ISACA®
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

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

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

Roma 09/07/2018

Bio

Giuseppe Giovanni Zorzino

Consulente e docente di sicurezza delle informazioni, attualmente mi occupo di cyberstrategies, sistemi di gestione della sicurezza, governance e sicurezza delle informazioni nelle organizzazioni, privacy, governance e compliance

35+ anni di esperienza nell'IT, nell'analisi e sviluppo di basi di dati complesse e una consolidata esperienza nella IT security

Accademia di Pozzuoli, Ufficiale del Corpo del Genio dell'A.M., coordinatore Cybersecurity del CESMA (Centro Studi Militari Aeronautici) "Giulio Douhet"

Membro della Comm. Sicurezza Informatica dell'Ordine degli Ingegneri, nonché di ISACA, ISC2 Italian Chapter, ERMAcademy, IAPP

Vasta attività di divulgazione e formazione c/o enti pubblici e PMI

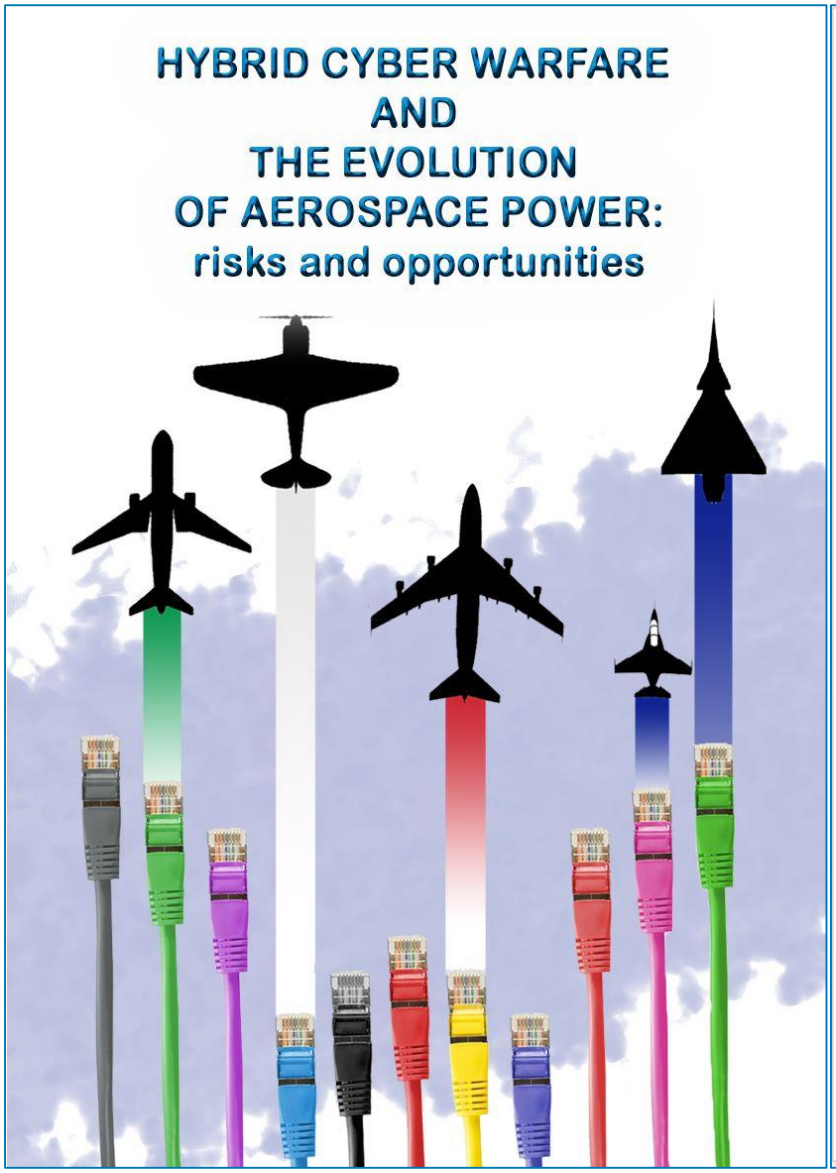
2 brevetti

Varie certificazioni attive tra cui ERMCP, CISA, CISM, CGEIT, CRISC, Lead Auditor ISO 27001, Security+, MCSASec 2003, Certificatore etico, IBM Cert Solution Architect, …

Agenda

1. Hybrid threats
2. Un breve glossario
3. Cyber threats
4. Hybrid Cyber Warfare
5. Rischi e opportunità
6. Il futuro

Il quaderno CESMA



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

Hybrid cyber warfare and the evolution of aerospace power: risks and opportunities 2

www.cesmamil.org

WG: "Hybrid Cyber Warfare"

TABLE OF CONTENTS

- Hybrid and Doctrine
- The cyber dimension of the Hybrid Warfare: the NATO view
- Hybrid and Cyber Warfare
- Hybrid and Satellite Systems
- Human factors in Hybrid Threats: the need for an integrated view
- Legal aspects of Hybrid Warfare in Space&Air domain
- Hybrid and Awareness: basic principles

Hybrid threats

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

Il termine "Hybrid" è facilmente associato a tutti i tipi di combattimento che usano mezzi non convenzionali, attori e metodi non altrimenti classificabili.

I "conflitti ibridi" sono considerati una nuova forma di confronto.

Il termine "hybrid" non è presente nel "NATO glossary of terms and definitions" del 2014.

Eppure il concetto di "hybrid threats" era già stato indicato nelle pubblicazioni NATO:
"**Multimodal, low intensity, kinetic and non-kinetic threats to international peace and security including cyber war, low intensity asymmetric conflict scenarios, global terrorism, piracy, transnational organised crime, demographic challenges, resources security, retrenchment from globalization and the proliferation of weapons of mass destruction were identified by NATO as so called *hybrid threats***".

Hybrid threats - dottrina

Non c'è una dottrina stabilita e neanche è l'indicazione ovvia di un conflitto asimmetrico.

In generale il termine "dottrina" si riferisce all'insieme di elementi (principi) nel campo civile e militare che costituisce il quadro di riferimento per la definizione di una campagna di operazioni, attacchi o conflitti. (NATO glossary)

C'è solo il manuale di SMD III "Evoluzione della terminologia nella descrizione di conflitti – impiego del termine 'ibrido'".

Per Von Clausewitz "la guerra *non è niente altro che la politica dello Stato proseguita con altri mezzi".*

Fino agli anni '80, la guerra (Cold War) era basata su bilanciamento di blocchi e forze, e sulla deterrenza determinata da minacce nucleari reciproche (*Mutual* assured *destruction* o MAD).

Nuovi principi generali per nuovi tipi di conflitti.

Conflitti ibridi

Nel 2005, Mattis e Hoffman scrivono un articolo parlando di nuovi tipi di conflitti detti "ibridi", che utilizzano simultaneamente e in modo adattativo mezzi convenzionali e non.

Dipendono dalla tecnologia e dallo stato dell'arte, non sono più basati sulle capacità cinetiche di una nazione, bensì sulla "narrativa" degli eventi per orientare le operazioni e l'efficacia degli interventi contro un oppositore.

Conflitti che impiegano mezzi eterogenei sono intrinsecamente "ibridi". Ma tutti i conflitti sono per qualche natura "ibridi".

"The use of any means and capabilities" ha effetti sull'intera popolazione.

The same use of unconventional means classifies conflict as “unconventional” according to the terminology in use.

Un breve glossario

Il termine "**regolare**" si applica a confronti tra organizzazioni militari strutturate come le forze armate di uno stato: Esercito, Marina, Aeronautica e Polizia Militare.

Sulla base delle leggi internazionali, sono considerate forze "**irregolari**" le truppe indipendenti non inquadrate nelle forze armate, ma incluse tra i combattenti legittimi.

Sempre più spesso, le azioni condotte da "**attori non statali irregolari**" utilizzano metodi asimmetrici per guidare il consenso e coinvolgere la popolazione.

Un breve glossario

Il termine "**asimmetria**" è considerato non solo per i metodi di confronto, ma anche nei rapporti di disuguaglianza tra forze combattenti.

Un conflitto è "**simmetrico**" quando coinvolge forze armate regolari di stati riconosciuti.

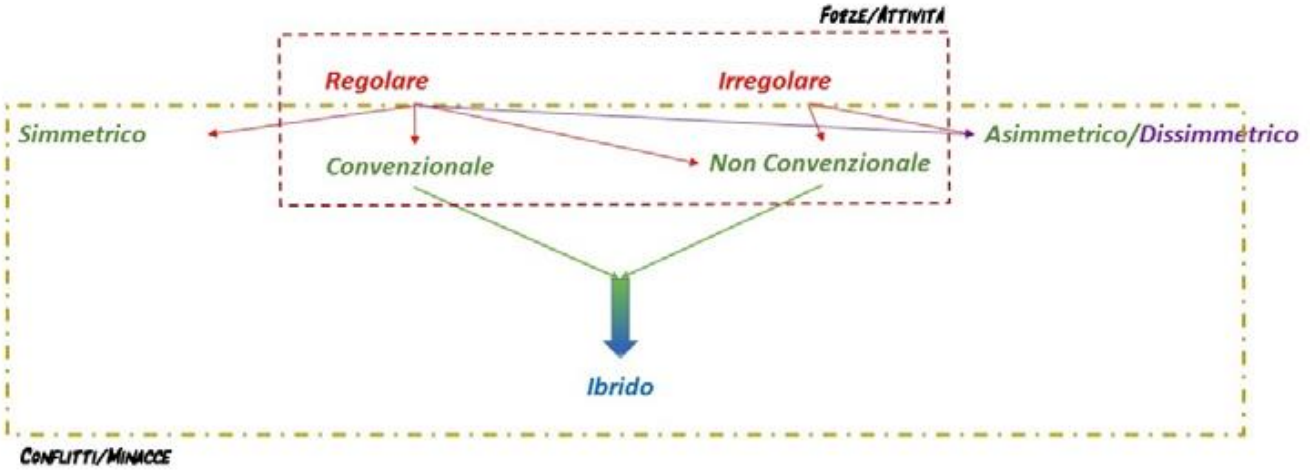
Un conflitto è "**asimmetrico**" quando una parte è rappresentata da forze "irregolari" senza capacità militari significative. Questa parte orienta i suoi sforzi verso le possibili debolezze della controparte: altri aspetti di uno stato quali economia, sociale, politica, energia, informazioni, infrastrutture, sanità, ambiente, ecc.

Un breve glossario

Per tradizione, i termini "**convenzionale**" e "**non convenzionale**" sono utilizzati per catalogare le tipologie di armamenti.

Un esame delle definizioni delle tipologie di armamenti serve per posizionare correttamente i tipi di mezzi usati nel campo delle attività offensive cyber.

Tutti gli armamenti sono "**convenzionali**" eccetto quelli CBRN che insieme alle forze speciali sono "**unconventional**". Questo termine è usato anche per le azioni e forme di confronto condotte da componenti irregolari delle forze avversarie che impiegano tutte le tattiche, procedure e tecniche non convenzionali disponibili.



Hybrid threats

Le minacce ibride sfruttano le 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

Unrestricted Warfare

Ci sono molte pubblicazioni con definizioni di Hybrid Threats e Hybrid Warfare, ma non dobbiamo dimenticare che i concetti sono stati ben espressi da due colonnelli del PLA, Qiao Liang e Wang Xiangsui, nel loro libro "Unrestricted Warfare" (1999) che ne definisce l'approccio cinese.

Gli autori teorizzano forme di combattimento integrate che fanno uso di tutte le espressioni di forza di una nazione definendo il concetto di "war beyond the limits", più precisamente "guerra combinata che va oltre i limiti", quale metodo di conflitto senza restrizioni di alcun tipo e che va oltre qualsiasi cosa.

Una "guerra senza vincoli" può iniziare ben prima di qualsiasi conflitto armato e tenta di distruggere l'avversario sfruttando le vulnerabilità dei suoi sistemi di informazione senza riguardo alle leggi e ai regolamenti internazionali.

Conflict hybrid and hybrid war

Secondo Patryk Pawlak, membro del EPRS (European Parliamentary Research Service), il termine “hybrid threat” rappresenta complessità ed incertezza, ma è anche usato per indicare "**conflict hybrid and hybrid war**" in funzione dell'intensità delle minacce e dell'intenzionalità degli attori:

Hybrid threat – risultato di diversi elementi interconnessi che causano una minaccia multidimensionale;

Hybrid conflict – mix di mezzi eterogenei, ma non forze armate;

Hybrid war – uso di forze armate con un mix di deterrenza, supremazia economica, sfruttamento di vulnerabilità politiche, strumenti tecnologici e metodi diplomatici.

La Commissione Europea presenta una definizione ampia delle minacce ibride nel documento "*Joint Framework on countering hybrid threats, a European Union response*", Brussels, 6.4.2016, sottolineando che la risposta deve assicurare un alto grado di flessibilità e adattabilità a qualsiasi complessità e soluzione tecnologica della minaccia.

Cyber Warfare

Come per il termine "hybrid", anche il termine "cyberwarfare" è spesso usato in modo improprio e non collocato nella corretta dimensione.

Secondo una definizione generale "***cyberwarfare*** *refers to a massively coordinated digital assault on a government by another, or by large groups of citizens. It is the action by a nation-state to penetrate another nation's computers and networks for the purposes of causing damage or disruption*."

Le operazioni condotte nel cyberspace sono essenzialmente **cyber threats**.

Secondo GNOSIS è "l'insieme delle operazioni condotte nel e tramite il cyberspace al fine di negare all'avversario – statuale o non – l'uso efficace di sistemi, armi e strumenti informatici o comunque di infrastrutture e processi da questi controllati. Include anche attività di difesa e "capacitanti" (volte cioè a garantirsi la disponibilità e l'uso del cyber-space)."

Computer Network Operations

Cyber threats, cyber warfare o cyber war non possono esistere senza accesso al cyberspace. Quindi, sono necessari strumenti e conoscenze IT per attuare concetti operativi per il "Network Centric Warfare". Si parla di **CNO** (Computer Network Operations) activities per indicare capacità di:

- attacco e distruzione delle reti avversarie;
- difesa dei propri sistemi informativi militari;
- sfruttare a fondo le vulnerabilità dei computer networks avversari.

In sintesi queste capacità sono brevemente indicate come:

Computer Network Defense (CND) – misure defensive per proteggere informazioni, computers, e networks dal blocco o distruzione.

Computer Network Exploitation (CNE) – preparazione dell'**IO battlespace** attraverso azioni di **intelligence, surveillance, and reconnaissance**, e un'approfondita pianificazione delle attività.

Computer Network Attack (CNA) - alterare o distruggere le informazioni residenti in computer e reti di computer utilizzando un flusso di dati come arma per eseguire un attacco.

Hybrid Cyber Warfare

È cyberwarfare implementato unicamente con tecniche non convenzionali , senza qualsiasi intervento militare o altra forma di minaccia o pressione (militare).

Bisogna anche considerare quanto sono estesi gli attacchi e come le differenti forme di attacchi cyber sono concorrenti affinchè riescano a saturare il cyberspazio dell'avversario.

Prendendo in prestito le definizioni di guerra cibernetica e ibrida, è ragionevole pensare alla "hybrid cyber warfare" come ad una forma di conflitto che coinvolge contemporaneamente attori statuali e non, realizzata usando solo mezzi di attacco cyber (non cinetici o convenzionali) i quali interagiscono persistentemente nel campo di battaglia del cyberspazio, con conseguenti effetti permanenti sulla controparte. In breve, "una forma di conflitto violento" in cui la "violenza" è il risultato delle operazioni di CNA con effetti permanenti sulle strutture organizzative, logistiche e militari dell'avversario.

Esempi

Gli obiettivi sono creare incertezza e confondere i decisori, ma anche causare potenziali effetti di danneggiamento permanente, alterare processi, intervenire nei sistemi di controllo.

Un esempio possibile, ma di errata attribuzione ad un attacco cyber è stato l'incidente alla più grossa diga idroelettrica della Siberia Sayano-Shushenskaya, August 17, 2009. un malfunzionamento dei sistemi di controllo ha causato 75 morti, 5 anni di ricostruzione, +1,3B$ di danni, 500.000 tons di alluminio non prodotte, 6500MW non distribuiti.

Ma ci sono stati attacchi alle infrastrutture critiche e alle reti che hanno afflitto tutti gli Stati dell'Ue:

- 2015 "How France's TV5 was almost destroyed by… " https://www.bbc.com/news/technology-37590375
- 2014 "Cyberattack on a German steel-mill"

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf

- 2015 "Zaporizhia power station in Ukraine was switched off…"

https://www.independent.co.uk/news/world/europe/ukraine-turns-off-reactor-at-nuclear-plant-after-accident-9947540.html

Rischi – military side

La strategia di risposta della NATO adattata alle minacce ibride richiede a tutte le nazioni dell'Alleanza di:

- riconoscere e attribuire gli attacchi ibridi in tempo utile;
- sviluppare una capacità di recupero per resistere all'attività ibrida;
- implementare processi che garantiscano una valutazione ed un processo decisionale rapidi ed efficaci;
- possedere le capacità necessarie per affrontare e rispondere in modo efficace.

Gli impatti, anche o principalmente, su obiettivi non militari ha portato ad uno stretto coordinamento tra la NATO e l'UE per un'efficace attuazione di una strategia comune di guerra ibrida.

La risposta NATO si basa su tre funzioni correlate:

PREPARE - raccolta di informazioni continua, completa, fusione e condivisione;

DETER - presenza militare visibile e credibile, capacità di schierare rapidamente le forze per rafforzare gli alleati, dimostrazione di coesione;

DIFEND - contenere e limitare la libertà d'azione dell'avversario e sconfiggere la minaccia.

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."

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.

Il futuro

Memes e social network sono diventati strumento militare, mentre molti governi non sembrano equipaggiati per comprendere la nuova realtà della guerra dell'informazione.

In internet, la parola "meme" si riferisce spesso a un'immagine divertente che diventa virale sui social media. Più in generale, tuttavia, «un meme è un'idea che si diffonde, sia che l'idea sia vera o falsa».

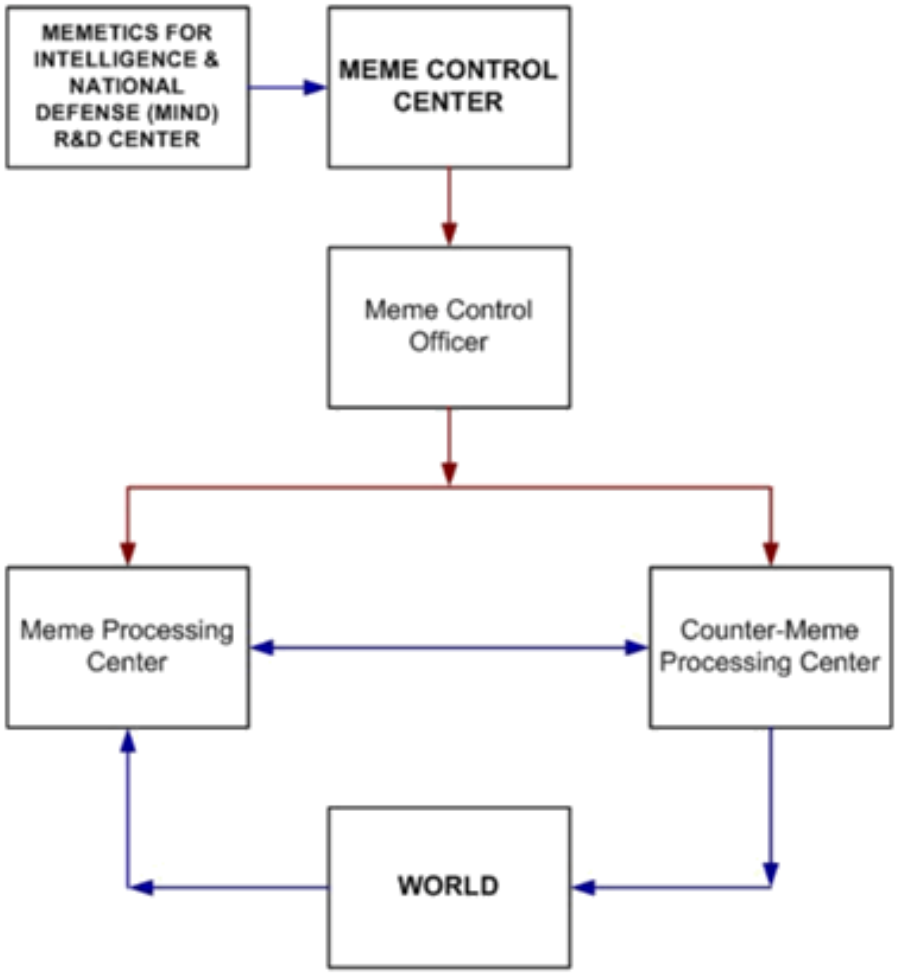
Come combatteremo la disinformazione e la propaganda sponsorizzata dallo stato in futuro?

Nel 2011, un professore universitario con esperienza in robotica ha presentato un'idea che all'epoca sembrava radicale.

Dopo aver condotto ricerche sostenute dalla DARPA - la stessa agenzia di difesa che ha contribuito a generare Internet - il dott. Robert Finkelstein ha proposto la creazione di un nuovo braccio dell'esercito americano, un "Centro di controllo del meme".

Meme Control Center

Da "Tutorial: Military Memetics", del Dr. Robert Finkelstein, presentato al Social Media for Defense Summit, 2011



Meme militari ed intelligence

Le elezioni presidenziali americane del 2016 sono state modellate da un mix volatile di notizie false, intromissioni straniere, immagini dottorate, enormi perdite di email e persino un meme di cartoni animati (Pepe the Frog). Per non parlare di un sito di notizie conservativo chiamato Infowars.

Non sembra più sciocco dire che il futuro della guerra non è sul campo di battaglia, ma sui nostri schermi e nella nostra mente.

Le agenzie militari e di intelligence di tutto il mondo stanno già conducendo guerre informative segrete nel cyberspazio. I loro meme influenzano già profondamente le percezioni pubbliche della verità, del potere e della legittimità.

E questa minaccia si sta intensificando solo man mano che gli strumenti di intelligenza artificiale diventano più ampiamente disponibili.

Provokatsiya

Gli attacchi informativi per screditare, sgomentare e confondere un avversario possono essere riassunti in una parola vecchia di secoli: Provokatsiya, che è russo per "atto di provocazione".

Oltre alle interferenze internazionali, i politici hanno anche messo in atto campagne di influenza digitale interna. La campagna del presidente Trump è stata sottoposta a un controllo crescente l'azienda britannica Cambridge Analytica ha dimostrato di aver utilizzato i dati di Facebook e influenzato il comportamento degli elettori durante le elezioni del 2016.

Tuttavia, l'attenzione dei militari si concentra sui casi di un avversario straniero che attacca un altro paese (al contrario delle campagne di influenza interna), e su atti di guerra dell'informazione sponsorizzati dallo Stato (in contrapposizione ad atti perpetrati da attori non affiliati).

Cambridge Analytica

Dr Alex Kogan [redacted] 9 May 2014 at 02:14
To: Christopher Wylie [redacted], [redacted]

Hey Chris and [redacted],

Great chatting with you both yesterday. Here is a list of traits that can be predicted now--good starting shopping list. More specific items can also be predicted within the bigger personality questionnaires, but this is a start to get you thinking about what you may want:

- openness
- conscientiousness
- extraversion
- agreeableness
- neuroticism
- life satisfaction
- iq
- gender
- age
- political views = conservative?
- political views = liberal?
- political views = uninvolved?
- political views = libertarian?
- religion (categorical)
- job (categorical)
- university subject concentration (categorical)
- self-disclosure (do you tell people about yourself or not?)
- fair-mindedness (fair or suspicious in dealings with others?)
- self-monitoring (do you change your personality depending on who you're with)
- sensational interests (has 5 factors, "militarism" [guns and shooting, martial arts, crossbows, knives], "violent occultism" [drugs, black magic, paganism], "intellectual activities" [singing and making music, foreign travel, the environment], "credulousness" [the paranormal, flying saucers], "wholesome interests" [camping, gardening, hill-walking], see: https://www.academia.edu/157864/The_first_sensational_interests_paper - it's used in forensic psychology to understand criminality)
- belief in star signs (5 point scale)

Le guerre del futuro

Le guerre del futuro useranno la propaganda computazionale e gli inganni digitali avanzati per distorcere la percezione della realtà da parte del nemico e manipolare l'opinione pubblica.

La catena di attacco di guerra dell'informazione:

- un avversario estrae/ruba i metadati degli obiettivi, li usa per creare un profilo psicografico per identificare le vulnerabilità dei bersagli.
- il software di editing con abilitazione AI è utilizzato per generare contenuti video e audio dannosi.
- i Bot pompano strategicamente un contenuto ingannevole nei sistemi di informazione online e i robot abilitati li alimentano alle persone che hanno maggiori probabilità di condividere file multimediali contraffatti.
- feed di notizie sociali consentono una condivisione e visualizzazione diffuse di contenuti ingannevoli
- la disinformazione corre dilagante online, erodendo la fiducia della società nelle istituzioni e portando al caos, alla confusione e persino alla ribellione.

Agenda

1. Hybrid threats
2. Un breve glossario
3. Cyber threats
4. Hybrid Cyber Warfare
5. Rischi e opportunità
6. Il futuro

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
MATICMIND
ing. Giuseppe Giovanni Zorzino
ERMCP CISA CISM CGEIT CRISC LA27001 MCSA2003:Sec
Security Consultant
+39 335.628.1204
+39 02.27426.1
giuseppe.zorzino@maticmind.it