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

Human factors in hybrid threats

Isabella Corradini
Social psychologist and criminologist
Scientific Director Themis Research Centre

Rome July 9, 2018

Agenda

- Speaker bio-notes
- Points of discussion:
  - Hybrid threats: why an integrated approach
  - Communication and social media
  - Human factors in cybersecurity: social engineering
  - Awareness
- References

Speaker bio-notes

Isabella Corradini

Social-psychologist and criminologist

Scientific Director of *Themis Research Centre*, an interdisciplinary research lab in psychology and criminology

Co-founder of *Link&Think Research Lab*, focused on socio-technical analysis of information technologies and informatics education (computational thinking)

Expert in human factors and awareness methodologies applied to security and safety

Speaker bio-notes

Isabella Corradini

Her cutting-edge research areas include: cybercrime, cyber(stalking) and cyber(bullying), work-related stress, social engineering, internet of things, social media and corporate reputation.

Lecturer in academic masters (e.g. University of Rome Tor Vergata) and industrial training programs. Ten years as a professor at University of L'Aquila.

Responsible in the educational Italian National Project "Programma il Futuro" (MIUR-CINI) for the part dealing with responsible and respectful use of digital technologies.

Editor of a book series on reputation with Franco Angeli, a major Italian publishing house, whose most recent volume is on the Internet of things (*Internet delle cose. Dati, sicurezza e reputazione*, 2017).

Hybrid threats: why an integrated view

- Central role of cyberspace
- Increasing connectedness between physical objects and Internet (IoT, Internet of Things)
- Cognitive and social factors are as relevant as technological and physical ones
- Lack of “sensors”

Communication and social media

DISINFORMATION

- Significant part of hybrid threats
- Psychological warfare
- Memes, rumor and gossip
- Persuasive communication

Micro-targeting

Micro-targeting

Demographic information,
social media profile,
shopping,
location,
customer behaviour,
ecc.

The Facebook-Cambridge Analytica scandal:

- more than 87 million data people improperly used for political goal
- psychographic profile

What have we learned from this experience?

Human factors in cybersecurity: social engineering

SOCIAL ENGINEERING

"A mixture of activities used to manipulate people's perception, gain their confidence and lead them to disclose sensitive information or do something (e.g. opening an mail attachment),
all for the benefits of those who use these strategies".

Corradini (2017),
Human factors in Hybrid Threats: the need for an integrated view,
CESMA Publication

Social and cognitive dimensions

Awareness is not «only» training

- *"*Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly*"*.

- *"*The 'Training' level of the learning continuum strives to produce relevant and needed security skills and competencies by practitioners of functional specialties other than IT security (e.g., management, systems design and development, acquisition, auditing).

NIST Special Publication 800-16, chapter 2, pp. 15-16

The real risk is ”desensitization”

Information about sensational incidents is certainly important for everyone because it increases awareness that they are all exposed to digital world risks.
But there is another side of the coin.

If people perceive that there is no way out of these risks, they will probably end up gradually accepting the situation: such a climate of passive acceptance, if not a resignation, can become a major risk to manage.

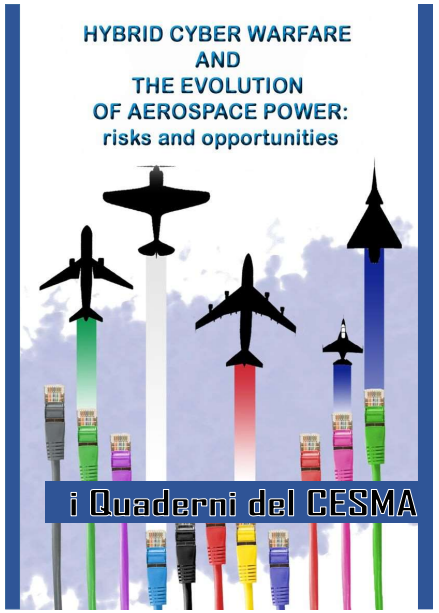
I. Corradini (2018), «The human behaviour is the real problem with security and privacy» https://www.cybersecobservatory.com/2018/06/05/human-behaviour-real-problem-security-privacy/

References

- Corradini I. (2017),"Human factors in Hybrid Threats" (Corradini, 2017) in Hybrid Cyber Warfare and The Evolution of Aerospace Power: risks and opportunities, by CESMA Working Group on Hybrid Threats, CESMA. ISBN: 978-88-941313-1-4

- Corradini I., Zorzino G. (2017), "Hybrid and awareness" in Hybrid Cyber Warfare and The Evolution of Aerospace Power: risks and opportunities, by CESMA Working Group on Hybrid Threats, CESMA. ISBN: 978-88-941313-1-4

- Corradini I. (2018), «The human behaviour is the real problem with security and privacy» https://www.cybersecobservatory.com/2018/06/05/human-behaviour-real-problem-security-privacy/



Contacts

- isabellacorradini@themiscrime.com

Thank you!