MILTEC 19

CONFERÊNCIA INTERNACIONAL

The changing face of warfare: from cyber to unmanned systems

21 Fevereiro, 2019

Lisboa, Instituto Universitário Militar (IUM)



ORGANIZAÇÃO:

AFCEA PORTUGAL

EMGFA

Agenda

01 **The global geopolitical and strategic situation**

02 **The operational situation: the new threats; the threat of cyberspace**

03 **The technological response: emerging technologies**

04 **The technological response: the weapons of the future**





Session 1

The global geopolitical and strategic situation

altice AIRBUS DEFENCE & SPACE aws indra Microsoft secunet THALES EDISOFT DEFENCE & AEROSPACE

General Pinto Ramalho

"Technology and the Challenges of the Operational Employment"



Work Experience

2006 ~ 2011 Army Chief of Staff.

2004 ~ 2005 Director of Military University Institute.

1999 ~ 2004 Head of Cabinet of the Minister of Defense;
Director General of National Defense Policy

1998 ~ 1999 Head of Planning and Programming Division;
Chief of Staff of the Ground Forces Command.

José Luiz Pinto Ramalho

Master´s degree in Strategy in the ISCSP of the University of Lisbon.

Professor of Strategy and International Relations the ISCSP.

He was Military Advisor at PODELNATO and NADREP as well as National Representative on Security and Protection of Nuclear Weapons.

Served in combat missions and at headquarters in Angola and Macau.



Major General Erich Staudacher

"Connection is key… to meet today´s security challenges"

General Manager
AFCEA Europe



Work Experience

2017 ~ 2019 General Manager AFCEA Europe

1974 ~ 2005 Served in combat missions and at several headquarters and ministerial levels. Dep Military Adviser to the German Mission at the United Nations

2005 ~ 2017 Vice Director of Staff Joint Armed Forces;
Director of Staff of the Air Force;
Vice Director of Bundeswehr Planning Office

https://www.linkedin.com/in/erich-staudacher-8261b6111//

Erich Staudacher

Master´s degree in Aeronautical and Space Technology.

Bachelor´s degree in Economics.

After retirement he joined AFCEA International as VP EMEA and General Manager Europe in January 2017.



Professor Eric Grove

"Naval Warfare in the 21st Century; What Has Changed and what Stays the Same?"

Naval Historian and International Strategic Analyst



Education:

- MA War Studies, King's College University of Hull;
- MA History, University of Aberdeen
- PhD Security Studies, University of Hull

His many books include:

- 'Vanguard to Trident', the standard work on post-1945 British naval policy
- 'The Future of Sea Power'

https://www.linkedin.com/in/eric-grove-ba23b8b5/

Eric Grove

He has taught at the Royal Naval Colleges at Dartmouth and Greenwich, the US Naval Academy, Annapolis and the Universities of Cambridge, Hull, Salford and Liverpool Hope.

He retired from full time teaching in 2015 although he continues as a visiting supervisor at Cambridge and an external examiner for PhDs at several universities and for the Plymouth University degree at Dartmouth.

He speaks at conferences around the world, does a great deal of writing and often appears in documentaries and news programmes on both radio and TV.

He was a co-author of the original edition of British Maritime Doctrine and is a First Sea Lord's Fellow.

UNIVERSITY OF CAMBRIDGE



Sérgio Barbedo

"The New Frontiers of Digital Transformation"

General Manager
Edisoft



Work Experience

2013 ~ 2019 General Manager of Edisoft

2010 ~ 2013 Aerospace & Defence Director at Thales PT

2011 ~ 2015 Security Committee of ASD Europe

2005 ~ 2010 Defence Committee of ASD Europe

2005 ~ 2010 Board of Directors GMV Portugal

2001 ~ 2005 Board of Directors Skysoft

https://www.linkedin.com/in/sergiobarbedo/

Sérgio Barbedo

Graduated in Civil Engineering by Instituto Superior Técnico

MBA from Portuguese Catholic University

National Defence Auditor by the Portuguese National Defence Institute

Additionally, has held positions as President of the General Assembly and member of the Audit Committee of **ANETIE** (National Association of Information Technologies and Electronics), member of the Board of Directors of **DANOTEC** (Industry Portuguese Defence and Armaments Association), **Proespaço** (Portuguese Space Industry Association) and **PEMAS** (Portuguese Association for the Aerospace Industry).

THALES
EDISOFT



EDISOFT
DEFENCE & AEROSPACE

The New Frontiers of Digital Transformation

Powered by THALES

AFCEA MILTEC19

Session 1 – The global geopolitical and strategic situation

A THALES Group Company

EDISOFT

DEFENCE & AEROSPACE

Engineering Solutions Without Borders



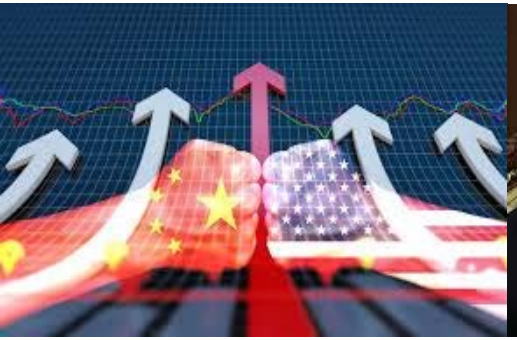
01 ACCELERATING TECHNOLOGICAL CHANGES

02 TECHNOLOGIES IN REAL LIFE
SEA - LAND – AIR – CYBER - SPACE

03 VOLATILITY IS BACK

04 GOING BEYOND the LAND & the SEA…

What´s Next...



US Trade war will hit China and make it face slowest growth in 3 decades https://asia.nikkei.com



New Ballistic Missile to Frighten Europe which travels at 20 times the speed of sound and has a range of 6,000km https://www.washingtonpost.com

The World is Going Digital



- Global Threats / Multiple Actors
- International Cooperation in a Human Centric Apps Environment
- Widening Rich/Poor gap
- Technology Sharing / Sovereignty
- Physical Walls / Digitally Borderless



Europe @ a crossroad







The European Framework EDA, PESCO, NATO & BREXIT

Nano + Quantum + AI Singularity
+ Super Conductors
may change Power Balance
Very, Very FAST!!



Session 2

The operational situation:
the new threats;
the threat of cyberspace

altice AIRBUS DEFENCE & SPACE aws indra Microsoft secunet THALES EDISOFT DEFENCE & AEROSPACE

Rear Admiral António Gameiro Marques

"New threats coming from cyberspace: are we prepared?"

National Information Security Authority



Work Experience

2016 ~ 2019 Director-General of the National Information Security Office

2013 ~ 2016 Deputy Secretary General of MoD

2009 ~ 2013 Navy *Chief Information Officer* (CIO)

2004 ~ 2007 Navy Military Adviser to the Portuguese Ambassador to NATO in Brussels

1981 ~ 2004 Served in several Navy Units

https://pt.linkedin.com/in/ant%C3%B3nio-gameiro-marques-981b4726

António Gameiro Marques

Degree in Naval Military Sciences, Navy Branch, Naval Academy, Lisbon.

Master of Science in Electrical and Computer Engineering, Naval Postgraduate School, Monterey.

Attended the 39th Senior Management Program (PADE) of AESE/IESE – Business and Management School, from NOV2013 to APR2014.

GNS
Gabinete Nacional de Segurança

REPÚBLICA PORTUGUESA

PRESIDÊNCIA DO CONSELHO DE MINISTROS

GNS Gabinete Nacional de Segurança PORTUGAL

CNCS Centro Nacional de Cibersegurança PORTUGAL

New threats from Cyberspace
Are we prepared?



National Information Security Authority
RADM António Gameiro Marques



Petr Jirasek

"Cyber security education in the age of unmanned systems"

AFCEA International
Cyber Security & IT Adviser



AFCEA International

2000 ~ 2019 Member of the Executive Committee of AFCEA International and AFCEA Vice President for Central Eastern Europe

Chairman Czech Cyber Security Working Group (AFCEA) & member of Cyber Committee AFCEA International

2018 ~ 2019 Cyber Committee Industry Liaison to ENISA Steering Committee for ECSC

https://www.linkedin.com/in/petr-jirasek-67b8344

Petr Jirasek

Mr. Petr Jirásek is a security leader and cyber evangelist. He is the author and co-author of 100+ publications, mainly in the security and IT area.

He is Master in Information technology and systems, he graduated from Defense & security master class and various course.

Mr. Jirásek is a Life member of AFCEA International.

He has been working in various positions in the private sector and on public projects as a project manager and director of ICT Department for Defense and Security, IBM Country Security Director or Public Sector Relationship. Executive.



Mark Ryland

"Cloud as na Enabler for Cyber Security"

Director Office of the CISO, Amazon Web Services



Work Experience

2011 ~ 2019 **AWS**
Director, Office of the CISO
Chief Architect, World Wide Public Sector

2008 ~ 2011 **Microsoft**
Principal Program Manager, IDAPG
National Standards Officer (USA)

2006 ~ 2008 Chief Technology Officer / Director of Engineering, Mpower Media

http://linkedin.com/in/markryland

Mark Ryland

J.D. in Law from University of California, Berkeley - School of Law

BA in Philosophy from University of San Diego

Mark works for the Chief Information Security Officer of AWS, leading a team of cloud security experts who interface with customers, partners, and internal stakeholders around security in the AWS cloud, and information security more generally.

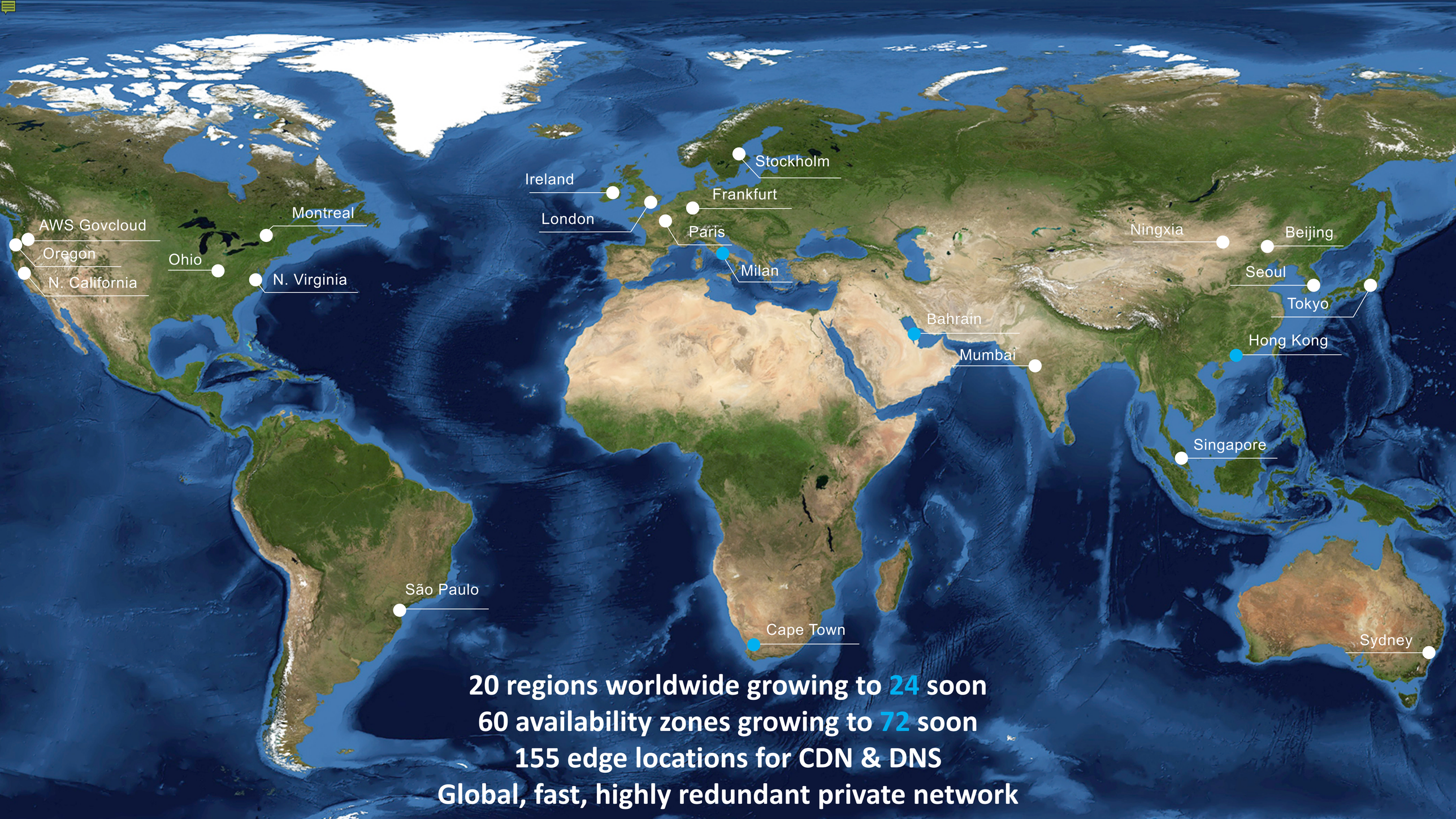
Ryland has more than 27 years of experience in the technology industry across a wide range of leadership roles in cybersecurity, software engineering, distributed systems, technical standardization, and public policy.

Cloud as an Enabler for Agility & Cyber Security

Mark Ryland

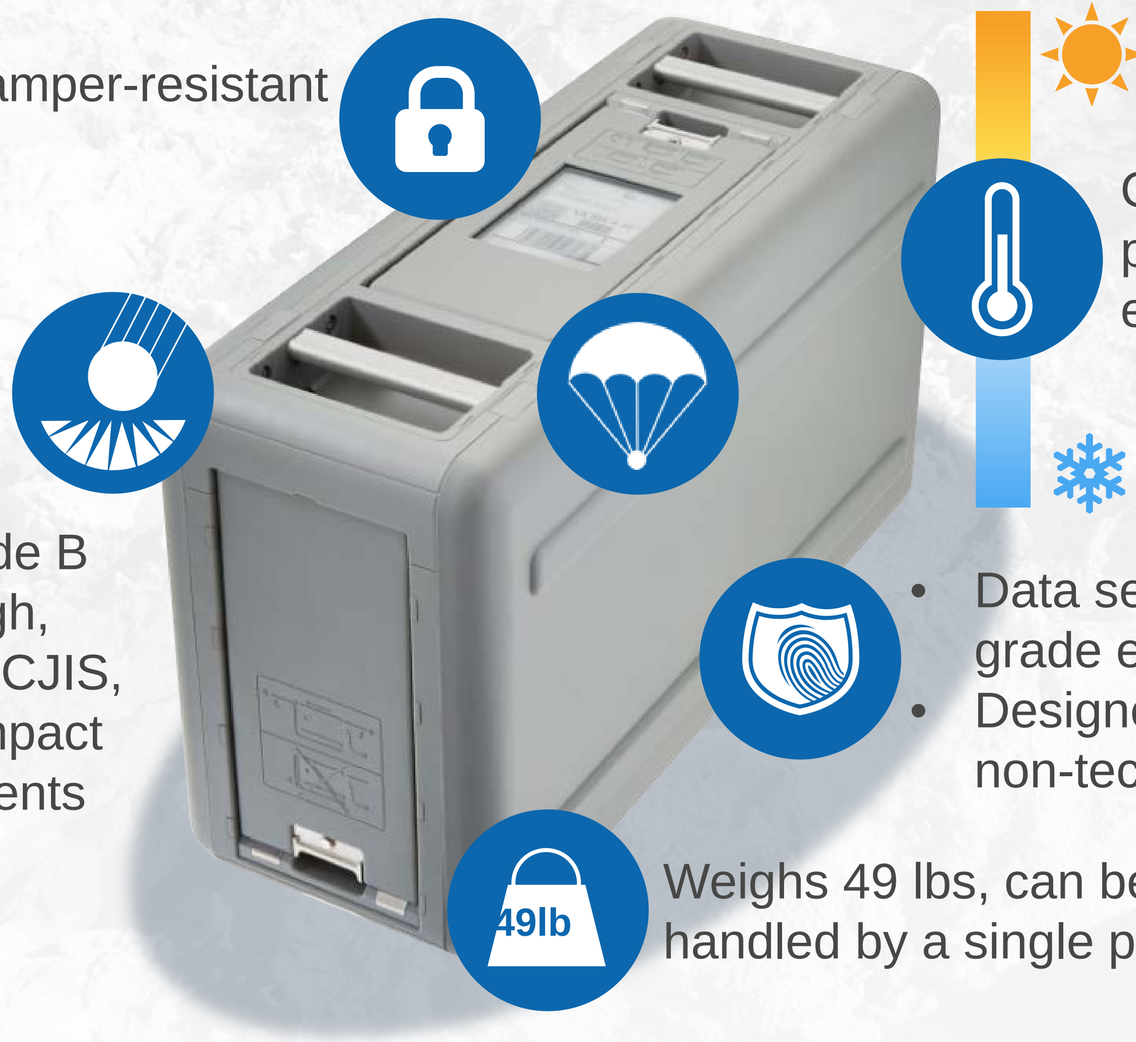
Director, Office of the CISO

Amazon Web Services


Stockholm
Ireland
Frankfurt
London
Paris
Milan
Montreal
AWS Govcloud
Oregon
Ohio
N. California
N. Virginia
Ningxia
Beijing
Seoul
Tokyo
Bahrain
Hong Kong
Mumbai
Singapore
São Paulo
Cape Town
Sydney
20 regions worldwide growing to 24 soon
60 availability zones growing to 72 soon
155 edge locations for CDN & DNS
Global, fast, highly redundant private network

AWS Snowball Edge for Defense Operations

Brings AWS to tactical field locations with no network connectivity



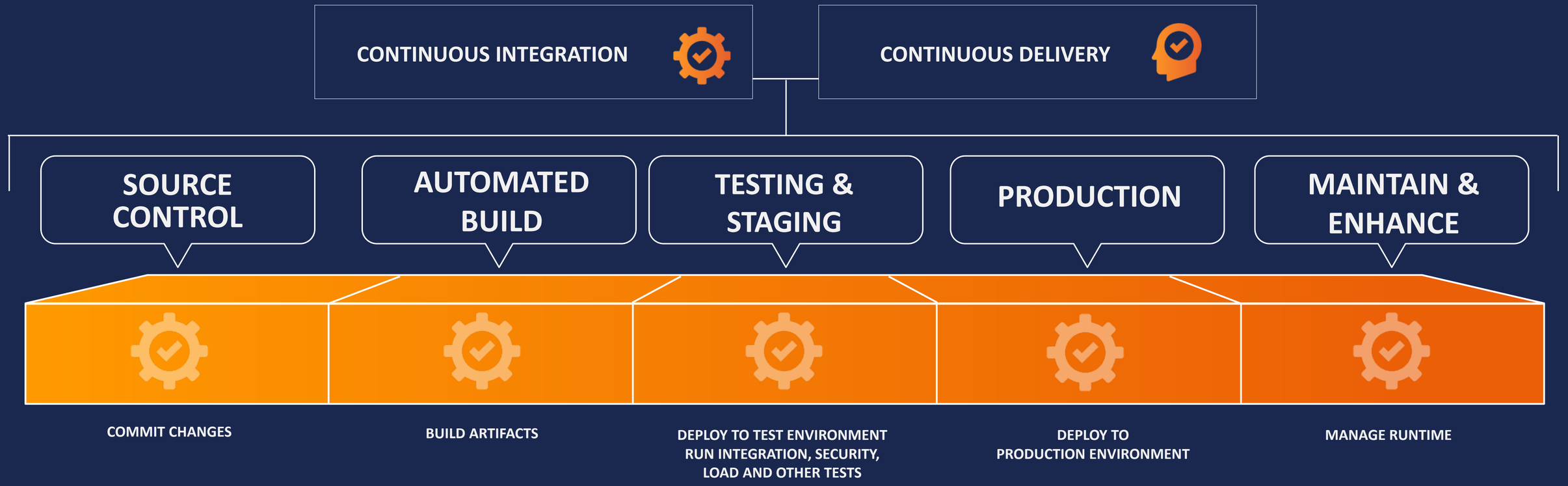
- Handles up to **200G impact**
- Airdrop-able
- MIL-S-901D Grade B
- Meets FISMA High, FedRAMP ITAR, CJIS, and DoD SRG Impact Level 6 requirements

Operates on unconditioned power and harsh environments (0° to 45°C)

- Data secured with military-grade encryption
- Designed to be operated by non-technical personnel

Weighs 49 lbs, can be handled by a single person

The changing nature of security



Secure development lifecycle applies equally to applications and **infrastructure as code**

Global MoD Use Cases in the AWS Cloud

Public-facing web applications (*e.g.*, photo services)

Service members and veteran services

Line of business applications (HR, payroll, etc.)

Geospatial data management and sharing

Development and test of major new control systems (*e.g.*, USAF GPS OCX)

AWS Snowball edge devices for data acquisition and analysis

Data science and machine learning (*e.g.*, cyber security analytics via data lakes)

Analysts desktops and “hiding in plain sight”

Brigadier General (R) Francisco Almerich

"Applications in Defense for Space Surveillance Radars (SST)"

Senior consultant for Defense Systems



Work Experience

2017 ~ 2019	Retired from the Spanish Air Force and joined the Company Indra Sistemas SA as senior consultant for Defense Systems
2015 ~ 2016	took part to trigger the Space Surveillance capability at the Spanish Air Force
2012 ~ 2016	Commander of the Spanish Air Force Command and Control System (JSMC).

Francisco M. Almerich Simó

Graduated from the Spanish Air Force Academy in 1982, and later attended the Telecommunications course (Command & Control School).

He's got the Staff Course (Spanish Air Force War College), a Master degree in Security and Defence Policy (Complutense University of Madrid) and a diploma in High International Studies (Society of International Studies, Madrid).

During his 34 years of active-duty, Brigadier General Almerich's career combined planning, procurement, management, and operational assignments. He is intimately acquainted with national and international defense, armaments and procurement issues. BG Almerich has in-depth knowledge of Air Command and Control Systems

indra

MILTEC 19
International Conference

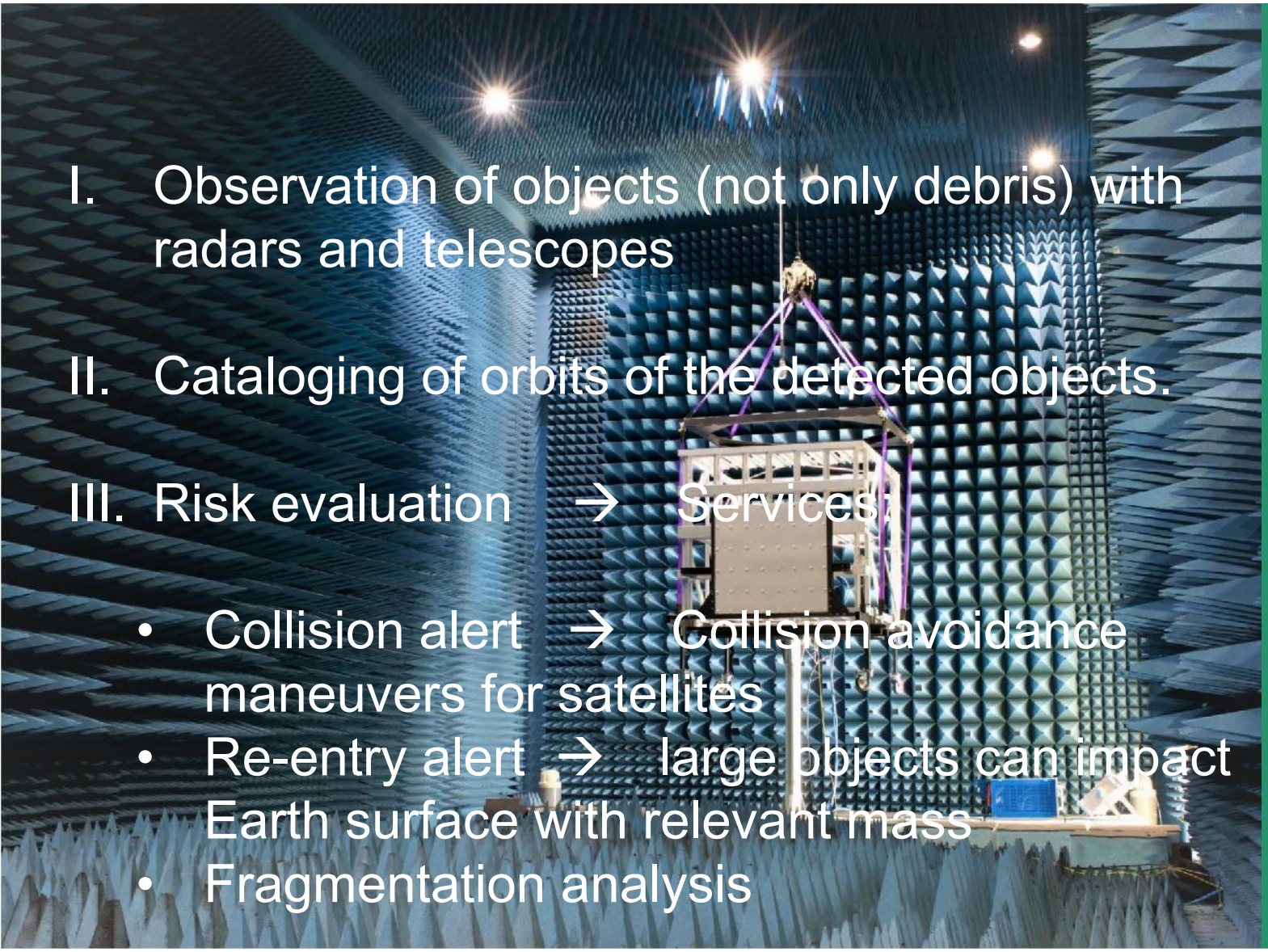
"Applications in Defense for Space Surveillance Radars (SST)"

Envisioning a safer tomorrow



Francisco M. Almerich – Brig. Gral. (R) Spanish Air Force

February, 21 / 2019
Lisbon, Instituto Universitário Militar (IUM)



Functions of SST System

I. Observation of objects (not only debris) with radars and telescopes

II. Cataloging of orbits of the detected objects.

III. Risk evaluation → Services:

- Collision alert → Collision avoidance maneuvers for satellites
- Re-entry alert → large objects can impact Earth surface with relevant mass
- Fragmentation analysis

Radar is the most important sensor to detect objects in the LEO orbit (200 to 2000 Km)



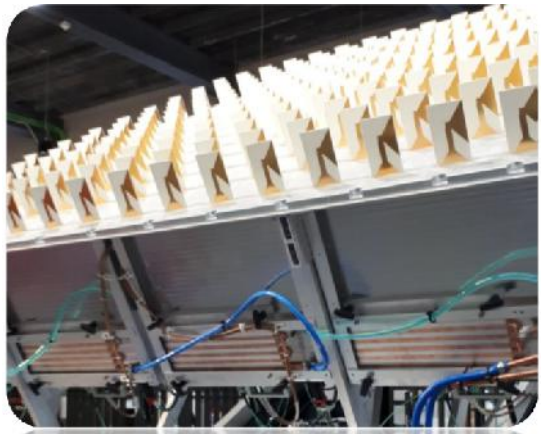
- S3TSR is a radar system developed by Indra, funded by Spanish Administration (CDTI)
- Technically managed by ESA

Spanish Space Surveillance & Tracking Surveillance Radar (S3TSR)

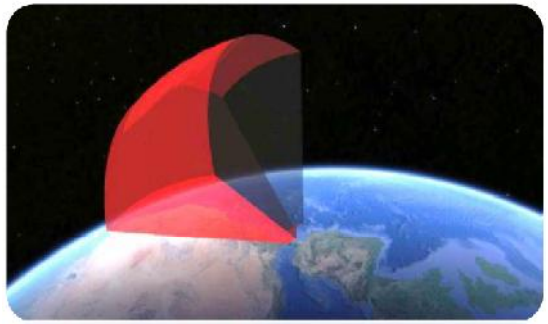
S3TSR (First versión)
Morón AB
(November 2018)

S3TSR

- AESA L band radar
- Ground-based radar, based in close monostatic configuration
- Automatic surveillance and tracking of space objects in Low Earth Orbit (from 200 to 2000 Km.)
- Continuously scanning the instrumented FoR,
- Tracks are sent to the Space Surveillance and Tracking Operation Center to generate/maintain a Catalogue
- High power amplifier modules based in GaN (Gallium Nitride tech.)
- The RX Antenna uses a full digital beamforming over optical fiber.



Rx Antenna Subsystem



Field of Regard (FoR)

Ronald Westerlaken

"Best practices with SINA for multinational commands and mission networks"

International Sales Director
secunet Security Networks AG



Work Experience

2015 ~ 2019 Sales Director (International Sales)

2009 ~ 2015 IT Security Consultant & Business Line Manager, Fox IT

2004 ~ 2009 PhD Researcher, Delft University of Technology

https://nl.linkedin.com/in/ronaldwesterlaken

Ronald Westerlaken

After graduation at the University of Technology in Delft worked for 6 year in the Crypto department of Fox.

Last 2 years as business line manager for the development of the high assurance product SINA RedFox .

In 2015 switched to secunet and being responsible for international relationships/sales.

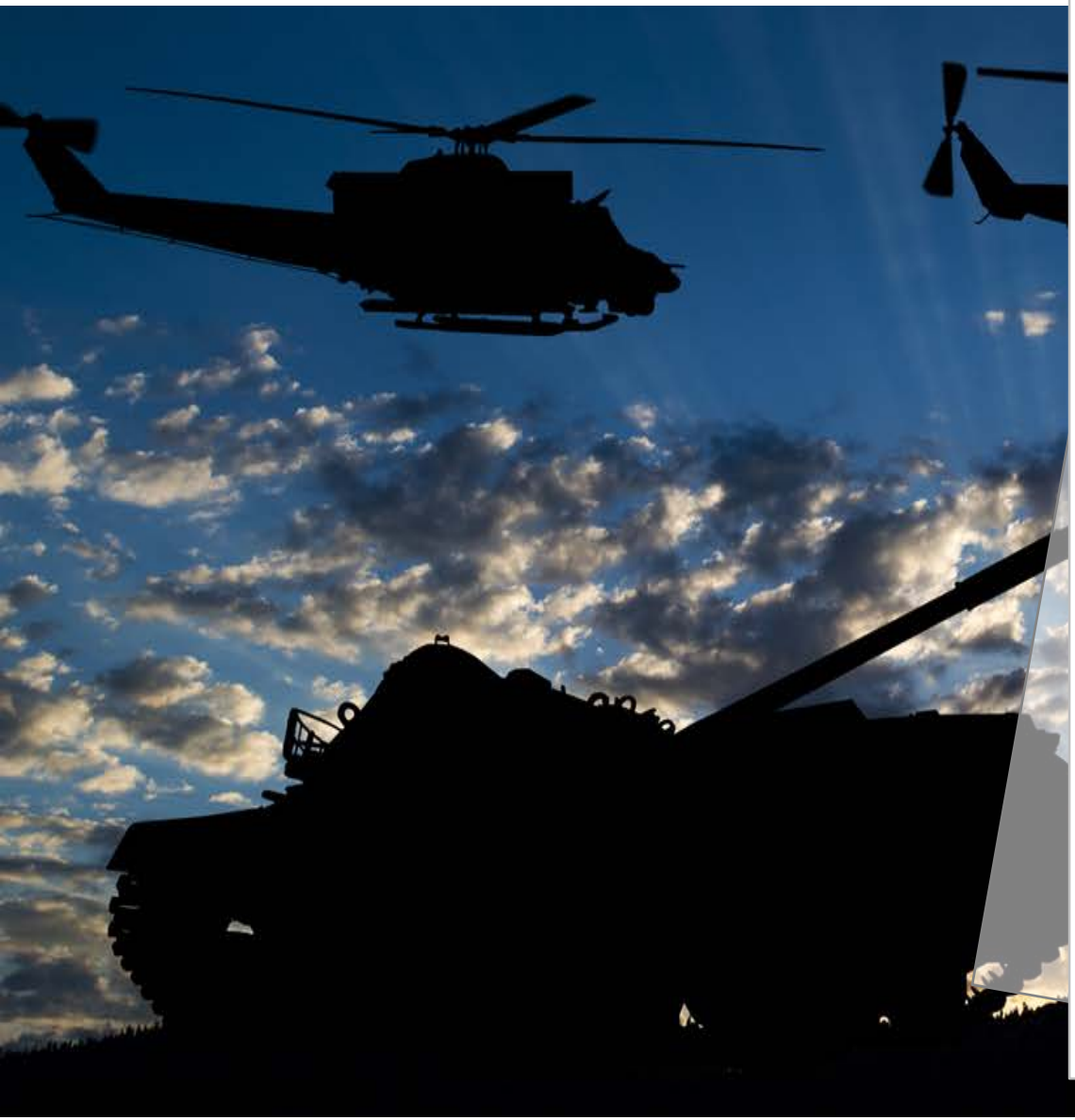
secunet

secunet

Best practices with SINA for multinational commandos and mission networks

MILTEC 2019 | February 21 2019

Executive Summary



- secunet is a reliable European partner in the field of crypto technology
- With long-term experience in
  - sensitive environments
  - multinational projects
  - cooperation with various integration partners, e.g. Orange, Airbus, T-Systems, Atos, GMV
  - designing security architectures
  - almost all areas of EU-institutions and -activities
- One of the few suppliers for crypto technology with approvals up to VS-GEHEIM, NATO SECRET, UE SECRET
- secunet's SINA technology has been appointed (in 2018) the main crypto architecture for the German Armed Forces

SINA – most successful crypto security solution Made in Germany

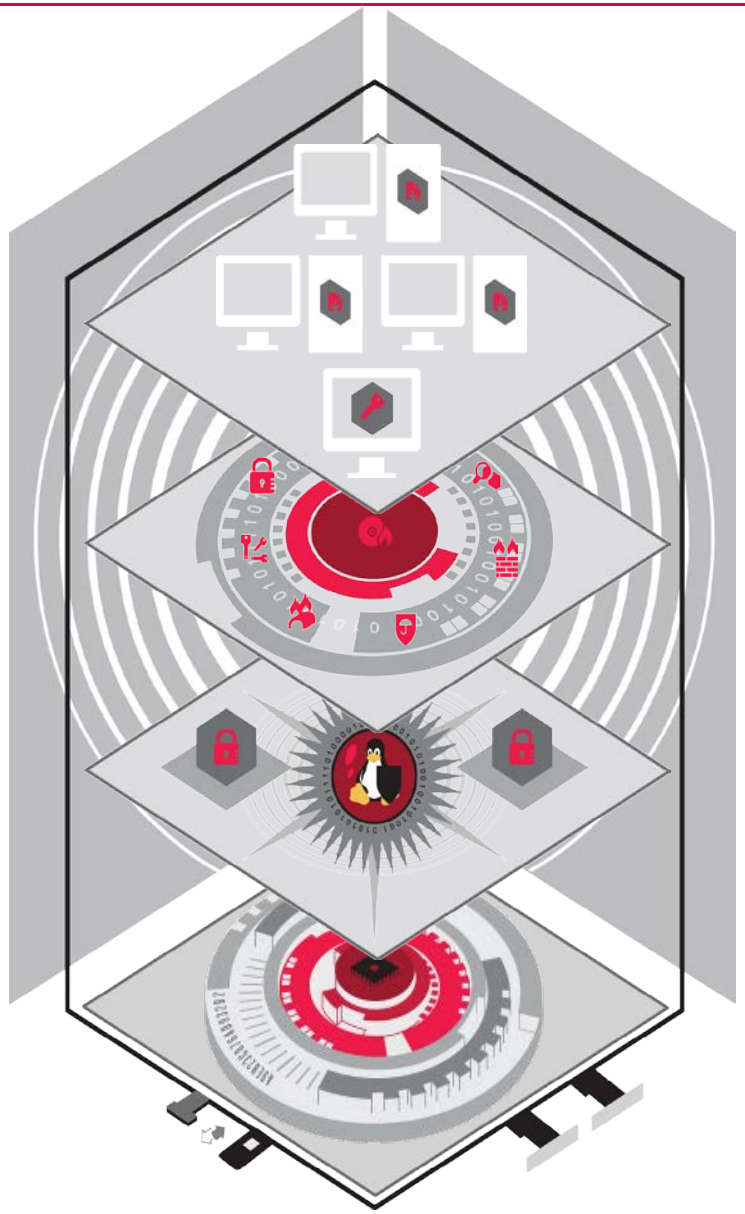
- Processing, storage, transfer and full audit trail of classified information

Bundesministerium des Innern

- Most secure mobile workstations in the world incl. ultra-mobile solutions
- Scalable solutions designed for complex national and international infrastructures
- Central administration capability; suitable for mass roll-outs
- Extensive product range – from tablets and crypto gateways to servers
- More than 100,000 instalations in Germany and more than 24 countries



The Architecture - Multiple Levels of Security



- **Applications and Guest Operating Systems**
  Multi data separation and multi level sessions of varied classification, (virtualisation via Oracle Virtual Machine VBox)
- **IT-Security Functions**
  Multistate supplementary security features
- **Secure System Platform (SINA OS)**
  Minimized, hardened and intensely evaluated
- **Hardware and Firmware (SINA BIOS)**
  Including smartcards and crypto modules dimensioned and configured according to approval standard

secunet

2000 2005 2010 2015 FUTURE

SINA E/H milestones

2019 First GBit IPsec Gateway for GEHEIM (SECRET DEU)

2016 First ethernet encryptor for GEHEIM (SECRET DEU)

2015 ff. SINA Workstation H Client III for HaCCIS (HaFIS)

2014 High international approvals; european crypto cooperation

2012 ff. SINA (Virtual) Workstation in Afghanistan

2009 First SINA (Virtual) Workstation H approved for GEHEIM (SECRET DEU)

2008 ff. SINA Infrastructure project ESA (German Armed Forces)

2005 ff. Roll-out thousands of SINA H components in FüInfoSys (C4I)

2004 SINA H „Blueprint“ for FüInfoSys SK (CCIS)

2003 First (PEPP-based) SINA H products

2000 Start of the initial secunet/BSI development project

1999 Basic SINA concept of the Federal Department of Information Security (BSI)



Bundesamt für Sicherheit in der Informationstechnik

Bundesministerium der Verteidigung



Session 3

The technological response: emerging technologies

altice AIRBUS DEFENCE & SPACE aws indra Microsoft secunet THALES EDISOFT DEFENCE & AEROSPACE



Dr. Michael Street

"How Data Science is changing NATO"

Head of Innovation & Data Science



Work Experience

2013 ~ 2019 Head, Innovation and Data Science at the NCIA.

2008 ~ 2013 Principal Scientist (CIS), Chief Technology Office, NATO C3 Agency (NC3A). Responsible for technology direction and coherence, and system acquisition.

1999 ~ 2009 Technical lead and Project Manager at NC3A for technology projects ranging from R&D to in-theatre deployments.

https://nl.linkedin.com/in/michael-street-1959721

Michael Street

Michael Street leads NCIA's Data Science Team, applying innovative approaches and data science technology (big data and machine learning) to extract value and insight from data for users across NATO.

He also leads the Agency's innovation activities where he is responsible for the identification, assessment and introduction of innovative and disruptive technologies.

Michael holds a B.Eng in computer systems, an M.Eng in satellite communications. His PhD in radio system automation *influenced* STANAG 4538.

He is a Fellow of the Institution of Engineering and Technology, was awarded the Sir Henry Royce Memorial Foundation's medal for engineering achievement and has authored over 40 scientific papers.

NCI AGENCY



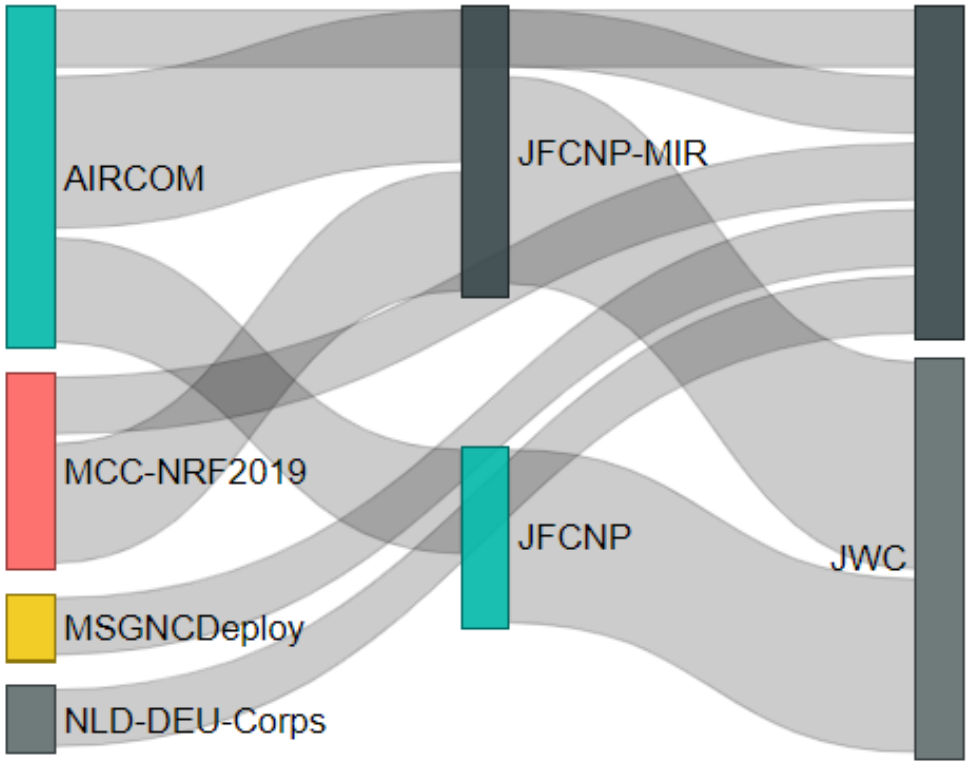
Better decisions, faster

How data science is changing NATO

Service Strategy & Innovation

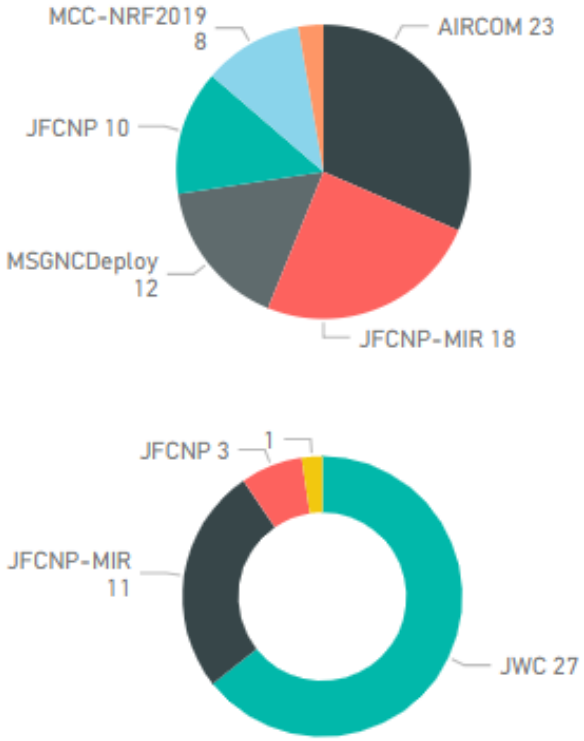
Dr Michael Street

TRJE18: Intel flows

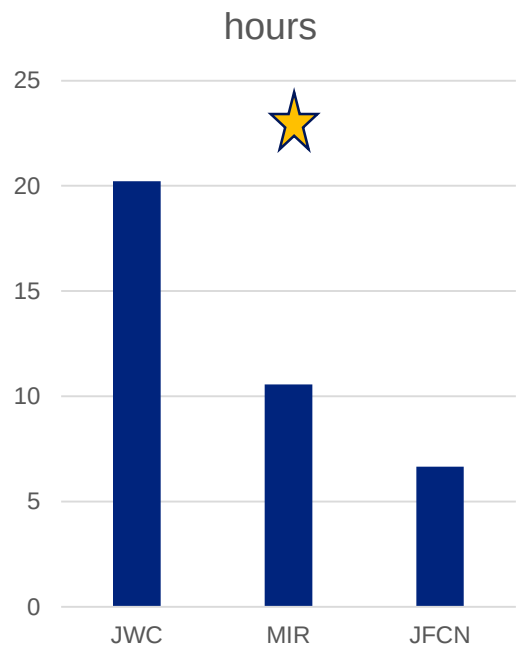


Requests

Responses



Requestors
&
Responders



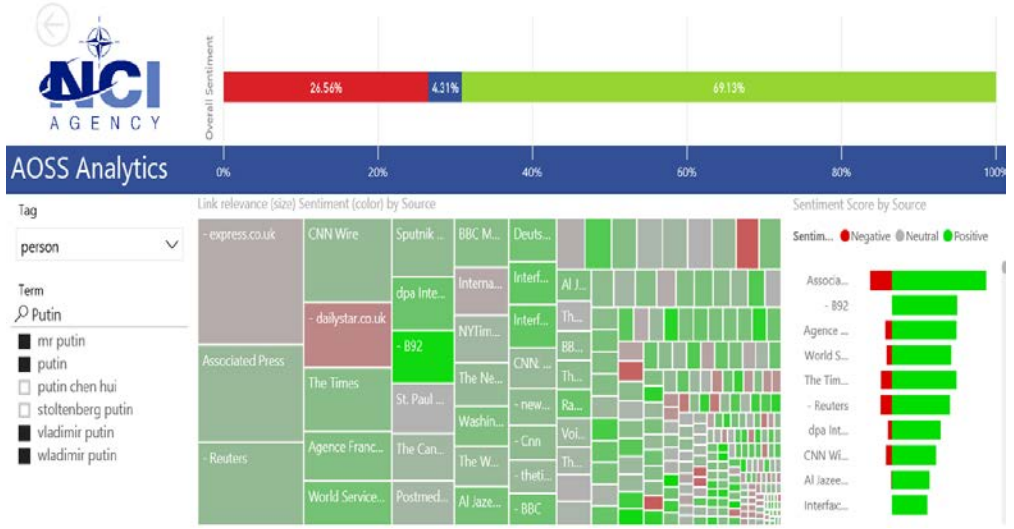
Response times

Immediate

V.1.0

Summary

- NCIA has expertise and capability
  - Supporting users across NATO
  - Working with industry and Nations



- Data collection becomes routine
  - A reference point for improvements fielded in the next exercise
  - Exploit data with advanced analytics and machine learning

- Understand and prepare for the security threats of AI and big data

V.1.0



For more information:

NATO Communications and Information Agency

PO Box 174, 2501CD The Hague, The Netherlands

Dr Michael Street

Head, Data Science and Innovation

T: +31 70 374 3444

E: michael.street@ncia.nato.int

Gabriele Rizzo

"Towards a Fourth Offset Strategy: maintaining the edge in hyperwar and hypercontested domains"

Leonardo & Sapienza University of Rome



Work Experience

2016 ~ 2019	Lead Futurist & Lead Scientist, Strategic Innovation, Leonardo
2017 ~ 2019	Member of the Board of Experts, Member of the Research Board, Professor of Strategy
2013 ~ 2016	Military Research Scientist & Senior Scientist, Leonardo
2008 ~ 2013	Optronics, Avionics, Radar and advanced targeting, Advanced optics Engineering staff, Leonardo

https://it.linkedin.com/in/gabrielerizzo

Prof. Dr. Gabriele Rizzo

Gabriele Rizzo is a visionary futurist and an enthusiastic innovator. Currently Lead Scientist, Strategic Innovation in Leonardo, futurist advisor in NATO, Member at Large for Strategic Foresight, and NATO expert for Cyberspace and Cyber Defence.

He held multiple position over 10 years in Engineering staff before moving to Strategy, where he contributed substantially, as lead author and even demiurge, to strategic visions and long-term thinking of Italy, Europe, NATO, strategic advisory firms, large industries and international organizations.

He also teaches Strategy and Defence of Cyberspace at Sapienza University of Rome. He has more than 40 publications to his credit, authored several capstone works on deep futures and was honored with national and international awards.

SAPIENZA UNIVERSITÀ DI ROMA

LEONARDO

Towards a Fourth Offset Strategy

Maintaining the edge in hyperwar and hypercontested domains

Gabriele Rizzo

MILTEC19: The Changing Face of Warfare, from Cyber to Unmanned Systems

– Instituto Universitário Militar, Lisboa, 21 February 2019

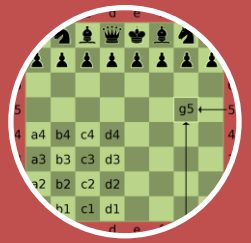


LEONARDO

1948 • 2018

Hyperbolic Warfare, or Hyperwar

AI-fueled, machine-waged conflict – a type of conflict where human decision making is almost entirely absent from the OODA loop.



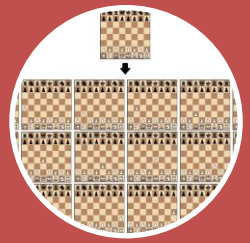
Infinite, distributed Command & Control capacity



Concurrency of action and perfect coordination



Logistical simplification



Instant mission adaptation

near-instantaneous responses

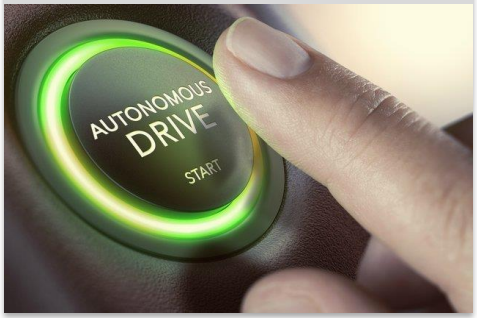
© Leonardo - Società per azioni

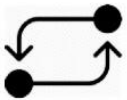
Four Centaur Intelligence Scenarios



Pass the baton

- It’s your turn now

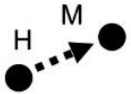




Symbiosis

- One can’t live without the other

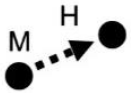




Take me to the next level

- Train me
- Show me the possibilities





Go the last mile

- Human in the loop



© Leonardo - Società per azioni

Want more?





© Leonardo - Società per azioni

Conclusions

- Disorganic disruptions ahead – impact of hyperwar
- Need to preserve the right side of the offset
- Cues to ignite your long term thinking
- Not adaptation, but Transformation

© Leonardo - Società per azioni

THANK **YOU** FOR YOUR ATTENTION

Dr Gabriele Rizzo gabriele.rizzo@leonardocompany.com

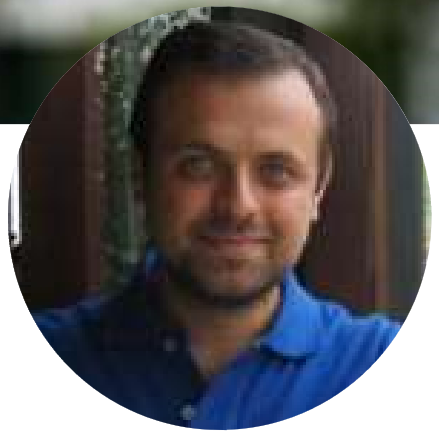
LEONARDO



Yasser Omar

"Quantum Technologies as Sovereignty Technologies"

Physics of Information and Quantum Technologies



Work Experience

Coordinator, *Physics of Information and Quantum Technologies Group*, Instituto de Telecomunicações

Associate Professor, Department of Mathematics, Instituto Superior Técnico (IST), University of Lisbon

Director, Doctoral Programme in the Physics and Mathematics of Information, IST, University of Lisbon

http://www.phys-info.org/yasser-omar.html

Yasser Omar

Fulbright Scholar, Massachusetts Institute of Technology (USA).

Ph.D. in Physics, University of Oxford (UK).

Technological Physics Engineering Degree, Instituto Superior Técnico.

His research work focuses on quantum information theory, quantum computing, quantum communications, and quantum sensors.

Since the founding of his Group in 2013, he has obtained six European research projects. The two most recent are related to the quantum internet and the quantum radar, both started in October 2018 under the new program of the European Commission *Flagship in Quantum Technologies*.

TÉCNICO LISBOA

Quantum Technologies as Sovereignty Technologies

Yasser Omar

yasser.omar@tecnico.ulisboa.pt

Physics of Information and Quantum Technologies Group, IT and Instituto Superior Técnico, University of Lisbon



TÉCNICO LISBOA



instituto de telecomunicações

Quantum Technologies

We want to develop and commercialize:

- **Quantum computation and simulation**
  for faster information processing
- **Quantum communications**
  for enhanced privacy
- **Quantum sensing and metrology**
  with enhanced precision

Require a lot of enabling sciences and technologies:
classical and quantum control, engineering, fabrication, …

Conclusions

Information is physical!

Quantum Technologies hold the promise for new and disruptive information technologies, exploring quantum science and engineering to attain:

- the ultimate levels of privacy in telecommunications,
- the ultimate levels of speed in computation,
- the ult. levels of precision in sensing and metrology.

There is still a lot to understand, to test & to build...

... and we can contribute significantly to this scientific and technological revolution!

Stephane Alestra

"Massive Intelligence solution for Defence & Security at AIRBUS DS"

Senior Marketing Manager



Work Experience

2018~ 2019	Senior Marketing Manager Massive Intelligence
	Airbus Defence and Space - Intelligence
2002 ~ 2018	Head of Customer Applications at DATADVANCE (Datadvance & Airbus Group)

https://fr.linkedin.com/in/stephane-alestra-612079171

Stephane Alestra

Dr in Mathematics, Inverse Problem, Optimization, Numerical Simulation, Université Paris Nord- Paris 13.

Master Numerical Analysis, Mathematics Simulation, Université Paris 13 Ecole Polytechnique

AIRBUS DEFENCE & SPACE



Massive Intelligence solution for Defence & Security AIRBUS DS

MILTEC 19

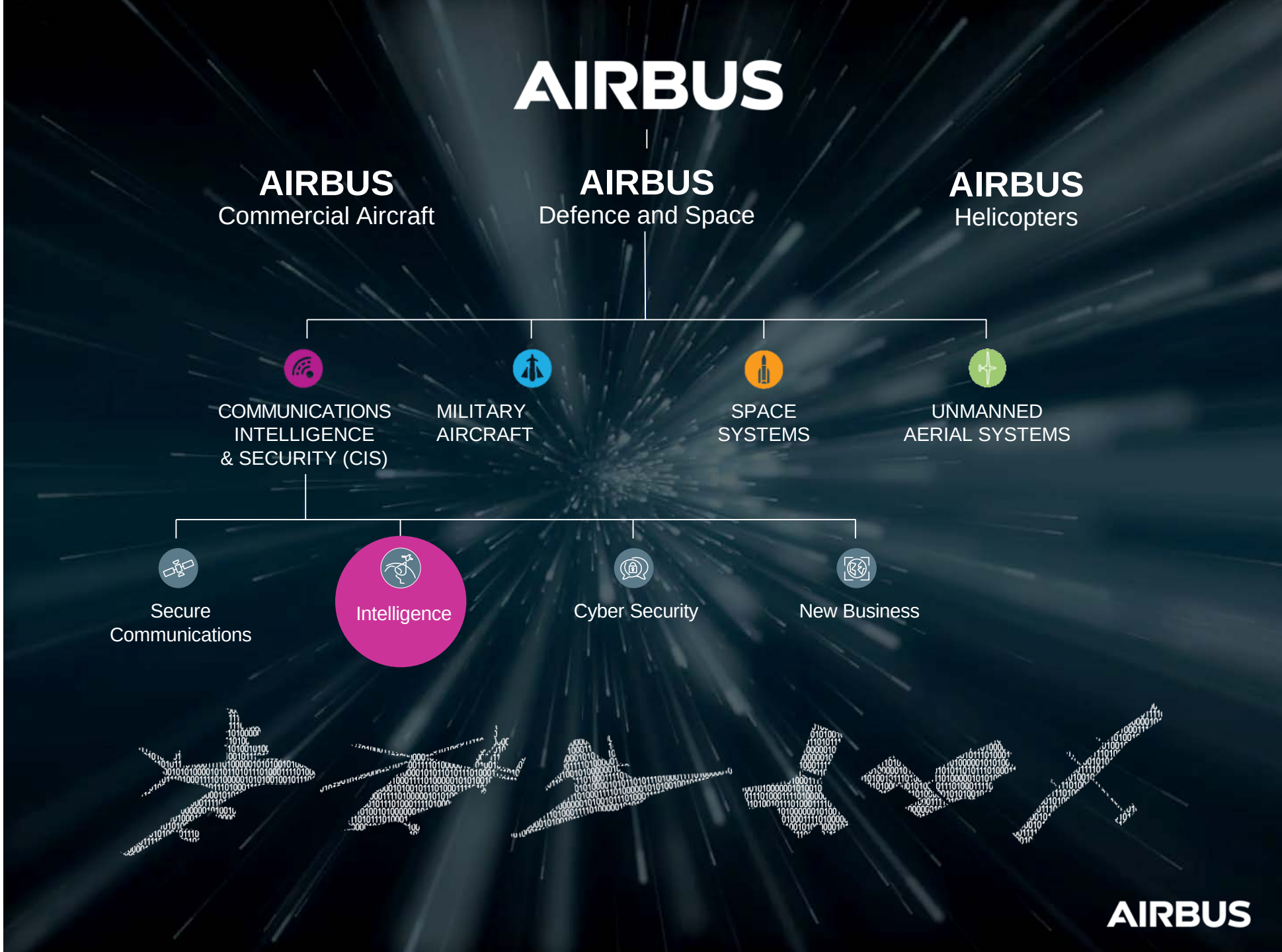
DEFENCE AND SPACE

February 2019

AIRBUS

Intelligence Positioning within **AIRBUS**

The **Power** of **AIRBUS**



MASSIVE INTELLIGENCE ADDED VALUE TO MULTI INT



BIG DATA

MASSIVE INTELLIGENCE

PREDICTIVE ANALYSIS

AUTOMATION

MULTI-INT

Multi-Sources Intelligence

FORTION family
I4D
ONE ATLAS

ARTIFICIAL INTELLIGENCE

ANALYTICS

CLOUD INFRA
DIGITAL SERVICES

AIRBUS

Massive Intelligence Solution adapted to your needs

DEFENCE

SECURITY

INTERNATIONAL ORGANISATIONS

HOME COUNTRIES & EXPORT/NEW MARKETS

Use cases

Conflict and crisis monitoring

Defence & Military Intelligence

Natural disaster monitoring & response

Critical Infrastructure

Radicalisation & terrorism threats

Police Missions

Maritime Intelligence Centers



MASSIVE INTELLIGENCE

Key Differentiators & Benefits

Key features

- AIRBUS Satellites & UAV
- AIRBUS Multi Intelligence Sources & Fusion
- Automatic processing & analytics & Artificial Intelligence
- Big Data capacities

Key benefits

- Reduce analysis time
- Early Detection, Prediction, Alerts
- Breaking silos
- Flexibility : Applications, Business models, Proof Concept

..



Session 4

The technological response: the weapons of the future

altice AIRBUS DEFENCE & SPACE aws indra Microsoft secunet THALES EDISOFT DEFENCE & AEROSPACE



Victor Lobo

"The challenges of Unmanned Systems in future warfare"

Director of the Naval Research Center



Work Experience

Visiting professor at the San Diego State University, at the French Naval Academy and at the Lisbon ISCTE

Professor at the Portuguse Naval Academy and New Univeristy of Lisbon (NOVA)

Director of the Naval Research Center of the Navy

Victor Lobo

Degree in Electrical Engineering, Instituto Superior Técnico (IST), Lisbon

Master and PhD in Computer Science, Faculdade de Ciências e Tecnologia (FCT), Lisbon

Habilitation (Agregação) in Information Management by the Higher Institute of Statistics and Information Management of the New University of Lisbon.

Represents the Ministry of Defense in NATO and in EDA R&D groups

http://www.novaims.unl.pt/magic/index.php/component/k2/item/192-vitor-jose-lobo.html



The challenges of Unmanned Systems in future warfare

Marinha

Victor Lobo, February 2019

Challenges – Ethical/Legal/Economic

Strong dependence on how society accepts Unmanned Systems in general





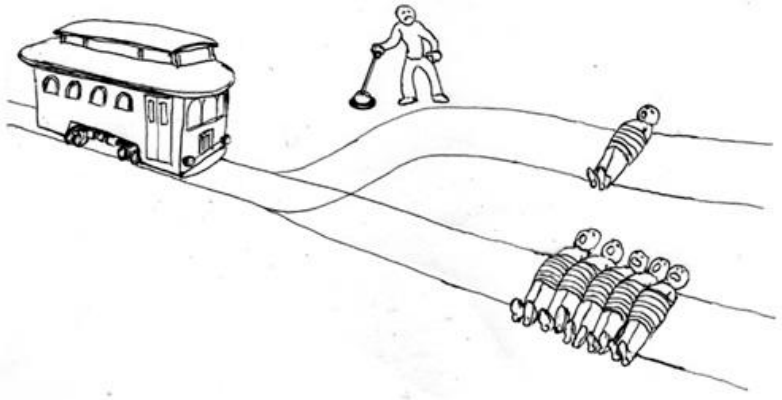
- Economic issues
  - Sharp drop in cost
  - Standards, Mass production

  Military implications: widespread use

- Legal issues
  - Fast progress or…Overrun by reality !

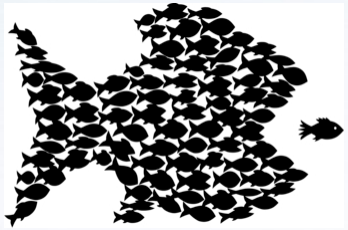
  Military implications: more choice, less restrictions

- Ethical issues
  - Advances in “artificial ethics”
  - Criteria: “Better than manned”
  - Variants of the Trolley Problem



Challenges - other issues

True **Swarm** Behaviours
- Beyond scripted interactions





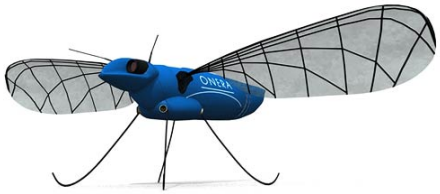
Biomimetic systems
- Multi-legged, flapping wings, crawling, etc



NBQR ready systems
- Developments due to Fukunaga



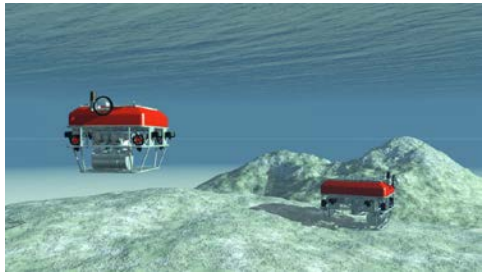
Maintenance and **Self-healing** systems
- Enhance survivability



Deepsea, nearspace, polar, desert/swamp/mountain systems
- Too hostile for man



Cyberwarfare
- Cyberdefence by design
- Two routs to attack cyberphysical systems !



What is CINAV (Naval Research Center) doing about it ?

Cooperating with Universities and Enterprises in National and International research programs

Gaining experience and knowledge in key areas

Talant de bien faire



Research and Development

in search of excellence with Universities and Industry

Fulfilling the Navy's Mission in the service of our Nation

Luís Amaral Arsénio

"Exploiting disruptive innovation in defence"

National Defence R&D Representative



Work Experience

2016 ~ 2019 R&D Representative of the MoD; National Coordinator for NATO Science and Technology and in "AS-IF" Committee on European Defence Research Programme

2011 ~ 2016 Navy staff officer, dealing with the navy's organizational transformation program

1994 ~ 2010 Served in naval missions & headquarters

Luís Filipe do Amaral Arsénio

Naval Military Sciences degree, in the area of Naval Engineering, Weapons and Electronics Branch, Naval School, Lisbon

In 2014, obtained a Master of Arts on Peace and War Studies with a dissertation thesis in the maritime security field.

Currently, he is developing a PhD thesis focused on disruptive innovation in Defence

REPÚBLICA PORTUGUESA
DEFESA NACIONAL

REPÚBLICA PORTUGUESA

DEFESA NACIONAL

Exploiting disruptive innovation in defence

MILTEC 19

CDR Luís Arsénio

21FEB19

Research and experimental development (R&D) comprise creative work undertaken on a systematic basis in order to increase the stock of knowledge, (…) and the use of this stock of knowledge to devise new applications

The term R&D covers three functional activities: basic research, applied research and experimental development

(Frascati Manual, 2002: 30)

Robotics in defence

a disruptive role in military operations (…) to change the way military operations are conducted in the future, and even to make it possible to envisage new type of missions

SPIDER project - *Sensor Platform & Network for indoor deployment and exterior-based radiofrequency awareness - provide a proof of concept for an innovative system to improve the soldier's inside-building awareness through the support of mobile robots*

(Marco Detratti, 2017, "10 Upcoming Disruptive Defence Innovations", European Defence Matters)

REPÚBLICA PORTUGUESA
DEFESA NACIONAL

Autonomy in defence: systems, weapons, decision-making

future unmanned systems will see higher degrees of autonomy provided inter alia by Artificial Intelligence (AI) or cognitive computing

(Marek Kalbarczyk, 2017, "10 Upcoming Disruptive Defence Innovations", European Defence Matters)

REPÚBLICA PORTUGUESA
DEFESA NACIONAL

Future advanced materials for defence applications

the potential to significantly shape future operational effectiveness in military missions (…) The most disruptive effects are expected to derive from the integration of functionalities such as energy harvesting, camouflage, structural and personnel health monitoring, protection in 'super-intelligent' materials for platforms and soldiers

(Patricia Lopez Vicente, 2017, "10 Upcoming Disruptive Defence Innovations", European Defence Matters)

CHALLENGES

REPÚBLICA PORTUGUESA
DEFESA NACIONAL

- Always engage the Armed Forces
- Prevent technology transfer problems
- To have a clear definition about what to develop (identify gaps)
- Lessons learned
- To join efforts (cooperation)
- Launching challenges targeting current priorities
- Promote prototyping and technology demos (Demand for higher TRL)
- To map changes in the technology landscape through horizon scanning and technology watch activities
- Linking scientists and military operators
- Additional funding instruments (EDF)

Inês Ferreira

"The new technological weapons for a safer world"

Internet of Things Product Owner



Work Experience

2013 ~ 2019	Responsible for Internet of Things portfolio development at PT Empresas
2008 ~ 2012	Project management of Analytics and Big Data projects
2003 ~ 2008	Business Intelligence projects
1998 ~ 2003	Responsible for Prepaid Product Management, in TMN

Inês Ferreira

Degree in Economics, Universidade Nova de Lisboa.

MBA from Universidade Católica de Lisboa.

Inês Ferreira is presently responsible for Internet of Things portfolio development at PT Empresas, Altice Portugal's Business to Business brand.

She believes in the revolutionary power of ICT (Information and Communication Technologies) to create a more efficient, inclusive and happy world.

altice



THE NEW THECHNOLOGICAL WEAPONS FOR A SAFER WORLD

INÊS FERREIRA

FEBRUARY 2019

UMA REDE DE POSSIBILIDADES

This document is the intellectual property of Altice Portugal, and its use and disclosure is strictly prohibited without express authorization.

PT EMPRESAS

DIGITAL TRANSFORMATION PARTNER



- Digital Business Strategy
- Processes Innovation
- Technological Efficiency & Flexibility
- Online, Smart Costumer Engagement

HOLISTIC APPROCH TO ORGANIZATIONAL SAFETY

CYBER SECURITY

COMMUNICATION NETWORK



IT & CLOUD INFRASTRUCTURE



PHYSICAL SECURITY

ASSETS | PEOPLE | SPACES



IT & CLOUD INFRASTRUCTURE

SOC (SECURITY OPERATIONS CENTER)

PT Empresas

HOW THE SERVICE WORKS

- CONTINUOUS MONITORING OF NETWORK AND IT INFRASTRUCTURE
- DETECTION AND REACTION TO SECURITY INCIDENTS
- SIEM PLATAFORM AND COLLABORATION WITH SECURITY PARTNERS (ALTICE PORTUGAL IS MEMBER OF ONE OF THE BIGGEST CYBER SECURITY NETWORK: TF - CSIRT / TRUSTED INTRODUCER)

24x7x365 - MONITORING

SOC

Alarm Management	SIEM
Incident Response	Reporting



ADVANTAGES

- NATIVE CAPABILITY TO MONITOR 70% OF PORTUGUESE INTERNATIONAL TRAFFIC, CROSSING ALTICE NETWORK
- HIGHLY SKILLED AND EXPERIENT SECURITY EXPERT TEAM
- WORLDWIDE ORGANISATION FOR SECURITY INCIDENTS RESPONSE – CSIRT /TRUSTED INTRODUCER

IT & CLOUD INFRASTRUCTURE
DISASTER RECOVERY

PT Empresas

HOW THE SERVICE WORKS

- DATA REPLICATION AND INFRASTRUCTURE RECOVERY
- RECOVERY PLAN ACCORDING TO PREFERENCES – VIRTUAL MACHINES, ORDER AND REPOSITION TIMES
- FAILOVER AND FALLBACK BASED ON MAIN AND SECUNDARY SITES SELECTED



DID YOU KNOW?

25% OF COMPANIES DO NOT REOPEN AFTER A DISASTER.

ADVANTAGES

- RECOVERY AVAILABLE BOTH FOR DATA CENTER OR CLOUD BASED DATA
- BUSINESS CONTINUITY IN CASE OF DISASTER
- AGILITY TO COPE WITH BUSINESS CHANGES ON REAL TIME VIA WEB PORTAL

ASSETS & PEOPLE
VIDEO SURVEILLANCE

PT Empresas

HOW THE SERVICE WORKS

- HIGH QUALITY IMAGE RECORDING AND STORAGE
- VIDEO ANALYTICS
- ACCESS VIA WEB PORTAL OR APP
- SOLUTION INCLUDING EQUIPMENT, CONNECTIVITY AND PLATFORM

VIDEO ANALYTICS PATTERNS EXAMPLES

Intrusion	Crowd estimation
Wander	Object counting
Tripwire	Speed detection
Abandoned object	Abnormal behavior
Removed object	Fallen people



ADVANTAGES

- AUTOMATIC DETECTION OF SECURITY FALTS
- COMPATIBILITY WITH LEGACY SOLUTIONS AND CAMERAS
- ANALYTIC SCENARIOS CAN BE ADAPTED TO SPECIFIC NEEDS



Closing Session



MILTEC 19

The changing of warfare:
from cyber to unmanned systems

Military University Institute
February 21, 2019