PROGRAMME - AGENDA
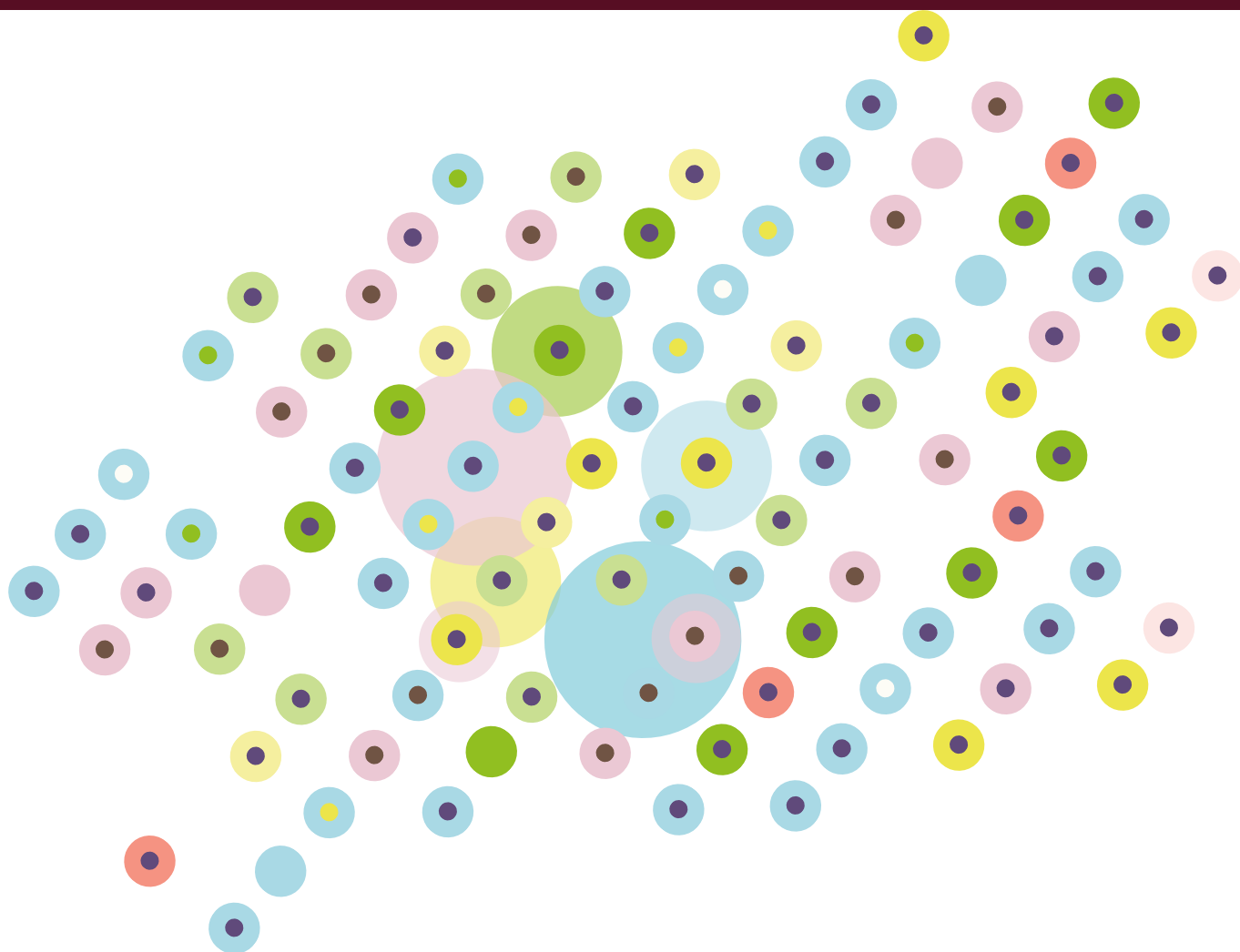
Dual-Use Technologies 2022

Cybersecurity & Digital Applications in Defence

Malaga, Nov 17-18 2022

ENDR Conference on Dual-Use Technologies 2022

Cybersecurity and Digital Applications in Defence
Malaga - 17-18 November 2022

CONTEXT AND OBJETIVES

The Roadmap on critical technologies for security and defence, adopted by the Commission on 16 February 2022, highlights the importance of cyber and digital technologies for defence.

"New technologies are transforming the security and defence sectors at a faster pace than ever before and blurring the dividing line between the civilian and military domain. Digital technologies in particular are affecting established balances of power within the global security landscape. It is thus essential to ensure that Europe's security and defence sectors remain technologically fit for purpose. Many critical technologies for security and defence increasingly originate in the civilian domain and use critical components of a dual-use nature."

> **"To accelerate innovation across domains and foster technological sovereignty in the security and defence sectors, better exchange between civilian and defence research and innovation communities is needed."**

On 10th November 2022, the Commission and the High Representative put forward a Joint Communication on an EU Cyber Defence policy, with this, the EU will enhance cooperation and investments in cyber defence to better protect, detect, deter, and defend against a growing number of cyber-attacks. The EU Policy on Cyber Defence aims to boost EU cyber defence capabilities and strengthen coordination and cooperation between the military and civilian cyber communities (civilian, law enforcement, diplomatic and defence). It will enhance efficient cyber crisis management within the EU and help reduce our strategic dependencies in critical cyber technologies, while strengthening the European Defence Technological Industrial Base (EDTIB). It will also stimulate training, attracting, and retaining cyber talents and step up cooperation with our partners in the field of cyber defence.

This Conference, organised by the **European Commission** and the Regional Government of Andalusia (through the **Agency of Innovation and Development of Andalucia**), aims to exchange views and raise awareness on the importance of the challenges of cybersecurity for European defence industry. Relevant EU programmes supporting cybersecurity and cyber defence R&D in these topics will be introduced.

The event will connect business stakeholders from all over Europe, via B2B meetings and Technical visits to industries. Participants will have the opportunity to provide solutions contributing to one of the eight cybersecurity challenges launched by the corporates (AIRBUS Defence & Space; Indra; Navantia and Telefonica Tech).

"Dual Use Technologies 2022" will be the seventh of its kind taking place in Andalusia demonstrating the strong commitment of the Spanish region to the 2015 Seville Declaration on enhancing the full potential of defence and dual use technologies and markets.

AGENDA
17th November 2022

Opening session

Master of ceremony: **Stéphane Ruiz Coupeau.** Project Officer, IDEA Agency.

08:30 - 09:00	**Registration and welcome coffee**
09:00 - 09:15	**Welcome** **Paul Anciaux,** Policy Officer, European Commission, DG DEFIS **Esperanza Nieto Lobo,** DG Planning, Economic and Financial Policy, Regional Government of Andalusia
09:15 - 09:55	**Introductory Keynote Speech** **Spanish Cyberspace Combat System: current and future technologies** **Colonel Francisco Palomo,** Joint Cyberspace Command (CMCCE). Spanish Ministry of Defence **European cybersecurity and cyber defence market** **Andreas Mitrakas,** Head of Unit, European Union Agency for Cybersecurity

Funding opportunities at EU level

In the current European multiannual financial framework, several programmes have been launched to support R&D cooperation projects in the field of cybersecurity and digital transformation. The European Union works on various fronts to promote research into digital security and others digital technologies critical for defence. During this session an overview of these programmes will be provided.

09:55 - 10:20	**Opportunities offered by the European Defence Fund: focus on cyber defence and digital transformation** **Getter Oper,** Policy Officer, European Commission, DG DEFIS
10:20 - 10:40	**Opportunities offered by Horizon Europe and Digital Europe: focus on cybersecurity and digital** **Fidel Santiago,** Programme Manager, European Commission, DG CNECT
10:40 - 10:50	**Building consortia: Enterprise Europe Network as a key enabler** **Nuria Villén,** Project Officer, IDEA Agency

10:50 - 11:15	**Coffee break**

Cybersecurity & cyber defence: how to strengthen cyber resilience and European cyber market

The aim of this session is to have an exchange of views on how cyber resilience and the European cyber market and the European Defence Industrial and Technological Base (EDTIB) can be strengthened.

11:15 - 12:15	Moderator: **Mar López,** Founder and VP, W4Cyber Spain **Roberto Cascella,** Head of Sector, European Cyber Security Organisation **Jorge Maestre,** Senior Specialist in Cyber Defence, Indra **Belén García Molano,** Vice President and Technology and Development Director, Airbus Defence and Space

Regional experiences on supporting cybersecurity industry

This session brings two regions together to exchange best practices on how to support cybersecurity industry and SMEs, and foster dual use (defence-related) development strategies, including the integration of defence industrial and research assets into smart specialisation strategies.

12:15 - 12:55	**Andalusian case-study. A regional cybersecurity strategy (2022-2025** **Enrique Rando González,** ITC Services Management, Andalusian Digital Agency **Bretagne case-study. What framework for the development of the ecosystem to meet the challenges of duality** **Hélène Morin,** Head of European affairs department, Bretagne Développement Innovation

12:55 - 14:25	**Lunch**

Pitches and demos

Space for SMEs, industry and research groups to introduce their innovative projects, share specific initiatives or tell about their success stories.

Moderator: **Maribel Bermúdez.** Project Officer, IDEA Agency.

14:25 - 15:25   Session 1: Digital Technologies critical for defence

ORGANISATION/SPEAKER	TITLE OF PRESENTATION	DESCRIPTION OF PRESENTATION
VISTORY	Remote secured production for Defense Industry and Armies overseas	This solution secures the industrial property of designers and manufacturers while being printed and used by armed forces. By using MainChain as trusted third party, it creates a business model and warranty aknowledgement between stakeholders, developed MainChain, which dematerializes and secures production and makes additive manufacturing accessible to all industry sectors. MainChain by Vistory brings together all the players in the value chain (manufacturers, specialized suppliers, end-customers, etc.), offers total risk control and builds trust throughout the digital supply chain through transparency and traceability.
SPACE HELLAS	PANDORA EDIDP Project Results	EDIDP Pandora project aims at contributing to EU cyber defence capacity focusing on endpoint protection, as well as information sharing. We are working towards building an innovative platform called PANDORA utilizing several well known open source frameworks and components. The system design covers the full chain of an attack to protect military infrastructure endpoints, from the Incident Detection and to Incident Respond and Information sharing. As we getting very close to the end of the project we have some demonstratable results and we have already attracted the interest of the related PESCO CTISP project members states to commercialize the outcomes of the project
INTEGRASYS, S.A.	Anti-jamming and Cybersecurity solutions for Defence	Electronic Protected Measures (EPM) is an essential part of the mechanism to protect the communications agains adversary. Integrasys proposes secure network solution based on RF protection (antijamming solution) and also using innovative technology based in blockchain to detect potential intrusion in the network at the digital level.
DECENTRALIZED SECURITY	Cybersecurity and Blockchain	Blockchain is a very promising technology with plenty of open challenges, among them security is of paramount importance. Also, the trade-off between privacy and transparency in blockchain poses many challenges. We work to make blockchain safer for all actors involved.
CLOUDLAN S.L. (TEKPYME)	Security as a Service	From Tekpyme we are going to review the main vulnerabilities that organizations have today that makes them vulnerable to cyber attacks, seeing how Tekpyme advises and applies solutions to its clients from the organization of the company to its end user to improve security of its structure
HISPASEC		
UNIVERSIDAD CEU SAN PABLO	Security evaluation and protection against side-channel attacks	An increasing concern in cyber-security are attacks that depend on hardware rather than software access or mathematical properties of cryptographic algorithms. Device electromagnetic radiation, power, sound and timing can reveal sensitive information, but commercial and end-user devices, including those dealing with raw personal information or biometric data, are often unprotected. Our goal is to explore possible system vulnerabilities, discover exploitable signal leaks and anticipate dangerous scenarios to develop proper countermeasures. So far we have developed a security evaluation platform for power side-channel attacks and we have analyzed the success rate of attacks on microcontroller and FPGA platforms as well as apply countermeasures based on voltage modulation.
STEFANINI GROUP	European cybersecurity resilience opportunities	

15:30 - 16:30	**Session 2: Digital Technologies critical for defence**	

ORGANISATION/SPEAKER	TITLE OF PRESENTATION	DESCRIPTION OF PRESENTATION
UNIVERSITY OF SEVILLE	Post-quantum cryptographic methods for protection and matching of imprecise sensitive data	This presentation shows how post-quantum cryptographic methods can be employed to protect data, store them securely in maybe malicious data base servers, and match them in the encrypted domain to obtain if they are enough similar or not without revealing sensitive information. The methods have interesting applications, such as to establish secure communication channels between biometric authenticated parties and to implement secure image retrieval systems.
COUNTERCRAFT	How cyber deception can help Defense organisations	We are currently working with a number of defense clients in EU and USA in cyber deception projects. There are a number of different use cases, making cyber deception a great technique when dealing with other nation state sponsored groups. By using cyber deception, organisations not only can detect other threat actor activities, but collect insightful threat intelligence about them.
CYBERCRIN	Computer security democratization	Cybersecurity startup that seeks to democratize computer security in SMEs
DRAGONPRAXIS	BackPack Close Air Support	Problem: The unavailability of Air Support increases the risk associated with the entry of limited firepower and protection Force into a hostile urban environment area; Solution: Provide the Force with organic air resources, remotely operated, that can take off without the need for a runway, escorting the contingent along the way or just taking off on approach to the urban area; prior to the entry of the Force, the air system will send visual information, IR as well as electromagnetic activity and NBC data; upon the Force entry into the area, the air system will provide cover with its ability to "hover" and launch grenades/rockets under the control of the Force moving on the ground.
EXPERTWARE	New Generation Security Operations Centre	Unique solution combining Network, IOC and Security Operation Centre, ingesting & matching multiple cyberthreat intelligence sources, continuous vulnerability scanning, advanced hunting and managed detect and response workbooks.
SILESIAN UNIVERSITY OF TECHNOLOGY	Our experience in Cybersecurity	
WAR STUDIES UNIVERSITY		

Business-to-Business (B2B)
Business-to-Corporations meetings (Tech Challenges)

The aim of this Brokerage Event is to provide participants with the opportunity to meet with potential business partners, clients and/or suppliers through 20 minute, pre-scheduled meetings (B2B meetings).

4 large corporations (Airbus Defence and Space, Indra, Navantia and Telefonica Tech) have launched 8 Technology Challenges. They will meet with the selected solution/technology providers through 20 minute, pre-scheduled meetings.

From 21st to 25th Nov, those on-site participants that cannot attend all the requested meetings during the on-site "Brokerage Event" on the 17th Nov, will have the possibility to hold online meetings.

16:30 - 18:30	**B2B Matchmaking facilitated by Enterprise Europe Network (EEN) at the venue**	

enterprise
europe
network

Business Support on Your Doorstep

16:30 - 18:30 **Business-to-Corporations meetings
(Tech Challenges)**

Navantia

1

CYBERSECURITY ON DYNAMIC MULTICLOUD

Technological solutions that enable the deployment of cybersecurity services in multicloud environments (national and international) that contemplate the protection of both infrastructure and data, in an adaptive way as the environment changes. The technologies will enable monitoring and vulnerability scanning, risk assessment and management, forensic analysis and integration with SOCs, as well as staff training.

2

QUANTUM COMPUTATIONAL

Technological solutions based on quantum simulators on traditional computers that allow the secure migration of encrypted data using traditional cryptography to post-quantum cryptography (based on OQS-type algorithms), so that this migration is fully automated and guarantees the preservation of the confidentiality and integrity of the migrated data.

Telefónica Tech

3

INTEGRATION OF INTELLIGENCE EXTRACTION TOOLS OVER NETWORK TRAFFIC SESSIONS FLOWS

Investigate and test the different forms of integration of both commercial and open-source intelligence extraction tools on network traffic directly or on network traffic processing tools (Arkime, Wireshark, etc.). As a result of this integration, it is expected that detected threats, especially those targeting OT/IoT devices, will be linked to network traffic sessions.

Airbus

4

DISINFORMATION WARFARE AND GREY ZONE

Disinformation and coordinated campaigns or actions intending to influence or change perception by spreading false or malicious information are a high risk to modern societies. This challenge is focused on technologies, methodologies or application of novel techniques that can help in identifying, uncover and fight against these campaigns and actions by malicious actors.

5

COOPERATIVE CYBER AND DATA-CENTRIC SECURITY

Security in distributed systems is of highest importance for future foreseen combat-cloud type of scenarios. This challenge focuses on agents able to identify and cooperate against identified threats and security breaches in dynamically changing networks. It also addresses the need to exchange data at multiple security-levels, using common networks and infrastructure, applying data-centric security paradigms in light and efficient ways.

Indra

6

CYBER-ATTACK ATTRIBUTION AND AGNOSTIC DECISION-MAKING PROCEDURES

When investigating a cyber-attack, attackers usually cannot be identified with full confidence, and if identified, the attribution starts with a post-mortem analysis, which affects real-time response time. This challenge will focus on the agnostic attribution of cybersecurity incidents to have a joint vision, adapting to changes in a dynamic way to perform risk management, helping in automation and in decision making when a threat is unclear.

7

CYBER AND ELECTROMAGNETIC ACTIVITIES

Cyber activities are activities to gain an advantage over adversaries both in cyberspace and across the electromagnetic spectrum. Emerging security threats, as well as lessons learned, have already shown that to achieve operational goals in traditional physical domains, it is crucial to secure dominance in non-physical domains, with the combination of cyber and electromagnetic activities a new challenge to obtain an operational advantage.

8

TRUSTWORTHY USE OF AI AT INCIDENT MANAGEMENT DECISIONS

Combining the output of ML models and domain expert knowledge is a known challenge. This will focus on having a Trustworthy AI, requiring a holistic and systemic approach, using interpretability mechanisms to 1)guarantee neutrality in decision making, 2)guarantee the reasoning of the model using only significant variables will infer a result, 3)facilitate the robustness by highlighting adversarial disturbances that can change the prediction

18th November 2022

09:00 - 14:00   Site visits

Malaga is a leading city in cybersecurity terms. The participants will have the opportunity to visit the local actors who play a leading role in the ecosystem through the following itinerary.

09:00h - Pick up at Eurostars Hotel. Málaga

Málaga Tech Park Headquarters

Located in Malaga, with more than 630 companies installed in and more than 60 international firms, the Málaga TechPark gathers 20.000 professionals that contributes to a sustainable economic growth. Málaga TechPark is a place where companies contribute to implement the 2030 Agenda towards a sustainable development.

Speakers:

Lourdes Cruz, Business Development & Investment Promotion Director

Javier López, Vice-Rector for Business, Digital Transformation and Territory at the University of Málaga

Hispasec

Hispasec is the oldest cybersecurity company in Spain with 24 years of history. From its SOC, it offers cybersecurity services to more than 70 banking institutions around the world. It also protects the brands of large retail companies, public entities and audits a multitude of companies from its technical and regulatory audit department.

Hispasec has managed to create state-of-art security products with a great impact on the industry. See the example of the sale of Virustotal to Google in 2012. Hispasec has the most important and relevant certifications on the standard for information security and the National Security Scheme.

Babel

Babel is a multinational technology company specialized in applying its technological services and knowledge to the digital acceleration process of its clients, big companies, and public organizations.

Babel has 2,700 highly qualified professionals distributed in 14 countries and its competitive advantage lies in the team and in the corporative culture, on where it builds, above personal leaderships, a long-term future project. The Babel Cybersecurity Global Hub has 30 years of experience, nearly 600 projects in more than 200 clients worldwide and is located in Malaga Tech Park.

Quandum

Quandum was established in 2006, thanks to the signing of several agreements with Airbus Military. Since then, it designs, develops and manufactures optoelectronic and electronic devices and systems for the Aerospace market and in general, for special industrial uses.

Their facilities have the equipments and tools that are needed to give the best service in each activity. There are measurement equipments to make different type of tests, as well as an electronic lab, an industrial design lab, manufacturing area and test benches.

14:00h - Arrival at Eurostars Hotel. Málaga

https://dualuse2022.b2match.io/signup

EEN CO-ORGANIZERS

SUPPORTERS