Assessment & Security Standards • Leadership In Security • Cybersecurity Law and Regulation • Secure Software Engineering • Applied Cryptography • Network Security • Incident Response • Malware Analysis • Trends in Cybersecurity • Ethical Hacking
Costs	€ 7,030 per year (total €14,060)
No of ECTS credits	90 ECTS
E-learning	Lectures will be delivered online and will be complemented by face-to-face.
Tools	-
Job opportunities	The course will prepare professionals for a rewarding career in cybersecurity; for example, to take role of a security manager, security engineer, security analyst, or IT security specialist.
Additional info	-
www	https://hub.ucd.ie/usis/!W_HU_MENU.P_PUBLISH?p_tag=PROG&MAJR=T380

Nr 619/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

MSc in Applied Cyber Security

Description	The Master of Science in Computing in Applied Cyber Security is designed to produce highly knowledgeable and skilled graduates to counter the cyber security threat. This course focuses on developing hands-on skills backed by theoretical knowledge. An essential part of the master's degree is the creation of a body of work presented as a thesis which demonstrates ability in research methods, analytics and report writing.
Organizer	Technological University Dublin
Cooperation with	-
Duration	1 year
Thematic Scope	• Digital Forensics • Secure Communication and Cryptography • Network Security • Research Skills and Ethics • Biometrics • Secure Programming • Application Security • Business Continuity and Cloud Security • Cyber Crime Malware • Security Intelligence
Costs	€8,500 total fee
No of ECTS credits	90 ECTS
E-learning	on-campus, online
Tools	-
Job opportunities	The Master of Science in Computing in Applied Cyber Security will give the skills and knowledge to secure business and personal data and allow graduates to work as security professionals in any of the business and industry sectors.
Additional info	-
www	https://www.tudublin.ie/study/postgraduate/courses/applied-cyber-security/

Nr 620/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Forensic Computing and Cybercrime Investigation

Description	This is a programme for law enforcement. It aims to provide high quality forensic computing and cybercrime investigation training and formal education. It is also designed to deliver cutting-edge, up-to-date cybercrime investigation techniques, strategies and tactics that allow students to understand and tackle emerging trends in cybercrime.
Organizer	University College Dublin
Cooperation with	-
Duration	1 year / 2 years
Thematic Scope	Computer Forensics, Network Investigations, Programming for Investigators, Case Studies, Research Project in Forensic Computing and Cyber Crime Investigation, Linux for Investigators, VoIP and Wireless Investigations, Malware Investigations, Live Data Forensics, Data & Database Forensics, Advanced Malware Analysis, Mobile Devices Investigation, Financial Investigation Techniques - Following the Money, OSINT Collection & Analysis, Online Child Abuse Investigations
Costs	Part time: EU/nonEU - fee per year: € 5544 Full time: EU - fee per year: € 11088 nonEU - fee per year: € 10994
No of ECTS credits	90 ECTS
E-learning	Lectures are pre-recorded and provided online via a virtual online learning environment. Exercises, reading, assignments and projects are conducted online and in our virtual labs. Students are required to come to Dublin or another UCD exam centre each year to complete in-person examinations.
Tools	-
Job opportunities	Graduates include senior staff at Europol and INTERPOL, members of national and regional police forces and police training colleges, government ministries and agencies with Law Enforcement (LE) powers, defence forces, specialist cybercrime agencies, revenue, customs and border protection.
Additional info	-
www	https://hub.ucd.ie/usis/!W_HU_MENU.P_PUBLISH?p_tag=PROG&MAJR=T146

Nr 621/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Master in Cybersecurity

Description	The overall goal for the master's programme is to give the students the knowledge and understanding of security that is necessary to ensure both trust and credibility to ICT-systems. Knowledge of ICT, cryptography and its uses, and understanding of systems are amongst the topics of the programme.
Organizer	University of Agder (Kristiansand, Norway)
Cooperation with	-
Duration	2 years
Thematic Scope	• Security Technologies (Trust, Threats, Risk and Vulnerability, Communication, Cooperation and Research Methods, Enterprise Systems and Security Architecture, Blockchain and distributed ledger technology, Security in IoT and Machine-Type Communication, Cryptography, WiFi and Internet of Things, 5G and IoT: Advanced) • Security Management (Ethical and Legal Aspects of Information Security, Enterprise Systems and Security Architecture, Communication and Teamwork in Cyber Security, Trust, Threats, Risk and Vulnerability, Strategic Information Security Management, Selected Security Topics, Blockchain and distributed ledger technology, Security in IoT and Machine-Type Communication, Research Methods in Information Systems, Current Topics and Research Areas in Information System Security, Security Management in IS Development Projects)
Costs	ND
No of ECTS credits	120 ECTS
E-learning	ND
Tools	-
Job opportunities	• Security technologies - this specialization educates people to work in preparation, integration, and development of technical solutions for security. • Security management - this specialization profile is centred around management and organizational, and user-centred aspects; this competence is essential when it comes to planning management, implementation, and deployment of systems where solid security is critical.
Additional info	-
www	https://www.uia.no/en/studieplaner/programme/M-SEC

Nr 622/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Cybersecurity

Description	Cybersecurity is a broad and multi-faceted subject. It ranges from fundamental computing theory to software engineering, computer communication, large-scale distributed systems, and physical process control into human and social behaviour. The programme is rooted in computer science and reaches out to aspects of the business and social context of cybersecurity. The master's programme in Cybersecurity gives you access to all courses offered by the faculty in cybersecurity at KTH.
Organizer	KTH Royal Institute of Technology (Stockholm, Sweden)
Cooperation with	-
Duration	2 years
Thematic Scope	software security, communication network security, ethical hacking, privacy, cryptography, cyber risk analysis, cyber-physical security and hardware security
Costs	Free
No of ECTS credits	120 ECTS
E-learning	The programme is campus-based, but much of the teaching is conducted digitally.
Tools	-
Job opportunities	Chief Information Security Officer, Cybersecurity Architect, Cybersecurity Analyst and Cybersecurity Specialist
Additional info	-
www	https://www.kth.se/en/studies/master/cybersecurity/msc-cybersecurity-1.1076022

Nr 623/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Cyber Security and Network Administration

Description	Cyber Security and Network Administration gives you the tools to implement, secure, and monitor digital systems and networks so that companies and organisations can keep their operations running in a secure manner. The programme combines network administration and server administration in both Windows and Linux environments with a clear focus on security.
Organizer	University of Skövde (Skövde, Sweden)
Cooperation with	-
Duration	3 years
Thematic Scope	data communication, network security, and operating systems, IT forensics, cyber security, risk management and wireless networks
Costs	Free
No of ECTS credits	180 ECTS
E-learning	No
Tools	-
Job opportunities	Cyber Security Analyst/Cyber Security Analyst, IT Security Specialist, IT Security Analyst, Network Security Expert, Network Technicians, Network Specialist, Information Security Specialist, Cyber Security Specialist, Red/Blue Team Member, Cyber Intelligence Specialist, Cyber Operations Specialist, Digital Forensics Analyst, IT Security Architect, Network, Security Administrator, Network Technician, Cyber Security Engineer
Additional info	-
www	https://www.his.se/en/education/informatics/cyber-security-and-network-administration-cnapg/

Nr 624/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Master's Programme in Network Forensics

Description	The Master's programme in Network Forensics has a multidisciplinary connection to technology and social sciences. During the programme, students build theoretical and practical skills for work in IT forensic network analysis. They also develop in-depth knowledge of data mining, cybersecurity and investigation into cybercrime.
Organizer	Halmstad University (Halmstad, Sweden)
Cooperation with	-
Duration	1 year
Thematic Scope	• Advanced Computer Networks and Security • Introduction to Digital Forensics • Applied Data Mining • Network Forensics and Cybercrime • Degree Project in Digital Forensics
Costs	Free
No of ECTS credits	60 ECTS
E-learning	No
Tools	-
Job opportunities	The Master's programme in Network Forensics prepares to work independently on criminal forensic investigations of computers or as a computer administrator specialising in computer networks and IT security.
Additional info	-
www	https://www.hh.se/english/education/programmes/masters-programme-60-credits-in-network-forensics.html?event=TANFO21h1

Nr 625/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Master's Programme in Embedded and Intelligent Systems

Description	In the Master's programme in Embedded and Intelligent Systems, students build up theoretical and practical skills for research, design and development of embedded intelligent systems. They can also obtain in-depth knowledge of robotics, embedded AI, autonomous vehicles, real-time computer systems, learning systems, computer vision and signal analysis, sensor systems, parallel computing, testing, data mining, and deep learning.
Organizer	Halmstad University (Halmstad, Sweden)
Cooperation with	-
Duration	2 years
Thematic Scope	Networks for Embedded Systems, Artificial Intelligence, Engineering Mathematics, Python - a Gateway to Machine Learning, Real-time Embedded System, Learning Systems, Intelligent Vehicles, Image Analysis, Robotics, Embedded Parallel Computing, Design of Embedded and Intelligent Systems, Real-Time Embedded Systems, Testing and Verification of Embedded Systems, Data Mining, Deep Learning, Computer Vision in 3D, Dependable and Real-time Data Communication
Costs	Free
No of ECTS credits	120 ECTS
E-learning	No
Tools	-
Job opportunities	The Master's programme in Embedded Intelligent Systems prepares students for advanced development work in industry. This may involve developing advanced computer technology applications in areas such as robotics and transport, data science and artificial intelligence, telecommunications, testing and embedded software development or health technology.
Additional info	-
www	https://www.hh.se/english/education/programmes/masters-programme-120-credits-in-embedded-and-intelligent-systems.html

Nr 626/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Master's Programme in Information Technology

Description	In the Master's programme in Information Technology, students develop theoretical and practical skills for research, development and implementation of computer technology. They obtain in-depth knowledge of computer science for the subject areas data science, machine learning, artificial intelligence, edge computing and internet of things, image analysis, big data parallel programming, data mining, digital service innovation, and deep learning.
Organizer	Halmstad University (Halmstad, Sweden)
Cooperation with	-
Duration	2 years
Thematic Scope	Python - a Gateway to Machine Learning, Perspectives on Data Science, Artificial Intelligence, Engineering Mathematics, Learning Systems, Edge Computing and Internet of Things, Image Analysis, Big Data Parallel Programming, Data Mining, Digital Service Innovation, Deep Learning, Computer Vision in 3D, Artificial Intelligence for Health, Intelligent Vehicles
Costs	Free
No of ECTS credits	120 ECTS
E-learning	No
Tools	-
Job opportunities	The Master's programme in Information Technology prepares the students for an advanced development role within the industry.
Additional info	-
www	https://www.hh.se/english/education/programmes/masters-programme-120-credits-in-information-technology.html

Nr 627/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Privacy, Information and Cyber Security - Master's Programme

Description	The programme offers comprehensive studies in privacy, information security and cyber security, providing you with unique skills. During the courses of the programme, students will learn how a systematic approach to information security can be implemented in an organisation through various management systems. They will also learn about data protection, methods for discovering and stopping data packages containing damaging files and the management of security risks in common solutions for the Internet of Things.
Organizer	University of Skövde (Skövde, Sweden)
Cooperation with	-
Duration	2 years
Thematic Scope	Principles of Privacy, Information Security and Cyber Security, Practical cryptology, Privacy, Information Security Management, Network security operations, Cyber Security for Internet of Things and Critical Infrastructures, Project in Privacy, Information Security and Cyber Security, Information Security Management – Research, Digital forensics for incident response,
Costs	Free
No of ECTS credits	120 ECTS
E-learning	The programme is offered on campus and online, but all sessions are combining online and campus students. Lectures, seminars and other sessions will not be recorded.
Tools	-
Job opportunities	After completion of the study programme, the student should be able to demonstrate in-depth knowledge and understanding of the program's themes of privacy, information security and cyber security respectively, but also deepened knowledge and understanding of the relationships between these fields linked to the digitization of sustainable development.
Additional info	-
www	https://www.his.se/en/education/informatics/privacy-information-and-cyber-security-masters-programme-iicma/

Nr 628/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Master's Degree Programme in Information and Communication Technology: Cyber Security

Description	In the Cyber Security track, students will gain knowledge, expertise and hands-on experience in the fields of cyber security and network security technology. The track focuses on cyber security technologies developed for networked systems and applications of the communication-intensive future.
Organizer	University of Turku (Turku, Finland)
Cooperation with	-
Duration	2 years
Thematic Scope	The technological topics covered include, among others, system and network security, security of Internet-of-Things (IoT) systems and applications, ethical hacking (penetration testing) and designing secure systems.
Costs	Free
No of ECTS credits	120 ECTS
E-learning	No
Tools	-
Job opportunities	Cyber Security Analyst, Penetration and Vulnerability Tester, Cyber Security Consultant, Cyber Security Manager, Network Security Specialist, Information Security Specialist, Cyber Security Entrepreneur, System / Network Administrator, Cryptography Engineer, Network Engineer, Business Information Security Officer, Chief Information Officer, Chief Information Security Officer, Head of Information Security, Head of Corporate IT,
Additional info	-
www	https://www.utu.fi/en/study-at-utu/masters-degree-programme-in-information-and-communication-technology-cyber-security

Nr 629/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	**C4ISTAR: command, control, communications, computers, information/intelligence, surveillance**
	Policy	Journal	**Cybersecurity**

Title:

Cyber Security, Master of Engineering

Description	Cyber Security Master's Degree programme student knows how about management, technical implementations, auditing, legislation and regulations of cyber security. The student will know how to plan, develop, implement and control different technological solutions in realistic company environments. The student will also learn how to test and audit these solutions. Student will gain the knowledge and skills to defend cyber security attacks in a safe, education-oriented cyber environment.
Organizer	JAMK University of Applied Sciences (Jyväskylä, Finland)
Cooperation with	-
Duration	As a part-time student, students can complete the programme in approximately two years. It is also possible to complete the programme in one year as full-time studies.
Thematic Scope	Modern Management of IT, Cyber Security Implementation in Practice, Auditing and Testing Technical Security, Cyber Security Exercise, Research and Development, Management
Costs	Free
No of ECTS credits	60 ECTS
E-learning	Blended
Tools	-
Job opportunities	-
Additional info	-
www	https://www.jamk.fi/en/Apply-to-Jamk/masters-degree/educate-yourself-to-be-a-cyber-security-professional

Nr 630/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

MSc in Cybersecurity

Description	The programme provides students with core skills in wide aspects of the security of information systems and specialised skills in the chosen specialisation. Students get a unique chance to study under high-level Cybersecurity practitioners from Estonian universities, industry, law enforcement, CERT and the NATO Cooperative Cyber Defence Centre of Excellence.
Organizer	Tallinn University of Technology (Tallinn, Estonia) and University of Tartu (Tartu, Estonia)
Cooperation with	-
Duration	2 years
Thematic Scope	• Cybersecurity • Digital Forensics • Cryptography
Costs	€6000 per year, free for EU/EEA citizens
No of ECTS credits	120 ECTS
E-learning	No
Tools	-
Job opportunities	The programme conveys the specialist knowledge and professional skills needed on a career path leading to high-end technical roles (e.g. security analyst, architect or research engineer; security incident handler or a digital forensic expert in a law enforcement agency) or managerial roles (e.g. project/team leader or technology officer). The studies are also an excellent addition to a previous background in legal studies or law enforcement, leading to unique career opportunities. Great networking possibilities and collaboration with leading specialists in the field will present graduates with a range of career opportunities. The studies can also be continued at doctoral level. The direct follow-up curriculum at TalTech is Information and Communication Technology (IAQD) PhD programme.
Additional info	-
www	https://taltech.ee/en/masters-programmes/cybersecurity

No 631/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Cybersecurity Engineering

Description	The mission of the academic master's study programme "Cybersecurity Engineering" is to provide a set of theoretical knowledge and practical skills for students to achieve competencies corresponding to a Master's degree in cybersecurity engineering. In the academic Master's studies, the student acquires the necessary knowledge, skills and competence for comprehensive and effective action in the field of cybersecurity engineering in the chosen economic sector – design, implementation, improvement and management of IT security systems, understanding of professional ethics and socially responsible management, which forms the basis for further studies for a higher level of knowledge and skills acquisition.
Organizer	Riga Technical University (Riga, Latvia)
Cooperation with	-
Duration	2 years
Thematic Scope	Introduction to Cybersecurity, Reliability of Information Systems, Information Security and Personal Data Protection, Cybersecurity Solutions in High Performance Computing Environment, Control Fundamentals of Critical Infrastructures, Industrial Safety, Network Security, Software Security, Cryptography and Data Security Technologies, Design of Adaptive Systems, Engineering Systems Security, Sociotechnical Systems Modelling, Data Mining and Knowledge Discovery, Project Management, Secure E-Commerce Technologies, Data Integration Technologies
Costs	-
No of ECTS credits	120 ECTS
E-learning	-
Tools	-
Job opportunities	Graduates of the study programme are prepared for work in both the state and local government, as well as in the private sector – in commercial companies, small and medium enterprises. The study programme is suitable for students who want to become a cybersecurity analyst, cybersecurity engineer, cybersecurity architect, cybersecurity consultant. Graduates are also prepared for continuing work in industrial research and development as well as in scientific research and higher education.
Additional info	-
www	https://international.rtu.lv/masters-studies/cybersecurity-engineering/

No 632/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Cybersecurity Engineering

Description	The course aims to provide the necessary competencies for a cyber security specialist who is responsible for strengthening information systems as well as preventing cyber-attacks and security incidents, carrying out risk analysis and offering security measures to mitigate threats in their workplace or for an external client.
Organizer	Vidzeme University of Applied Sciences (Valmiera, Latvia)
Cooperation with	-
Duration	2 years
Thematic Scope	• Strengthening of information systems: Web application Penetration Testing; Reverse Engineering; Mobile and Cloud Computing Security; Digital Forensics; Intrusion Detection and Prevention; Security Incident Management; Information System Security Engineering; Applied Cryptography; Fundamentals of Computing for Security Professionals; IT security, administration and protection. • Entrepreneurship and Innovation: Project Management Methods and Tools; Innovation and Creative Problem Solving; Strategic IT Management; Cyber Security Requirements Engineering. • Collaboration in the digital age: Introduction to Propaganda and Persuasive Communication; Information Collection Techniques; Internet psychology. • Legal and ethical aspects: Obligations, Responsibilities and Rights in the Internet; Protection and investigation of personal data. • Cyber security management: Cyber security Policy; Information System Audit and Security; Information Security Risk Management; Security Culture.
Costs	EU, EEA, Swiss Confederation - 4200 EUR per academic year
No of ECTS credits	120 ECTS
E-learning	-
Tools	-
Job opportunities	Graduates can work in various public and private sector organisations as integrated security testers and cybersecurity specialists, who can collaborate effectively, think critically and make data-based decisions.
Additional info	-
www	https://va.lv/en/study-here/masters-degree/cybersecurity-engineering/about-programme

Nr 633/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Information Systems and Cyber Security

Description	The Information Systems and Cyber Security study programme is aimed at prepare professionals in information systems and cyber security, who will gain fundamental and applied knowledge in informatics engineering and develop the skills required for the secure analysis, design, structuring and maintenance of information systems.
Organizer	Vilnius University (Kaunas, Lithuania)
Cooperation with	-
Duration	3,5 years
Thematic Scope	A graduate is able to: analyse and formalise the information flows in a business enterprise, technologically justify the directions of the implementation of IT, design, implement, structure, maintain and professionally assess a secure IS, understand computer architecture, employ programming languages and technologies for providing information on the internet, design the IS architecture and databases, create IS with the use of both traditional and modern mobile technologies, know about security components, basic structures, assessment criteria and administration basics, effective firewall concepts, architecture and content scanning; detect cases of hacking and carry out prevention measures, identify the gaps in incorrect programming, access the files of cyberattacks DoS and DDoS, and know about Burp Suite, understand the security of WEB components, knows the security context of a particular OS, recognise cases of phishing and understand the subtleties of session management and replay attacks, perform manual and half-automatic systems and software testing by identifying security gaps and security vulnerabilities, know about the legal regulations in relation to cyber security.
Costs	Tuition fee per year: 4 900€
No of ECTS credits	210 ECTS
E-learning	
Tools	-
Job opportunities	Graduates of this study programme will be able to work as: experts, consultants and information systems security professionals in government organisations and business enterprises of various sizes.
Additional info	-
www	https://www.vu.lt/en/studies/bachelor-and-integrated-studies/information-systems-and-cyber-security

No 634/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Cybersecurity Management

Description	Cybersecurity Management is an interdisciplinary study program, with topics of cybersecurity risk management, cybersecurity modelling, personal data protection, security economics, intellectual property, cybersecurity regulation and so much more.
Organizer	Mykolas Romeris Universityn (Vilnius, Lithuania)
Cooperation with	-
Duration	2 years
Thematic Scope	Economic Basics, Management, Decisions of E-governance and E-Democracy, Fundamental Principles and Risk Management of Cybersecurity, Legal Environment of Cyber Security, Organisational Cyber Security Culture, Privacy and Data Protection, Security Economics, Modeling of Electronic Information Security, Management of IT Projects
Costs	€4294 per one academic year
No of ECTS credits	90 ECTS
E-learning	No
Tools	-
Job opportunities	After completing the degree, students will be able to apply your knowledge in State bodies and/or businesses which manage important electronic data, critical infrastructures and other electronic resources (departments of public institutions security and IT, business units, and units of the management of risks, the IT departments, etc.). They may also establish their own cyber security consultancy or cybersecurity related products business.
Additional info	-
www	https://www.mruni.eu/en/study_program/cybersecurity-management/

No 635/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Information and Information Technology Security

Description	This study programme is aimed at training highly qualified specialists in Information and Information Technology Security thus forming a systemic approach to the occurrence of information security problems and to their prevention, solution and compensation methods. The students are provided with the latest specific knowledge and gain the ability to apply modern information security assurance techniques and technologies by developing original and critical thinking, leadership, research and innovation skills.
Organizer	Vilnius Gedmininas Technical University (Vilnius, Lithuania)
Cooperation with	National Sun YAT-sen University
Duration	2 years
Thematic Scope	Information Technology Security Methods, Ethical, Legal and Human Aspects of Information Security, Cryptographic Systems, Fundamentals of Scientific Research and Innovations, Computer Networks and Operating System Security, Virtual Infrastructure and Cloud Computing Security, Malware Analysis Methods, Software Security, SOC Methods and Technologies for Information System Defense, Information Security Management
Costs	-
No of ECTS credits	120 ECTS
E-learning	No
Tools	-
Job opportunities	• Work as an Information Security Officer (CISO). • Work as an information security auditor. • Work as an inspection specialist in technical information security. • Work as a specialist in cybercrime investigation. • Work as an information system designer or a project manager having a specific knowledge of security. • Studying a Doctoral degree programme.
Additional info	-
www	https://vilniustech.lt/studies/study-programmes/master-study-programmes/317411?element_id=317413&sp_id=44_pr_2023&f_id=4&qualification=a%3A1%3A%7Bi%3A0%3Bs%3A1%3A%22M%22%3B%7D#About

No 636/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

University Master's Degree in Computer Security Engineering and Artificial Intelligence

Description	The Master's Degree in Computer Security Engineering and Artificial Intelligence prepares students to carry out responsible work in a wide range of areas, including industry, academia and public administration. The master's degree curriculum includes research topics related to information production, application security, machine learning, modelling and problem-solving, among others. When students finish the master's degree, they will be able to tackle problems of high technical difficulty or that require a high level of innovation and research.
Organizer	Universitat Rovira i Virgili (Tarragona, Spain)
Cooperation with	-
Duration	1 year
Thematic Scope	Cryptology and Information Security, Computer Forensics, Biometric Identification, Multi-agent Systems, Artificial Vision and Pattern Recognition, Neuronal and Evolutionary Computation, Privacy Protection, Multi-criteria Decision Support Systems
Costs	1806€ (for students from the UE, Iceland, Norway, Liechtenstein, Switzerland and Andorra*, or resident in Spain, price for 2023-24). Rest of students: €2,913.
No of ECTS credits	60 ECTS
E-learning	Face-to-face / Online
Tools	-
Job opportunities	The Master's produces professionals with the skills to work in the following positions, among others: • Head of Computer Security and Artificial Intelligence projects. • Management of groups of developers for Computer Security and Artificial Intelligence projects. • Analyst of advanced ICT applications, particularly in the ambits of Computer Security and Artificial Intelligence. • Academic and research career in universities and research centres.
Additional info	-
www	https://www.urv.cat/en/studies/master/courses/computer-security-engineering/

No 637/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

MASTER OF LIFELONG LEARNING IN CYBERSECURITY

Description	The Master's Degree in Cybersecurity at La Salle-URL (MCS) aims to help fulfil this business need and trains experts specialised in ICT security, incorporating the key skills in both defensive and offensive cybersecurity with a focus on such indispensable aspects as reverse engineering, cyberintelligence and forensic analysis, among others.
Organizer	La Salle Campus Barcelona - Ramon Llull University (Barcelona, Spain)
Cooperation with	-
Duration	1 year
Thematic Scope	Ethical Hacking, Security Analysis, Soc and Response to Incidents, Forensic Analysis, Reverse Engineering, Ciber Intelligence, Web Security, Cybersecurity Ecosystems
Costs	-
No of ECTS credits	60 ECTS
E-learning	No
Tools	-
Job opportunities	• Reverse engineering expert. • Cybersecurity consultant. • Information Security Analyst • Malware Analyst • Forensic analyst • Secure software engineer • Security engineer in mobile devices • Security Auditor • Security Manager
Additional info	-
www	https://www.salleurl.edu/en/education/master-cybersecurity

No 638/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

MSc Software Engineering and Internet Computing

Description	In Software Engineering and Internet Computing students will focus on software development for distributed systems, mobile computing, Internet security and electronic payment as essential technological prerequisites for a virtual Internet business location. The specialization in Security and Privacy offers the opportunity to deepen your knowledge in various topics, such as system security, network security, cryptography, formal methods for security and privacy, and many more, acquiring the background required to become an IT Security specialist.
Organizer	Vienna University of Technology (Vienna, Austria)
Cooperation with	-
Duration	4 semesters
Thematic Scope	This master degree enables the students to critically understand the theories and principles that enable them to develop highly specialized problem solving software architecture, systems software, Internet computing, or security. They will receive profound knowledge in computer languages, programming, distributed systems, algorithmics as well as economics and management. The learned methods and tools are used professionally for the analysis and the design of solutions, let them implement and verify software systems. In addition, they are firm in dealing with technologies, standards and software tools. During the studies, students will acquire important social skills such as communication and presentation, decision-making responsibility, leadership in complex projects.
Costs	-
No of ECTS credits	120 ECTS
E-learning	No
Tools	-
Job opportunities	The graduates of this degree program, are internationally competitive for further qualification in the context of a relevant doctoral program, but also for a career in academic or industrial basic research, in applied research and software development for industrial companies as well as in the areas of system analysis, software architecture and consulting.
Additional info	-
www	https://informatics.tuwien.ac.at/master/software-engineering-and-internet-computing/

No 639/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Cyber Security and Resilience

Description	In this master degree programme, students learn to develop and operate resilient information systems which are essential foundations for the functioning of our digital society. Taught in English, this programme is the best possible preparation for a successful career in both national and international companies. The dual structure of the master degree programme allows the students to put their acquired know-how into practice within the framework of projects with targeted mentoring. In this way, they achieve the best possible learning outcomes and are well prepared for current challenges.
Organizer	Sankt Pölten University of Applied Sciences (Sankt Pölten, Austria)
Cooperation with	-
Duration	4 semesters
Thematic Scope	Data Science, Network Security, Privacy and Cryptography, Security Management, Software Security, Digital Forensics and Incident Handling, Leadership and Problem Solving, Security Analysis, Security Networks, Cloud Computing Security,
Costs	EUR 363.36 (for students from third countries: EUR 1,500, performance-based tuition fee waivers are available) + student union fee
No of ECTS credits	120 ECTS
E-learning	Blended
Tools	-
Job opportunities	After completing the study programme, the graduates will have countless career opportunities in the domain of cyber security and resilience. Possible occupational fields include: (Chief) Information Security Officer, Cyber Defense Analyst, Security Consultant, IT Forensic Expert, Cyber Risk Manager, Information Security Auditor, Cyber Resilience Specialist, Data Protection Officer.
Additional info	-
www	https://www.fhstp.ac.at/en/academic-studies-continuing-education/computer-science-security/cyber-security-and-resilience?utm_source=www.fhstp.ac.at&utm_medium=www&utm_campaign=Kurzurl%20(Server)

No 640/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Data Intelligence

Description	The master degree programme Data Intelligence is your ticket to a comprehensive AI education. Students of this degree programme acquire all the competencies that are necessary for the sustainable promotion of data-driven innovations.
Organizer	Sankt Pölten University of Applied Sciences (Sankt Pölten, Austria)
Cooperation with	-
Duration	4 semesters
Thematic Scope	AI Architecture Management, Consulting Skills, Federated Machine Learning, IM-Clean Coding & Software Engineering, Knowledge Discovery & Information Retrieval, Trustworthy & Sustainable AI, DevOps for Machine Learning, Generative AI, Human-Centered AI, Innovation Management & Product Development, Reinforcement & Deep Learning, AI for Social Good, Change Management, Cloud Infrastructure, Data Intelligence Project Internship,
Costs	EUR 363.36 (for students from third countries: EUR 1,500) plus Students' Union (ÖH) fee
No of ECTS credits	120 ECTS
E-learning	-
Tools	-
Job opportunities	Graduates of this degree programme are able to meaningfully analyse and process data and information in order to take better, data-based decisions. As data can be collected in every sector, they will have the opportunity to work in various lines of business (e.g., production, logistics, health, marketing, security). Classic fields of activity include: Data scientist, Business analyst, Data architect, Data engineer, DevOps, Machine learning engineer, Chief Data Officer, Chief Data Scientist
Additional info	-
www	https://www.fhstp.ac.at/en/academic-studies-continuing-education/computer-science-security/data-intelligence

No 641/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Information Security

Description	Through the practice-oriented training in this Master's programme, you will learn competencies in the areas of IT infrastructure, software security, security management, privacy and incident handling.
Organizer	Sankt Pölten University of Applied Sciences (Sankt Pölten, Austria)
Cooperation with	-
Duration	4 semesters, full-time/ 5 semesters part-time programme
Thematic Scope	The curriculum includes the key topics of organisational security, infrastructure security, incident management & security analysis as well as detailed specialisation options, such as: Organisational Security, Infrastructure Security, Incident Management & Security Analysis
Costs	EUR 363.36 (for students from third countries: EUR 1,500) + student union fee
No of ECTS credits	120 ECTS
E-learning	No
Tools	-
Job opportunities	Prospective career options: • Chief information security officer • IT infrastructure engineer • Security consultant • Industrial security expert • IT security solution engineer/architect • Computer forensics expert • Compliance officer and risk manager • IT governance expert • IT solution architect • Malware analyst • Auditor
Additional info	-
www	https://www.fhstp.ac.at/en/academic-studies-continuing-education/computer-science-security/information-security

No 642/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Digital Innovation and Research

Description	The degree program offer a highly qualified education at this interface of applied research, innovation and digitalisation with a focus on topics such as artificial intelligence, governance and protection. This study programme, which is taught entirely in English, enables you to make an important contribution to the realisation of digital transformation.
Organizer	Sankt Pölten University of Applied Sciences (Sankt Pölten, Austria)
Cooperation with	-
Duration	4 semesters
Thematic Scope	Foundations of Research & Ethics, IM-Artificial Intelligence, Design Thinking, Entrepreneurship, IT Governance, Innovation Management and Product Development, IT Protection, Data Driven Innovation
Costs	EUR 363.36 (for students from third countries: EUR 1,500, performance-based tuition fee waivers are available) + student union fee
No of ECTS credits	120 ECTS
E-learning	-
Tools	-
Job opportunities	Graduates of this international master degree programme acquire competences at the interface of digitalisation, innovation and research, which provides them with the best possible preparation for the job market.
Additional info	-
www	https://www.fhstp.ac.at/en/academic-studies-continuing-education/computer-science-security/digital-innovation-and-research

Nr 643/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

IT & Mobile Security

Description	This Master's degree programme responds to modern IT concerns: the security of sensitive data, networks and systems is more important than ever before. Cyber-attacks on companies and private individuals have become the norm. Highly qualified specialists in the development and implementation of secure software are in great demand. The degree program allow to discover new approaches to enhancing IT security for digital solutions.
Organizer	FH JOANNEUM GmbH (Kapfenberg, Austria)
Cooperation with	-
Duration	4 Semesters
Thematic Scope	Secure Mobile Software Development, Security Fundamentals, Software Security, Cryptography, Cloud Computing, Operating Systems, Platform Specific Mobile Apps, Basic Network Security, Native mobile Apps, Secure Software Design, Secure Web Applications, Applied Cryptography, Database Security, Mobile Network Security, Mobile Cross-Platform Development, Ethical Hacking, Secure Big Data, Secure Service Oriented Architectures, Advanced System Exploitation, Operating System Security, Quantum Cryptography, Secure Systems, Secure Server Environments
Costs	Free
No of ECTS credits	120 ECTS
E-learning	Blended
Tools	-
Job opportunities	Our graduates are qualified for jobs in companies processing sensitive data, e.g.: • ICT service companies, • providers and businesses relying on ICT as a tool such as legal databases or e-government, • system providers and IT consultancies, • businesses active in the field of data security, • investigation and prosecution of ICT crime, • research and development.
Additional info	-
www	https://www.fh-joanneum.at/it-und-mobile-security/master/en/

No 644/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Data Science and Artificial Intelligence

Description	This degree programme provides students with an education in the field of data and information science. They gain in-depth knowledge of mathematical and statistical data and information analysis and learn to use intelligent analysis tools for transforming data and information into valuable knowledge. They will also be familiarised with business intelligence, database management and computational intelligence issues. Based on fundamentals in mathematics, statistics and informatics, they will learn the methods and tools required to transform data into valuable decision-making knowledge.
Organizer	FH JOANNEUM GmbH (Kapfenberg, Austria)
Cooperation with	-
Duration	4 Semesters
Thematic Scope	Scripting for Data Scientists, Information and coding theory, Database basics and query language, Relational Database Management, Introduction to Data Science, Descriptive Statistics, Probability theory and inductive statistics, Agent-based programming, High Performance Computing, Data Structures and Algorithms, Optimization and Numerics, Neural Networks, Analytical Information Systems, Multivariate statistics and data mining, Advanced information visualization, Data quality and data cleansing, Cloud computing for data scientists, Decision theory and game theory, Swarm intelligence and evolutionary algorithms, Business Development und Innovation, Project Management and Evaluation of Software Solutions
Costs	Free
No of ECTS credits	120 ECTS
E-learning	-
Tools	-
Job opportunities	Graduates are qualified for jobs in companies processing sensitive data, e.g.: ICT service companies, providers and businesses relying on ICT as a tool such as legal databases or e-government, system providers and IT consultancies, businesses active in the field of data security, investigation and prosecution of ICT crime, research and development.
Additional info	-
www	https://www.fh-joanneum.at/data-science-and-artificial-intelligence/master/en/

No 645/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Artificial Intelligence and Cybersecurity

Description	The Master's degree programme is heavily focused on the core subjects of artificial intelligence and cybersecurity. Additionally, it addresses social, ethical and legal aspects.
Organizer	Alpen-Adria University Klagenfurt (Klagenfurt, Austria)
Cooperation with	Università degli studi di Udine
Duration	4 semesters
Thematic Scope	Foundations of Artificial Intelligence and Cybersecurity, Social, Ethical and Legal Aspects of Artificial Intelligence and Cybersecurity, Introduction to Artificial Intelligence, Machine Learning and Deep Learning, Cybersecurity, Verification and Validation for Artificial Intelligence and Cybersecurity, Responsible Innovation
Costs	Free
No of ECTS credits	120 ECTS
E-learning	Blended
Tools	-
Job opportunities	Graduates of the Master's degree programme in Artificial Intelligence and Cybersecurity are distinguished by their special expertise in the fields of Artificial Intelligence and Cybersecurity. They are able to develop and implement complex solutions based on Artificial Intelligence Cybersecurity, taking into account social, ethical and legal aspects. In addition, the Master's programme prepares graduates for doctoral studies in the field of computer science.
Additional info	-
www	https://www.aau.at/en/studien/master-artificial-intelligence-and-cybersecurity/

Nr 646/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Information and Communications Engineering: Autonomous Systems and Robotics

Description	The branch of study "Autonomous Systems and Robotics" in the Master's degree programme "Information and Communications Engineering" provides you with the tools you need to work in many emerging fields of technology: autonomous robotics, driving assistance systems, self-driving cars, networked sensor and actuator technology, networked control technology and intelligent production systems are just a few of them.
Organizer	Alpen-Adria University Klagenfurt (Klagenfurt, Austria)
Cooperation with	-
Duration	4 semesters
Thematic Scope	Autonomous Systems and Robotics: Fundamentals, Autonomous Systems and Robotics: Advanced, Information and Communications Engineering: Supplements, Technical Complements
Costs	Free
No of ECTS credits	120 ECTS
E-learning	-
Tools	-
Job opportunities	Graduates of the Master's degree programme are qualified for a wide range of professional activities, for instance in the development or product management for technical systems for automotive manufacturers and suppliers, in automation engineering, in microelectronics, in consultancy services, and in medical technology. The branch of study Autonomous Systems and Robotics also offers the opportunity to acquire specialised expertise, for example in the following areas: autonomous robotics, driving assistance systems, self-propelled cars, networked sensor and actuator technology, networked control systems engineering, intelligent productions systems, automation engineering, intelligent traffic systems.
Additional info	-
www	https://www.aau.at/en/studien/master-ice-autonomous-systems-and-robotics/#structure

No 647/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title: **Cybersecurity**	
Description	Cybersecurity is a second year program (Master 2 with semesters 9 and 10) of the Mathematics and Computer Science Masters. Courses are in English and the program follows a first year Master 1 in Mathematics or Computer Science or equivalent.
Organizer	Université Grenoble Alpes (Grenoble, France)
Cooperation with	-
Duration	2 semesters
Thematic Scope	Topics covered in the training include: • Robustness of critical infrastructures when facing cyberattacks (e.g., stuxnet, wannacry), • Robustness of security components when facing software vulnerabilities and data leakage (e. g., heartbleed), • Privacy protection and cloud infrastructure security, • Robust design and evaluation of security components, • Detection of vulnerabilities in protocols for hardware and software components (e.g., meltdown, spectre). Topics covered in the degree program include also additional areas of Cybersecurity, such as cryptology, forensics, fuzzing or anonymization, especially for embedded systems and distributed architectures.
Costs	approx. 250 euros /per year
No of ECTS credits	70 ECTS
E-learning	No
Tools	-
Job opportunities	-
Additional info	-
www	https://casys.gricad-pages.univ-grenoble-alpes.fr/cybersec/

No 648/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	Robotics, autonomous systems, artificial intelligence
	European, national, regional project	University course **Postgraduate studies**	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	**Cybersecurity**

Title:

Master's Degree in Computer Security Engineering and Artificial Intelligence

Description	The Master's Degree in Computer Security Engineering and Artificial Intelligence prepares you to carry out responsible work in a wide range of areas, including industry, academia and public administration. The master's degree curriculum includes research topics related to information production, application security, machine learning, modelling and problem-solving, among others.
Organizer	Universitat Rovira i Virgili (Tarragona, Spain)
Cooperation with	-
Duration	2 semesters
Thematic Scope	Cryptology and Information Security, Computer Forensics, Biometric Identification, Multi-agent Systems, Artificial Vision and Pattern Recognition, Neuronal and Evolutionary Computation, Privacy Protection, Multi-criteria Decision Support Systems
Costs	1806€ (for students from the UE, Iceland, Norway, Liechtenstein, Switzerland and Andorra*, or resident in Spain, price for 2023-24). Rest of students: €2,913.
No of ECTS credits	60 ECTS
E-learning	Yes
Tools	-
Job opportunities	The Master's produces professionals with the skills to work in the following positions, among others: • Head of Computer Security and Artificial Intelligence projects. • Management of groups of developers for Computer Security and Artificial Intelligence projects. • Analyst of advanced ICT applications, particularly in the ambits of Computer Security and Artificial Intelligence. • Academic and research career in universities and research centres.
Additional info	-
www	https://www.urv.cat/en/studies/master/courses/computer-security-engineering/

No 649/2023

Fiche developed in the frame of	TYPE:		AREA:
	Conference	Training	**Robotics, autonomous systems, artificial intelligence**
	European, national, regional project	University course Postgraduate studies	C4ISTAR: command, control, communications, computers, information/intelligence, surveillance
	Policy	Journal	Cybersecurity

Title:

Automation, Robotics & Communications for Industry 4.0/5.0 (ARCI' 2024): 4th IFSA Winter Conference

Description	The ARCI' 2024 conference will incorporate main fields covering research and development in a broaden range in automation, robotics, communication and data analyses, and united by the Industry 5.0 challenges. However it will be not a conference only about the future concepts and new visions. It will be also to discuss how to adopt the current R&D results for Industry 4.0 and to customize products under the conditions of highly flexible (mass-) production.
Goal	The purpose of ARCI' 2024 is bring together leading international researchers, developers and practitioners to attain synergetic exchanges of ideas and practices. The conference will offer plenary and invited talks, contributed oral and poster presentations, special sessions, industry tracks, panel discussions, tutorials and exhibition of commercial products.
Organizer	International Frequency Sensor Association
Co-organizers/ Patrons	-
Topics	• Industry 4.0 / 5.0 • Automation • Robotics • Communications
Date	7-9 February 2024
Costs	450-690 EUR
www	https://arci-conference.com/

No 650/2023