HYBRID CYBER WARFARE AND THE EVOLUTION OF AEROSPACE POWER: RISKS AND OPPORTUNITIES

Il fattore umano nelle minacce ibride: la necessità di un approccio integrato

Titolo originale nella pubblicazione CESMA, 2017:

Human factors in hybrid threats: the need for an integrated view

Isabella Corradini

Scientific Director Themis Research Centre

isabellacorradini@themiscrime.com

Roma, 09 Novembre 2017

by

CESMA Working Group on Hybrid Threats

TABLE OF CONTENTS

ISBN: 978-88-941313-1-4

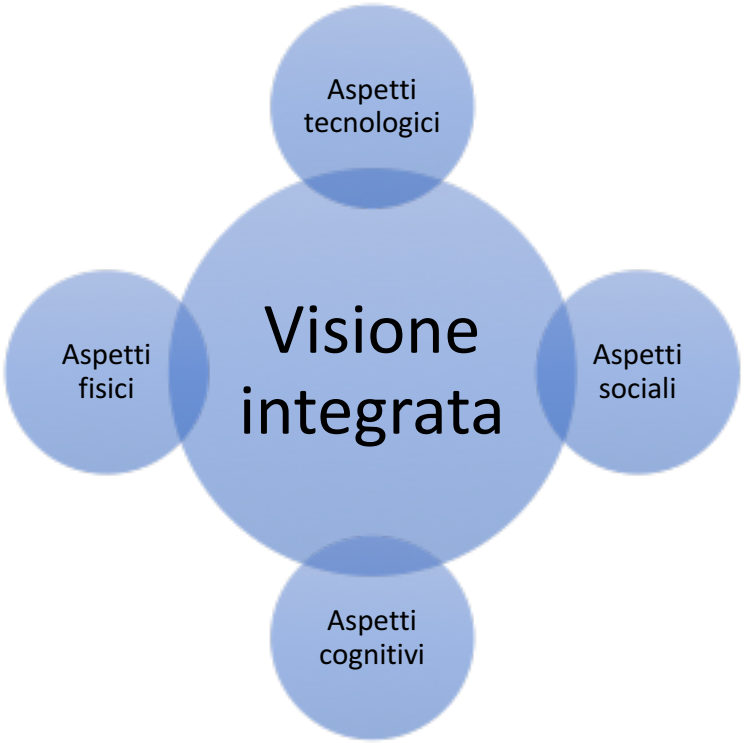
I punti chiave affrontati

- Approccio integrato al tema delle minacce ibride
- Lo scenario dei social media (ruolo dell'informazione e della comunicazione)
- Rilevanza del fattore umano nella cyber security
- Nuove esigenze di awareness

Perché una visione integrata

Lettura dello scenario di riferimento:

- Centralità del cyberspazio (e dei relativi aspetti di sicurezza)
- Evoluzione dell'Internet delle cose (Internet of Things, IoT)
- Ruolo dei social media (dimensione sociale/cognitiva)



Il **fattore umano** è il **comune denominatore**

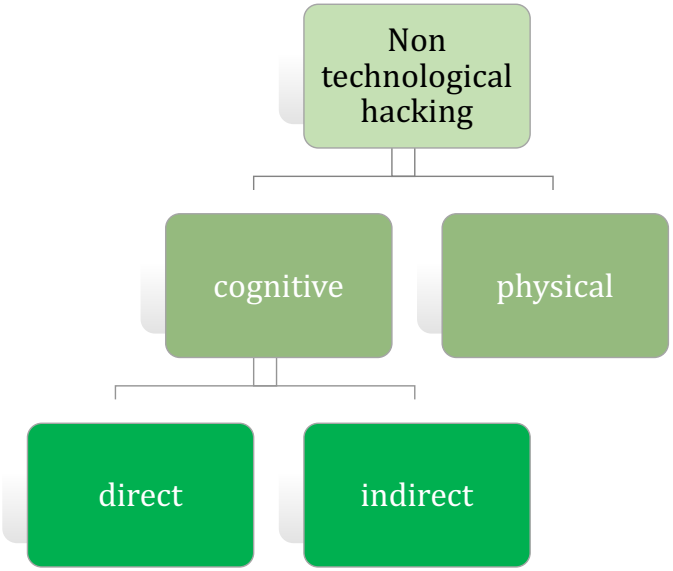
Social media

- Concetto neutro ma utilizzo “non neutro”
- Uso strategico per attività di persuasione/propaganda (es. campagne di disinformazione)
- Utilizzo ad opera di diversi attori con effetto “destabilizzante”(es. creazione di falsi profili per amplificare le notizie)
- Sfruttamento dei social media per costruire “reputazione” o manipolarla
- Il paradosso della società dell’informazione

Attacchi di social engineering

L'ingegneria sociale è uno degli elementi più critici nella cyber security, perché è legato agli esseri umani (e alle loro vulnerabilità)

Autorevoli rapporti annuali sulla sicurezza informatica sottolineano l'importanza e la diffusione di questo tipo di attacchi.



Corradini I. and Nardelli E. (2016), Link&Think Research Lab

Dimensione sociale e cognitiva

Come affrontare le minacce ibride

Prima linea di azione: incrementare awareness

(oltre a: cellula dell'UE per l'analisi delle minacce ibride, comunicazione strategica, centro di eccellenza per la lotta alle minacce ibride ecc.)

"*Quadro congiunto per contrastare le minacce ibride - La risposta dell'Unione europea", Bruxelles, 6.4.2016*

Il fatto che queste minacce si evolvono esige **flessibilità** nel definire contenuti e metodologie utili alla presa di consapevolezza.

Principi di awareness

Chiarire il concetto di awareness

Individuare strategie ad hoc

(es. metodologie per sviluppare specifiche competenze)

tailor-made awareness programs

Resilience

BUILDING EU RESILIENCE TO CYBER ATTACKS

Strong cyber resilience needs a collective and wide ranging approach. […] It also requires a more comprehensive, cross-policy approach to building cyber resilience and strategic autonomy, with a strong Single Market, major advances in the EU's technological capability, and far greater numbers of skilled experts. At the heart of this is a broader acceptance that cybersecurity is a common societal challenge, so that multiple layers of government, economy and society should be involved.

European Commission, Brussels, 13 September 2017,
Joint Communication to the European Parliament and the Council.

Resilience, Deterrence and Defence: Building strong cybersecurity for the EU

Persone e tecnologie

Persone e tecnologie rappresentano un binomio inscindibile, a condizione che vengano rispettati i limiti degli uni e degli altri e si faccia leva sui reciproci punti di forza.

Spesso ci si dimentica che le persone non sono macchine,
e che restano l'elemento chiave di ogni organizzazione, oltre che della società nel suo complesso.

Corradini I. (a cura di), "*Internet delle cose. Dati, sicurezza e reputazione*",
Franco Angeli, 2017, pag. 44.

Grazie per l'attenzione!