EUROPEAN DEFENCE AGENCY

PT Cyber Defence Industry Day on Air & Space

7th March from 10:00 to 8th March 14:00
EUROCONTROL, Rue de la Fuseé 96, 1130 Brussels
Meeting Room : EUROPA

AGENDA

Day 1, 7th March 10:00– 1700	
1	**Welcome and introduction** (10:00 – 10:10)
2	**EDA intervention: Air Domain** (10:15 – 10:40) Hannes Alparslan (EDA)
3	**EDA Intervention: Space Domain** (10:40 – 11:05) Ferdinando Dolce (EDA)
Coffee Break (11:05 – 11:40)	
4	**NCIA perspective on Cyber Security and Mission Assurance in support of the Air Domain** (11:40 – 12:10) Federic Jordan, Kevin Mepham (NCIA, NATO)
5	**Cyber Security Risk Analysis of Military Aerospace Systems** (12:10 – 12:40) René Wiegers (NLR)
Lunch Break (12:40 – 13:50, non-hosted)	
7	**Using AI for user and entity behavior assessment** (13:50 – 14:20) Sylvain Navers (Airbus Cyber Security)
8	**Cyber Resilience for Avionics Defence** (14:20– 14:50) Luigi Lupoli (Leonardo)
Coffee Break & visit of the exhibition (14:50– 15:20)	
10	**The Cyber-dimension in context of hybrid warfare** (15:20 – 15:50) Josef Schröfl (The European Centre of Excellence for Countering Hybrid Threats)
11	**Round Table Discussion** (15:50– 17:00) This interactive sessions will accommodate the presenters of the industry of day 1 and offer the opportuntiy for the audience to engage into a dialogue.
Day 2, 8th March 09:00 – 13:00	
1	**Welcome and introduction to newcomers** (09:00 – 09:15)
2	**EDA – ESA intervention: Study on Cyber Defence in Space** (09:15 – 09:45) Florent Mazzurelle (ESA), Patrick Langlois (EDA)
3	**“Confidence in Security”: the new slogan of an interconnected world**

	(09:45– 10:15) Marco Brancati (Telespazio)
4	**Security Accreditation in Classified Projects** (10:15– 10:45) Julio Vivero Millor (GMV)
Coffee Break (10:45– 11:15)	
5	**Contributing to a secure environment for the Air and Space domain** (11:15– 11:45) Dirk-Roger Schmitt (DLR)
6	**Round Table Discussion & Closure of the event** (11:45– 13:00) This interactive session will accommodate the presenters of the industry of day 2 and offer the opportunity for the audience to engage into a dialogue.
	End of Industry Days (13:00)

Abstracts

Challenges in the Air Domain

(Hannes Alparslan, EDA, Day I, 10:15 – 10:40)

Cyber Defence in the Air Domain has been an emerging topic for several years. New entrants to the airspace, 5th Generation Aircraft and Digitalisation account only for a subset of reasons that require appropriate actions. This intervention will provide the EDA perspective on current and future challenges and shall inform about ongoing and planned ambitions in this area.

Challenges in the Space Domain

(Ferdinando Dolce, EDA, Day I, 10:40 – 11:05)

In the past decades, exercises and missions for military but also the daily life of civil society became increasingly dependent on the use of space assets, e.g. in the form of GNSS (Global Navigation Satellite Service). Degradation or even disruption of services from space assets have significant impacts thus, must be mitigated. EDA will provide an overview on which activities are ongoing or foreseen.

NCIA perspective on Cyber Security and Mission Assurance in support of the Air Domain

(Frederick Jordan, Kevin Mepham, NCIA, Day I 11:40)

The presentation will provide an overview on the NCIA's mandate in Cyber Security, on the Cyber Threat landascape and will then focus on security and safety of air systems in a multilateral federated environment.

Frederick Jordan is Section Head for Capability Development, Cyber Security Service Line, NCIA. Kevin Mepham is Head CIS Security, AMDC2, NCIA.

Cyber Security Risk Analysis of Military Aerospace Systems

(René Wiegers, NLR, Day I, 12:10)

To support their operation, military aircraft are becoming more and more reliant on advanced on-board software and connection to networks, making cyber-security an essential part of flight operations. A preliminary high-level security cyber security risk assessment framework for military flight operations is presented, which is a first step in the development of a dynamic security risk assessment methodology.

Mr. René Wiegers is Senior R&D Manager at the Netherlands Aerospace Centre NLR. René holds a Master of Science degree in Software Engineering and leads NLR's aerospace cyber security research.

Using AI for user and entity behavior assessment

(Sylvain Navers, Airbus Cyber Security, Day I, 13:50)

Analysis of the behavior of individuals and entities (UEBA), is an area of artificial intelligence that can be used to detect hostile actions (e.g.: attacks, fraud, influence, poisoning) through the unusual nature of the observed events, by opposition to a mechanism based on signatures. A UEBA process usually includes two phases, learning and inference.

Intrusion Detection Systems (IDS) market still suffer from bias in particular over-simplification of the problems, an under-exploitation of the potential of the AI, of an insufficient consideration of the temporality of events, and perfectible management of the memory cycle of behaviors. In addition, while an alert generated by a signature-based IDS can refer to identifying the signature on which

the detection is based, the IDS of the domain UEBA produce results, often associated with a score, whose explicable character is less obvious.

Our unsupervised approach is to enrich this process by adding a third phase to correlate the of events (incongruities, weak signals) allegedly related to each other, with the benefit of a reduction of false positives and negatives. We are also looking for avoiding a so-called "boiled frog" bias inherent in continuous learning. Our first results are interesting and have a explicable character, both on synthetic and real data.

Cyber Resilience for Avionics Defence

(Luigi Lupoli, Leonardo, Day I, 14:20)

The growing demanding for a more efficient and effective defense systems operation, their suitable integration and interoperability with other assets and a certain unavoidable degree of technologic interoperation of military networks with the external civil environment in the domains air, sea and land, are intrinsically introducing potential vulnerabilities in the cyber space. The employment of systems and assets of an antecedent generation to the current cyber threat as today known and, last but not least, the use of "Dual Use" technologies, may bring a rapid and continuous evolution of threats.

Air Superiority and the modern Air Force operational effectiveness could be exposed by the sophistication of cyber attacks and their rapid propagation in the various assets and systems and nodes of a military network. For these reasons the need arises to implement appropriate strategies, processes and procedures to ensure the Air Forces an adequate Cyber Resilience of their assets throughout the operational life cycle of airborne platforms.

The Cyber-dimension in context of hybrid warfare

(Josef Schröfl, The European Centre of Excellence for Countering Hybrid Threats, Day I, 15:20)

Hybrid CoE has been established in 2017 in Helsinki, Finland, is an international hub and operates through networks of practitioners and experts. The goal is to build member states' + institutions' capabilities and enhance EU-NATO cooperation in countering hybrid threats. Main focus areas are: Hybrid warfare, related strategies and implications for security policy, military and defence. This includes the work on improving the conceptual understanding on hybrid warfare, - also in context to Cyber War.

"Confidence in Security": the new slogan of an interconnected world

(Marco Brancati, Telespazio, Day II, 09:45)

With respect to the entire Cyber Security process Telespazio is both a "service provider" (see for instance its activity related to Galileo Data Distribution Network (GDDN) and its "Ground as a Service" provided solutions) but also a "stakeholder". As a matter of fact Telespazio is working to make its space centers and teleports increasingly robust compared to cyber attacks. This is of great importance as these are its access points from space segment to the global terrestrial network, but they are also the infrastructures on which Telespazio bases its services provision.

Existing infrastructures must be made as resilient as possible, being aware that 100% coverage against cyber attacks risk is an asymptote to be aimed at but not practically achievable. Today, security requirements must be considered right from the design phase of the new systems. In case of complex systems, the level of security with respect to the cyber risks is defined by the resilience degree of the weakest element in the whole chain. Hence, the importance of having a suppliers chain adequately equipped with respect to this risk.

Telespazio is focusing on the "Cyber4Space" service segment to minimize the risks deriving from possible attacks to SatCom and SatNav signals. In doing that, integration with proposition provided by LDO, that has methodologies and services for cyber risk management, secure by design approach and monitoring of the security status, is also fundamental.

Security Accreditation in Classified Projects

(Julio Vivero Millor, GMV, Day II, 10:15)

Air and Space has been widely recognized as a critical infrastructures, providing and supporting uncountable services to the society. Often, part of the mission data used or exchanged is considered EU classified. When this happens the mission security has to be accredited. This has several implications that must be known and fulfilled in order to get authorisation to start the mission operations.

The main document that governs the rules for protecting classified information in the EU is the Council Decision 2013/488/EU. From this Council Decision more specific documentation is derived to deal with the specificities of the missions and of some technical requirements.

The main requirements for accreditation of missions processing EUCI (EU Classified Information) can be organized in the following categories:

- Facility and Personnel Security Clearances (FSC and PSC)
- Protection of classified information
- Certification of network equipment
- Double approval of cryptographic equipment
- Accreditation process
- Accreditation milestones

The accreditation is granted by a Security Accreditation Board (SAB) which will be assigned to the mission based on several factors. Usually, the National Security Agencies (NSA) of the Member States where mission infrastructure processing EUCI is located also participate in the process.

Contributing to a secure environment for the Air and Space domain

(Dirk-Roger Schmitt, DLR, Day II, 11:15)

Since its foundation the German Aerospace Centre is conducting civil and military research in the air and space domain. Following the apparent security breaches of the last decades and the ever-changing threat vector evolution for these critical applications, the DLR has set up dedicated projects and programmes to develop and apply appropriate counter actions. Examples based on recent projects like GAMMA (Global ATM Security Management Project) are given.