ASSOCIAZIONE ARMA AERONAUTICA
CESMA
Centro Studi Militari Aeronautici Giulio Douhet

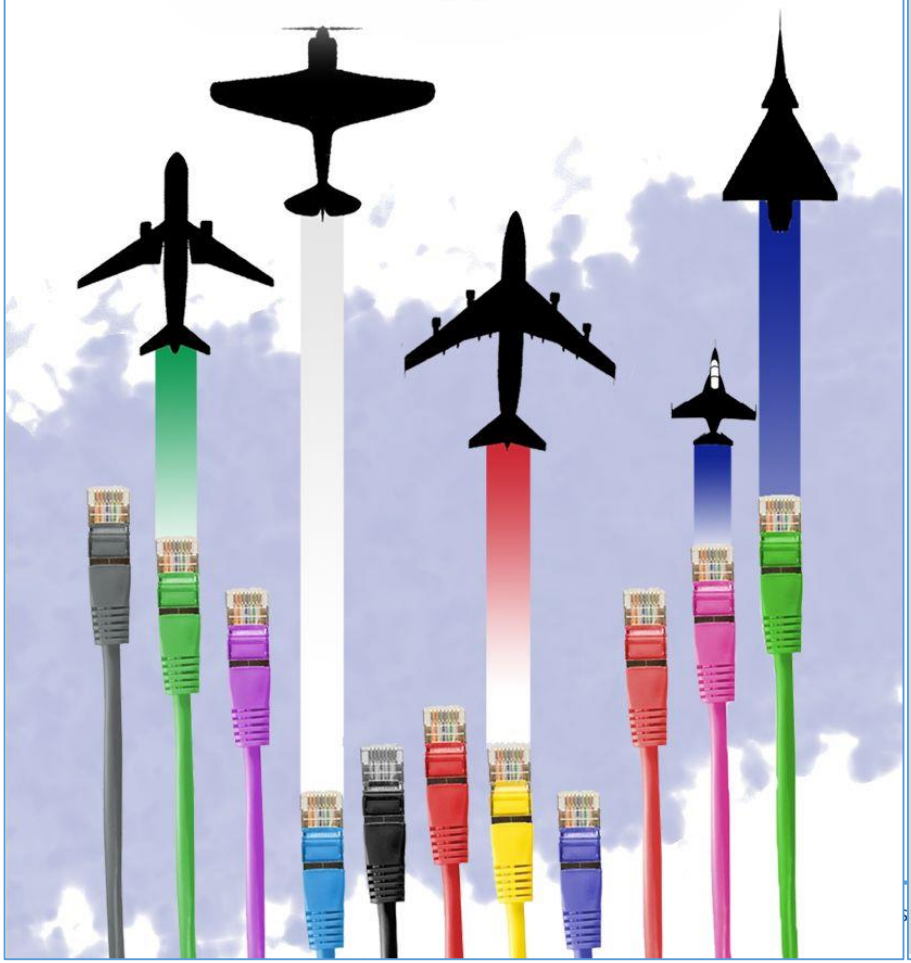
HYBRID CYBER WARFARE AND THE EVOLUTION OF AEROSPACE POWER: risks and opportunities

ing. Giuseppe G. Zorzino
ERMCP, CISA, CISM, CGEIT, CRISC, LA ISO27001

09/11/2017

ASSOCIAZIONE ARMA AERONAUTICA
CESMA
Centro Studi Militari Aeronautici Giulio Douhet

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



ASSOCIAZIONE ARMA AERONAUTICA
CESMA
Centro Studi Militari Aeronautici Giulio Douhet

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

WG: "Hybrid Cyber Warfare and the aerospace power: risks and opportunities"

TABLE OF CONTENTS

Hybrid threats

Hybrid è il nuovo "termine di moda (buzzword)" nel campo militare

Non è l'indicazione ovvia di un conflitto asimmetrico e non c'è una dottrina stabilita. C'è solo "Evoluzione della terminologia nella descrizione di conflitti – impiego del termine 'ibrido'" – SMD III CID

"hybrid" non è presente nella pubblicazione AAP-06 "NATO glossary of terms and definitions" edition 2014.

Il concetto di "ibrido" era già presente in altre pubblicazioni NATO:
"BI-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats.", 2010

"Multimodal, low intensity, kinetic and non-kinetic threats to international peace and security including cyber war, low intensity asymmetric conflict scenarios, …. were identified by NATO as so called hybrid threats".

Hybrid threats

Sfruttamento di vulnerabilità del target, usando metodi convenzionali e non convenzionali per generare ambiguità ed ostacolare i processi decisionali al fine di:

- ✓ generare sorpresa;
- ✓ prendere l'iniziativa;
- ✓ generare inganno e ambiguità;
- ✓ evitare l'attribuzione dell'azione;
- ✓ massimizzare il disconoscimento della responsabilità per azioni aggressive.

Cyber threats

"Cyber threats resemble threats in the fifth dimension of warfare, as cyber warfare is often termed, and refer to a sustained campaign of concerted cyber operations against the IT" (Sacha Bachman)

Il Cyberspace è un facilitatore che correlato con i domini di Aria e Spazio, può rappresentare un rischio per gli interessi nazionali … anche in tempo di pace, senza preavviso e eseguito in totale autonomia

Si tratta di una tendenza effettiva e preoccupante dell'utilizzo di capacità cibernetiche legate a operazioni militari di operazioni ibride: la cosiddetta "dimensione informatica della guerra ibrida" (Amb. Ducaru)

Due visioni:

- sfruttare le opportunità del cyberspazio come un dominio per una comunicazione gratuita, veloce ed efficace
- usare il cyberspazio come un mezzo di attacco al dominio della guerra

Rischi – military side

"Hybrid is the dark reflection of our comprehensive approach. We use a combination of military and non-military means to stabilize countries. Others use it to destabilize them." (Stoltenberg, 2015)

http://www.nato.int/cps/en/natohq/opinions_118435.htm

È "Unrestricted warfare", l'uso integrato di tutte le espressioni di forza di una nazione.

L'uso di tecnologie COTS ha potenziato notevolmente la capacità di impatto sul sistema di sicurezza di un paese.

Tecnologie a basso costo utilizzate nei domini dell'aria e del cyber possono rappresentare un problema militare quando causano imprevedibili minacce agli interessi nazionali ed alla sicurezza.

Minacce aeree di tipo *Low, Slow and Small (LSS)*

Difesa da minacce ed attacchi ibridi è responsabilità delle singole nazioni (resilienza).

Rischi – civilian side

Il Consiglio Europeo a giugno 2015 ha ricordato la necessità di mobilitare gli strumenti dell'UE per aiutare nel contrasto delle minacce ibride.

EU Commission - "Joint Framework on countering hybrid threats, a European Union response", Brussels, 6.4.2016

> "While definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare."

Minacce alle infrastrutture critiche e alle reti affliggono tutti gli Stati dell'UE

- "How France's TV5 was almost destroyed by… "
- "Cyberattack on a German steel-mill"
- Air Traffic control
- …..

Opportunità

Hybrid warfare strategy → cooperazione NATO - UE (Warsaw 2016)

- Riconoscimento delle minacce
- Resilienza nazionale delle Infrastrutture Critiche e (Air) Defence Systems
- Sviluppare sistemi di rapida valutazione e decisione
- Migliorare le capacità nazionali
- Riempire i divari tecnologici con la cooperazione industriale

Migliorare l'applicazione degli standards IT (ISO27001, NIST Framework, ISO31000)

- Governance
- Gestione delle minacce
- Gestione delle conseguenze
- Non c'era un framework legale utilizzabile fino a Tallinn Manual 2.0. E ora?

Action 12: The Commission, in coordination with Member States, will work together with industry within the context of a contractual Public Private Partnership for cybersecurity, to develop and test technologies to better protect users and infrastructures against cyber aspects of hybrid threats.

Domande?


ASSOCIAZIONE ARMA AERONAUTICA
CESMA
Centro Studi Militari Aeronautici Giulio Douhet
CESMA
via M. Colonna, 23
00192 Roma
+39 06 32.15.145
info@cesmamil.org
Dr.
Giuseppe G. Zorzino
Cyber Security Coordinator
+39 347.18.72.858
g.zorzino@cesmamil.org
Max italia
ing. Giuseppe Giovanni Zorzino
ERMCP CISA CISM CGEIT CRISC LA27001 MCSA2003:Sec
Security+ CMMIappr Certificatore etico IBM_Cert_Spec
Governance & Sistemi di Gestione
+39 347.18.72.858
+39 06 879 30500
g.zorzino@max-italia.it