

HYBRID CYBER WARFARE AND THE EVOLUTION OF AEROSPACE POWER: risks and opportunities



i Quaderni del CESMA

GRUPPO DI LAVORO CESMA “HYBRID CYBER WARFARE”



With the support of





HYBRID CYBER WARFARE AND THE EVOLUTION OF AEROSPACE POWER: risks and opportunities

by
CESMA Working Group on Hybrid Threats

Foreword by
Professor Umberto Gori
President of CSSII and Director of ISPRI

CESMA

“HYBRID CYBER WARFARE AND THE EVOLUTION OF AEROSPACE POWER: risks and opportunities”

Edited by Giuseppe G. Zorzino

Copy-editing: Giuseppe G. Zorzino

Graphics and cover design by Sara Zorzino

ISBN: 978-88-941313-1-4

The views expressed in this CESMA Paper are the responsibility of the authors and do not necessarily reflect the opinion of the CESMA, the Associazione Arma Aeronautica or any of the institutions and companies represented by the contributors.

CESMA is the acronym of Centro Studi Militari Aeronautici “Giulio Douhet”, a nonprofit Think Tank of the Italian Air Force Association.

His mission is:

- to contribute to the diffusion of the Aerospace and Defence culture in Aerospace and Defence, both within Italy and internationally;
- to make studies, exchange ideas and discuss the trends of Defence and Aerospace, making a common space available to all Stakeholders (Air Force, Civil Aviation, Italian Space Agency, Air Component of the other Armed Forces, Industry, Academia, International and European Organizations).

His vision is to be widely recognized, at the European and International level, as value providers for all the stakeholders and for the Italian nation.

CESMA has organized and organize several workshops and lectures on UAVs, Space, History of the Italian Air Force, Military Ethics, Cyber, etc.

Portions of this CESMA Paper may be quoted or reprinted without special permission for academic purposes, provided that a standard source credit line is included.

© Associazione Arma Aeronautica 2017 all right reserved

Limited copies of this CESMA paper are available and may be obtained directly from
Centro Studi Militari Aeronautici “Giulio Douhet”
Via Marcantonio Colonna, 23 - 00192 Rome, Italy
Tel. +39 06 3214879 / 3215145 (ext 109)
Fax +39 06 3214879
E-mail: segreteriaacesma@assoaeronautica.it
<http://www.cesmamil.org>

TABLE OF CONTENTS

CONTRIBUTORS	7
EXECUTIVE SUMMARY	11
PREFACE , by Umberto Gori.....	13
1. HYBRID AND DOCTRINE , by Giuseppe G. Zorzino.....	19
2. THE CYBER DIMENSION OF THE HYBRID WARFARE: the NATO view , by Marco Donfrancesco, Alessandra Bruni.....	49
3. HYBRID AND CYBER WARFARE , by Fernando Rizzo, Riccardo Rossi.....	59
4. HYBRID AND SATELLITE SYSTEMS , by Emanuela Acquaviva, Gianluca Scialanga, Vittoria Piantelli, Giorgio Sciascia, Daniele Frasca.....	72
5. HUMAN FACTORS IN HYBRID THREATS: the need for an integrated view , by Isabella Corradini.....	83
6. LEGAL ASPECTS OF HYBRID WARFARE IN SPACE&AIR DOMAIN , by Carlo C. Carli.....	95
7. HYBRID AND AWARENESS: basic principles , by Isabella Corradini, Giuseppe G. Zorzino.....	111

CONTRIBUTORS

Emanuela Acquaviva

Doctor in Theoretical Physics, she developed a mathematical model that reproduce the behaviour of turbulence in space plasmas. Within the Master of Science and Space Technology, she holds an internship at Thales Alenia Space Italia to study the statistical properties of a new generation cryptographic algorithm. She started working at TAS-I in the Department of Security and Assurance Unit as Cyber Security Architect. The main activities concern aspects of cyber security applied to space systems.

Alessandra Bruni

A Leonardo's Marketing Manager currently involved in different Cyber Defence and Cyber Security main themes focusing on National Grid Critical Infrastructures and National Security issues.

C. Carlo Carli

Solicitor & a counselor, Bar of Rome. President AE/AGEIE THINK TANK. Resp. legal dept & brand manager USERS&CONSUMERS NETWORK. OF2(r), served as officer and teacher for about 6 years in G.d.F. . Certified expert 'army leg.ad.', acts as military & security legal adviser. Worked abroad for foreign relations of Italian companies, as tax or compliance manager. Seconded to OCSE and many other entities as tax expert. Appointed of teaching 'international & comparative tax law', as well 'Analysis Techniques'. Written about 200 scientific publications. Often part in international and national public Study & Working Groups.

Isabella Corradini

Social and cyber-psychologist, and criminologist, expert on human factors and awareness methodologies, security and safety, communication and reputation. She is President and Scientific Director of *Themis Research Centre*, an interdisciplinary research lab in psychology and criminology, and co-founder of "*Link&Think research lab*", focused on socio-technical analysis of information technologies and informatics education (computational thinking). She lectures in academic masters and industrial training programs. She has written many papers and books in the expertise areas and she is the editor of a book series about reputation with Franco Angeli, a major Italian publishing house.

Marco Donfrancesco

A Leonardo Senior Manager with over 38 years of experience, involved since ten years in different Cyber Defense and Electronic Warfare domains roles and positions. Currently he is focusing on future Leonardo Cyber Electromagnetic Capabilities developments and on the Cyber Resilience of the Military Platforms and Defence Systems.

Daniele Frasca

Master Degree in Electronic Engineering. Daniele is the Head of the System Security Department and Security Advisor to Senior Executive Vice President Business Line Observation Exploration & Navigation in Thales Alenia Space Italy. He has been Information Technology Security and Computer Science researcher in the Italian National Defence Department and Security Project Leader of the Military Defence Telecommunication System in ELMER LEONARDO SpA.

Umberto Gori

Emeritus professor at Florence University, President of CSSII and Director of ISPRI.

Vittoria Piantelli

Engineer in Electronic Automation, she is employed in Thales Alenia Space since 2011. In the security department, she has worked as System Security Engineer for national and international programs: MUSIS as responsible for security aspects for Satellite and Ground Segment (Italian MoD, International Defense - OCCAR - DGA); SENTINEL as security advisor for TASI and ESA/ESTEC; COSMO 2nd GENERATION as security responsible for Risk Analysis and Common Criteria Certification Process.

Fernando Rizzo

Ph.D. in Strategic Studies (University of Turin's graduated, research thesis about the strategic thinking of Islamic movements), Arabic speaker, expert of international relations and Arab-Islamic culture. Retired Officer of Arma dei Carabinieri, he served in the Counter Terrorism Special Branch of Raggruppamento Operativo Speciale (ROS) Carabinieri. Nowadays, he is "Corporate Sales Area Manager Army and Law Enforcement" for Elettronica Group.

Riccardo Rossi

Riccardo Rossi has received the Master Degree in Computer Science Engineering from Tor Vergata University of Rome with a thesis on Support Vector Machines based Cloud detection over QuickBird imagery. He spent six months as a Research Trainee at the Joint Research Centre of the European Commission working in the field of Artificial Intelligence applied to Computer Vision. He has been 5 years with AgustaWestland as Software Engineer, working on flight simulation in virtual and augmented reality. He is currently the team leader of Cyber Intelligence Unit of Cy4Gate, responsible of the design and development of the integrated solutions of data analytics retrieved from heterogeneous sources.

Gianluca Scialanga

For Thales Alenia Space, as technical responsible of security certifications for the Earth Observation Programs (CSG, Sicral). For Selex ES (now Leonardo), since 2013 as IT Security Evaluator accredited by the Italian NSA and OCSI (an office of the Italian Department of Economic Development) for the security evaluations of products or systems. For Nexse (now Alten), since 2003 as web application developer for Wind S.p.A. . Master Degree in Computer Science Engineering (2002, Rome La Sapienza).

Giorgio Sciascia

Giorgio Sciascia, degreed in Telecommunication Engineer in 2002 in Rome, has worked for two years in German Aerospace Centre (DLR) in Munich. Afterward he has been employed in Thales Alenia Space Italia (TASI) where he is working in the field of Security. He has been the technical responsible of Engineering Security for main TASI telecommunication and earth observation Programs, managing accreditation and certification activities.

Giuseppe Giovanni Zorzino

Teacher and consultant of information security. Graduated in Electronic Engineering (Naples – Italian Air Force Academy), he is working at Max Italia Srl. He is also serving as CyberSecurity Coordinator at CESMA. He has more than 35 years' experience in the IT industry where has devoted the last 20 years of his career to IT security, governance, and management systems consultancy. He holds 2 patents deposited and recorded, and maintains many certifications in good standing like ERMCP, CISA, CISM, CGEIT, CRISC, Lead Auditor ISO27001, Security+, MCSASec.

EXECUTIVE SUMMARY

Today there are many definitions of "hybrid warfare". They refer, in different ways, to those strategies that prefer the use of any advantage to the opponent on the entire elements of national power spectrum, in short DIMEFIL¹, in order to affirm their will, not necessarily within the declared wars.

This is a high interest scenario for individual nations and for the entire NATO Alliance due to the potential impact on aerospace power deriving from the malicious use of emerging technologies today.

In particular, the potential impact on the Air Domain resulting from the use of hybrid technologies causes significant upheavals in traditional security concepts. These are currently based on the design of reaction capacities towards "traditional threats" in the relationship between the strategic concept of "Integrated Defense" of the Alliance and the National Defense.

Therefore, there is the need to develop a comprehensive analysis of how traditional Defense Systems will have to evolve and adapt their own political, legal, regulatory and procedural peculiarities (details), without excluding technological/industrial development aspects that will respond to this potential "emerging challenge".

The document is a set of interpretations of the same phenomenon according to different visions that specific domains have and cause effects on Air Power and the Defense System.

The industrial vision of the effects of hybrid cyber threats on space communications and electronical warfare together with the role that psychology can have in implementing sophisticated threats, and last but not least, the legal implications, are the aspects covered by this analysis. In addition, psychology is also involved in staff aware to recognize threats affecting the human dimension of attacks.

¹ DIMEFIL stands for Diplomatic/Political, Information, Military, Economic, Financial, Intelligence and Law Enforcement (Elements of National Power; US DoD), <http://www.acronymfinder.com/>