09:00 09:30	**Institutional opening**		
09:30 10:00	**Threat Intelligence from southern Europe to LATAM** Description: We are going to discuss Threat Intelligence, the type of comprehensive solutions that stem from it and how they can be tailored to protect national defence entities from an ever-evolving landscape of cyber threats.	Hispasec	Anabel Nsue
10:00 10:30	**LiFi data communications for last mile connections** Description: Radio frequency detectable, poor connectivity, hundreds of meters of cables and junction boxes and excessive deployment time are some of the current problems that command posts have to face during operations deployed around the world. However, the most dangerous issue is the interception or detection of communications by third parties, which can put lives and missions at risk. DATLIGHT has developed in collaboration with the BRIX a solution based on LiFi technology, which provides security to wireless communications and cannot be intercepted by unauthorized personnel and continues to optimize the product to the required military specifications with the participation of the University of Malaga. The collaboration with the X Brigade of the Army of Cerro Muriano Córdoba (Spain) has demonstrated that this disruptive and dual technology is ideal to solve all these problems, even more so in the current global geopolitical context.	Datlight	Covadonga Fernández Nebreda, CEO and Co-Founder, DATLIGHT, SL., and Juan Herrero, Industrial Organization Engineer CUD (Defense University Center)
10:30 11:00	**The challenge of supply chain cybersecurity in shipbuilding** Description: In 2020, a cyberattack using software produced by SolarWinds as a vector affected thousands of customers. This is the most serious of the so-called supply chain cyber-attacks.	Ghenova	Enrique Cubeiro

	These attacks are becoming increasingly frequent and have a high success rate. They are structured in at least two phases: the first phase compromises the supplier, who is used in the second phase as a vector to gain access to the final target, taking advantage of his privileged position to increase the chances of success. Many of these attacks are perpetrated by State actors (APT groups, Advanced Persistent Threat), specialized in targeted, sophisticated, complex to detect and difficult to attribute attacks. A naval unit is a clear target of interest for State actors (espionage, sabotage) and the supply chain necessary for its construction is particularly long and wide. In addition, many shipyards are integrators, so their suppliers are suppliers of equipment or systems that have their own supply chain. In general, these attacks use the software provided by suppliers as a vector, but there is an infinite amount of equipment on board that has some kind of embedded software and interconnects with other systems on the ship, so they can be used to attack critical systems. Managing this risk is complex, but it is possible. It requires the coordinated adoption of a wide range of measures, bearing in mind that a ship's exposure to cyber threats is greatest in the construction and operation phases, but already exists from the definition and design phases.		
11:00 11:30	**Coffee Break**		
11:30 12:00	**Sharing information without compromising or exposing data: the GMV u-Tile approach** Description: Security controls within organizations makes it difficult for data scientists to perform aggregated analyses of multiple data silos, particularly if they are dispersed. To date, it has been necessary to choose between privacy and usability.	GMV	José Carlos Barrios, Jefe de proyecto en la división de Big Data e Inteligencia

	At GMV we are posing the following question: "Would the problem be solved if instead of sharing data we shared information?" From that question arose the idea to develop uTile PET (Privacy-Enhancing Technologies), a solution which allows calculations to be made using distributed data in a safe, private manner, without exposing them or moving them out of the organizations. This solution uses confidential data in order to improve machine learning algorithms and analytical models, while at all times meeting organizational cybersecurity requirements and guaranteeing data privacy in accordance with current legislation or data classification. This new paradigm opens the door to cooperation between organizations from different fields, for example, public-private or inter-sector collaboration exploiting synergies.		
12:00 12:30	**Deployable SOCs** Description: This presentation will address aspects related to deployable SOCs in military operations environments and the importance of an orchestrated view of the operation for rapid decision-making, with an emphasis on the information intake necessary for creating dashboards, safeguarding the complexity between various systems, and managing different security classifications in operational environments.	Bertrandt	Diego Fernández
12:30 13:00	**Indra Cyber Defence - more than 10 years collaborating in the operationalization of cyberspace in Europe** Description: In recent years, Indra has become an essential player in understanding and accompanying cyber commands in the development of essential capabilities for their operations in cyberspace. We are currently leading from the Industry the development of strategic and operational Command and Control capabilities for the European Union, as well as the capacity to acquire situational awareness in cyberspace.	Indra	Joan Enrique Vicent

	In this proposal we want to highlight the value of multidisciplinarity and understanding of native military needs in cyberspace, beyond cybersecurity.		
13:00 13:30	**Malware Hunting in the age of IA**	Google	Francisco Perdomo, Security Engineer en Google
13:30	Networking Cocktail		