Cybersicurezza & Cyberspazio

CS_01.03

Paolo PRINETTO

Director
CINI Cybersecurity
National Lab

Paolo.Prinetto@polito.it
Paolo.Prinetto@imtlucca.it

Mob. +39 335 227529

CYBERSECURITY
NATIONAL LAB

https://cybersecnatlab.it

License & Disclaimer

License Information

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Obiettivo della presentazione

- Introdurre i concetti di
  - Cybersicurezza
  - Cyberspazio
- Offrire puntatori a
  - Tassonomie & Glossari

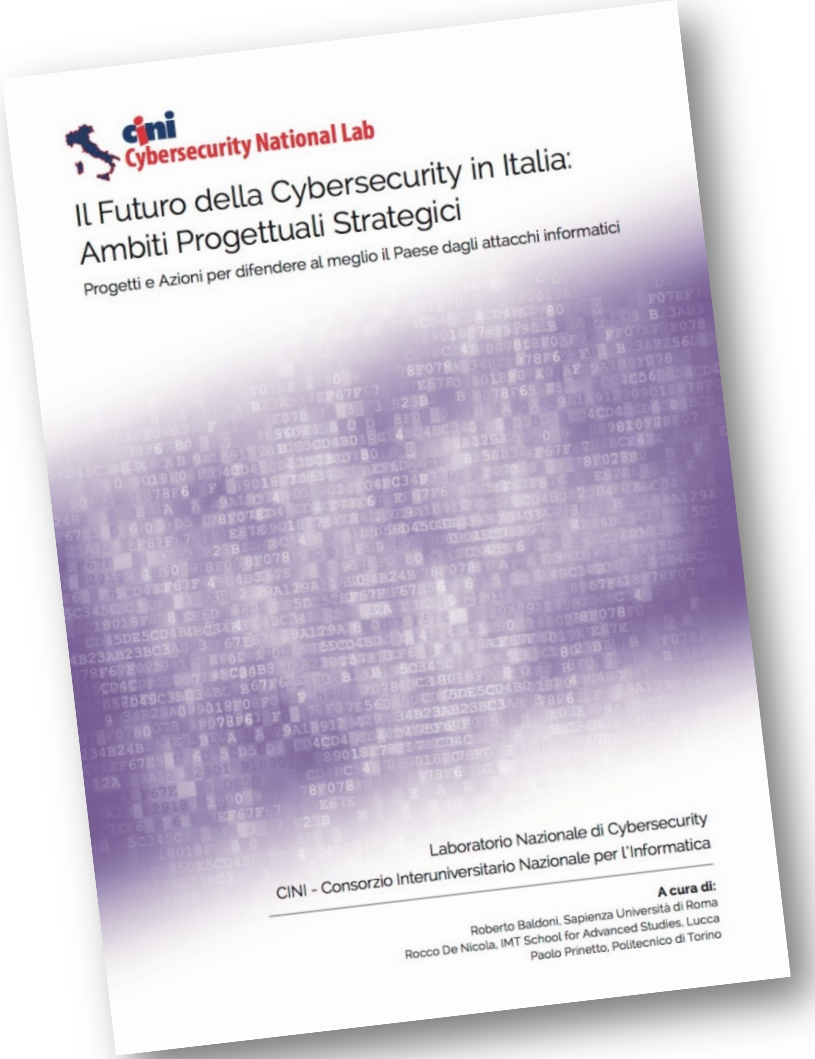
Prerequisiti

- Lezione:
  - *CS 1.01 - Introduzione alla Sicurezza*

https://www.acn.gov.it

Letture consigliate

https://cybersecnatlab.it



Roberto BALDONI
Rocco DE NICOLA
Paolo PRINETTO

Letture consigliate

CYBERSECURITY NATIONAL LABORATORY

Premessa

- La Trasformazione digitale, l'informatizzazione della società e la digitalizzazione di beni, merci e servizi, pubblici e privati, ci obbligano ad avere una grande attenzione verso la sicurezza degli asset informatici.

Cybersicurezza

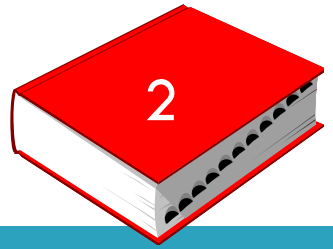
- In letteratura si trovano numerose definizioni (alcune sono riportate nell'Approfondimento #1).
- Qui ci limiteremo a queste tre:

Cybersicurezza

- La cybersecurezza è il modo in cui individui e organizzazioni riducono il rischio di attacchi informatici.
- La sua funzione principale è proteggere i dispositivi che tutti noi utilizziamo (smartphone, laptop, tablet e computer) e i servizi a cui accediamo - sia online sia al lavoro - da furti o danni.
- Si tratta anche di impedire l'accesso non autorizzato alle vaste quantità di informazioni personali che memorizziamo su questi dispositivi e online.

[https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security]

Cybersicurezza



- Insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la *disponibilità*, la *confidenzialità* e la *integrità*, e garantendone altresì la *resilienza*.

[DL 14 giugno 2021, n. 82 - Art.1]

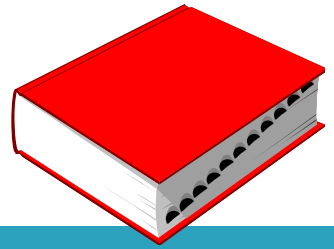
Cybersicurezza

- Pratica che consente a una entità (organizzazione, cittadino, nazione, …) la protezione:
  - dei propri *asset fisici*
  - della *confidenzialità*, *integrità* e *disponibilità* delle proprie informazioni

  dalle minacce che provengono dal *cyberspace*.

[standard ISO/IEC 27000:2014 e ISO/IEC 27032:2012]

Cyberspazio

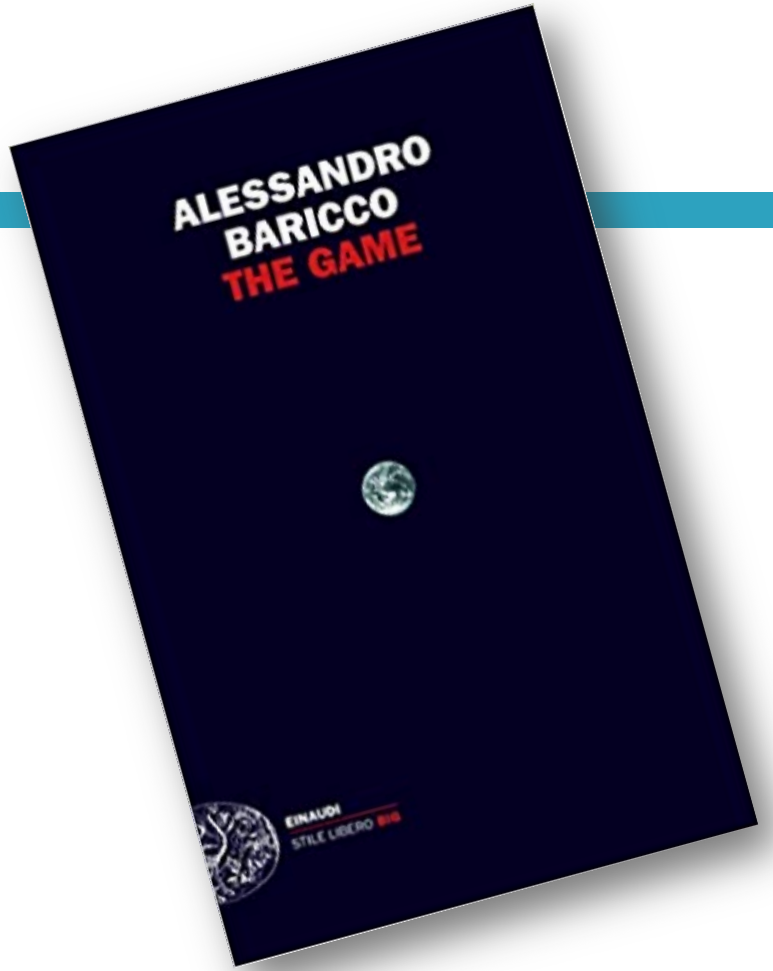


- Quel complesso risultante dall'interazione di persone, software e servizi su Internet per mezzo di tecnologie, dispositivi e reti a esso connesse

[standard ISO/IEC 27000:2014 e ISO/IEC 27032:2012]

Cyberspace

- Quello che Alessandro Baricco chiama l'*oltremondo*



Cyberspace

- … e Luciano Floridi l'*infosfera*

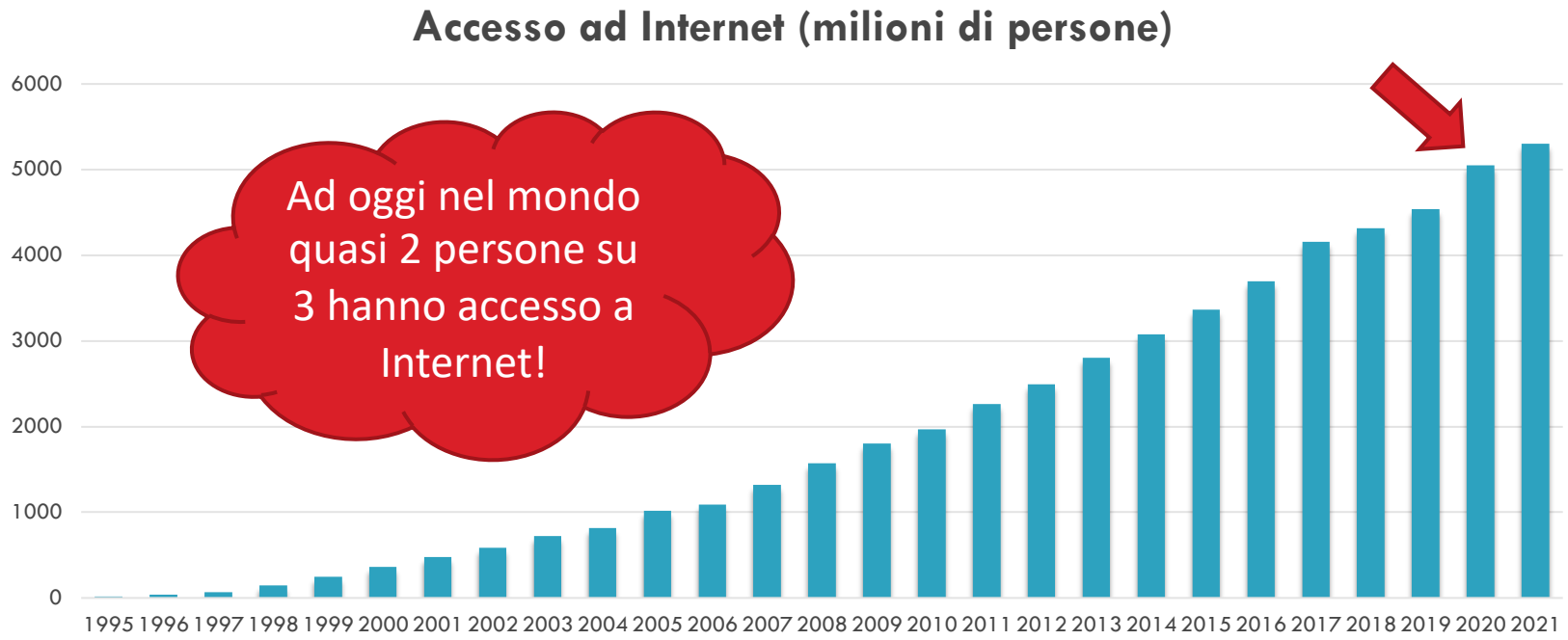
Cyberspace

- … e Luciano Floridi l'*infosfera*

Cyberspace -- Potenzialità

- Ci consente di:
  - comunicare e interagire dovunque, in ogni momento
  - svolgere un maggior numero di attività per unità di tempo
  - memorizzare e gestire maggiori quantità di dati
  - superare le barriere spazio-temporali (frontiere comprese)

Quanto cresce internet nel mondo?



[Nunzia CIARDI,
Vicedirettrice Generale ACN - Agenzia per la Cybersicurezza Nazionale]

L’uso della tecnologia in Italia

nel **2009** in relazione alla popolazione:

solo il **15%** utilizzava smartphone

[Nunzia CIARDI,
Vicedirettrice Generale ACN - Agenzia per la Cybersicurezza Nazionale]

L’uso della tecnologia in Italia

nel **2009** in relazione alla popolazione:

solo il **15%** utilizzava smartphone

nel **2022** in relazione alla popolazione:

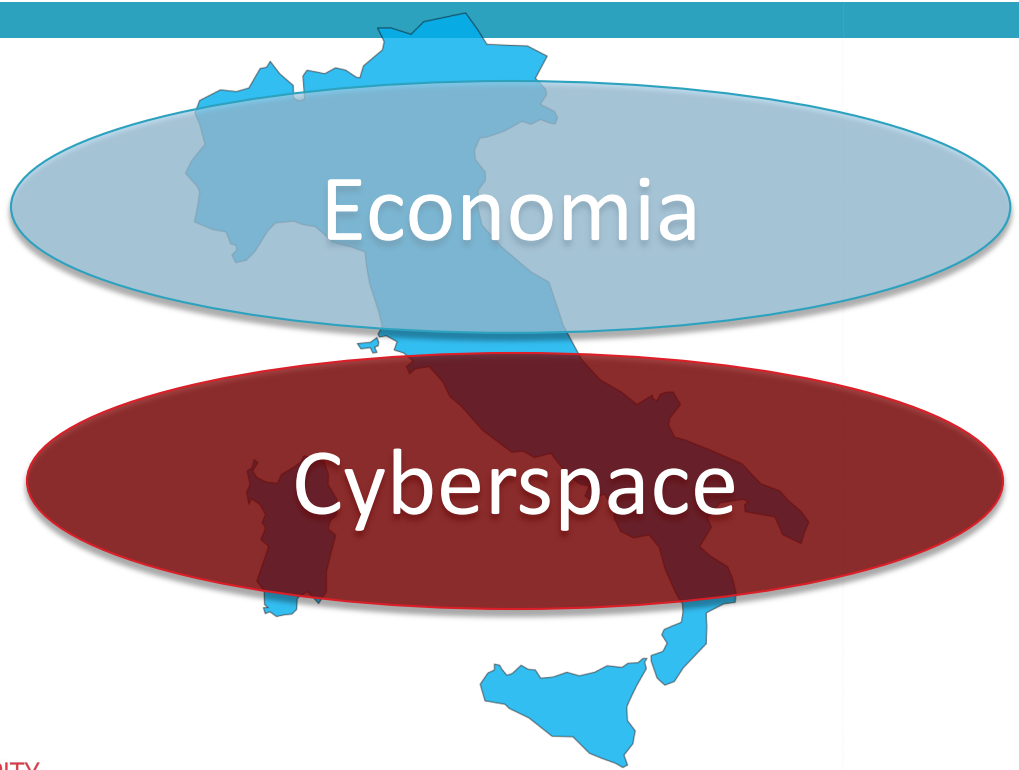
129,7% ha un dispositivo mobile connesso

84,3% utilizza internet

71,6% utilizza i social media

[Nunzia CIARDI,
Vicedirettrice Generale CAN - Agenzia per la Cybersicurezza Nazionale]

Cyberspace -- Impatto



Cyberspace -- Complessità

- La cosa *più complessa* che l'uomo abbia mai costruito:

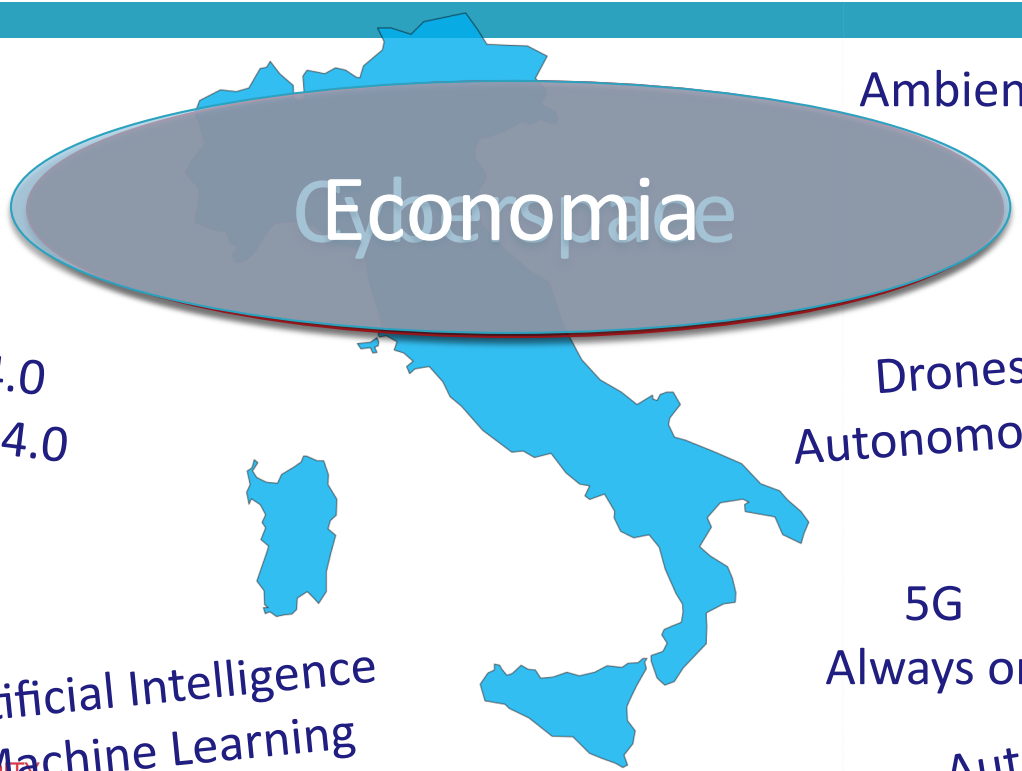
Cyberspace -- Complessità

- La cosa *più complessa* che l'uomo abbia mai costruito:
  - unione di migliaia di reti
  - stratificazione di programmi software e protocolli
  - eterogeneità di apparati e terminali

Cyberspace -- Complessità

- La cosa *più complessa* che l'uomo abbia mai costruito:
  - unione di migliaia di reti
  - stratificazione di programmi software e protocolli
  - eterogeneità di apparati e terminali
  - Internet pensata come strumento di collaborazione *friendly* e con servizi *best-effort*
  - …

Cyberspace -- Pervasività



Ambient Assisted Living

IoT, IoE,
IIoT

Wearable devices
IoMT

Industry 4.0
Agricolture 4.0

Drones – UAV
Autonomous Vehicles

Smart-*

Robotics

Crypto Currencies

5G
Always on

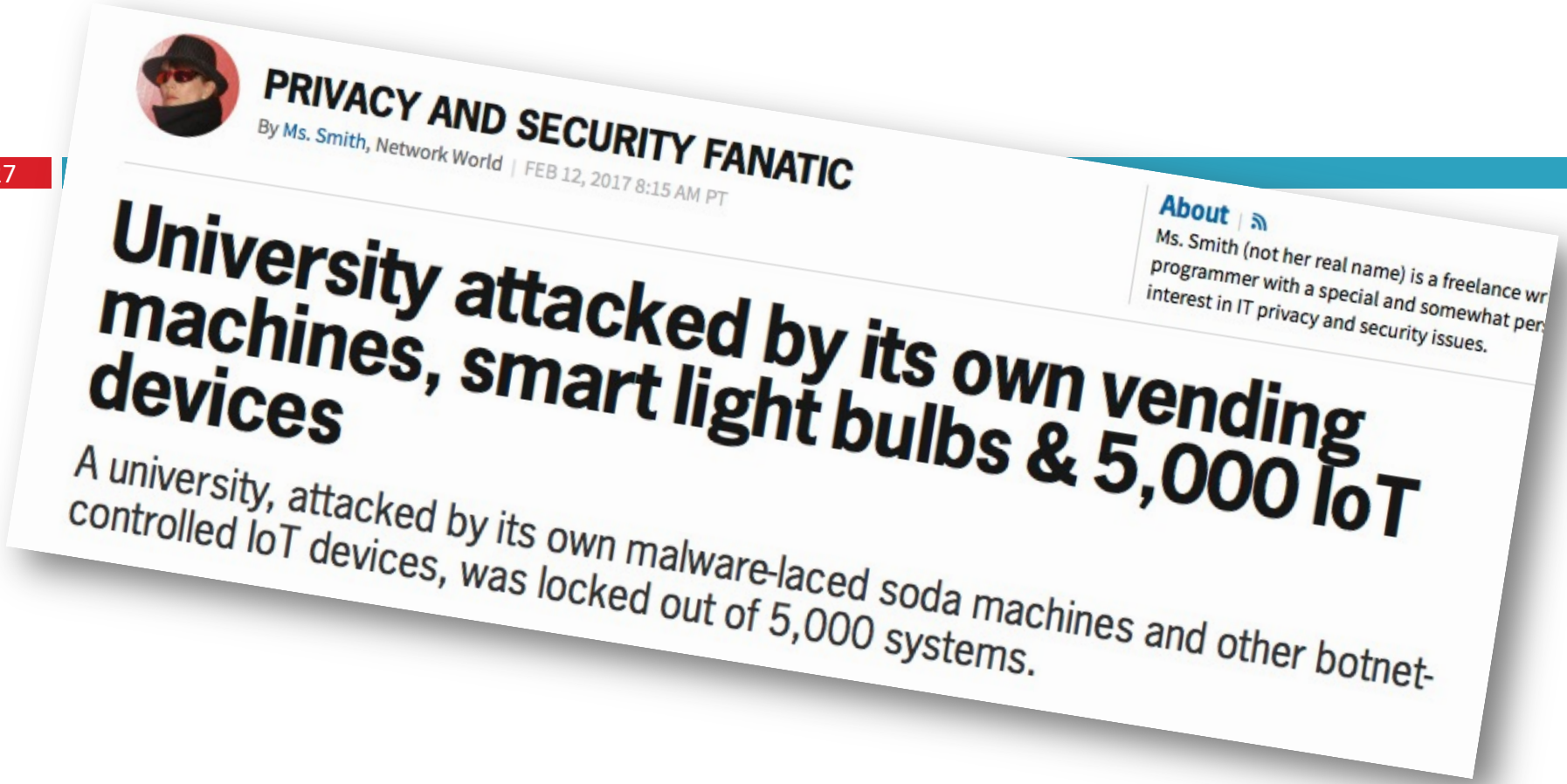
Artificial Intelligence
Machine Learning

Autonomous Weapon Systems

Conseguenze

- Incredibile aumento della *superficie di attacco*

Alcuni esempi “sintomatici”



PRIVACY AND SECURITY FANATIC

By Ms. Smith, Network World | FEB 12, 2017 8:15 AM PT

University attacked by its own vending machines, smart light bulbs & 5,000 IoT devices

A university, attacked by its own malware-laced soda machines and other botnet-controlled IoT devices, was locked out of 5,000 systems.

About

Ms. Smith (not her real name) is a freelance wr
programmer with a special and somewhat per
interest in IT privacy and security issues.


CloudPets
THE INTERNET OF HACKABLE THINGS
Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings
LORENZO FRANCESCHI-BICCHIERAI
Feb 27 2017, 10:00pm
A company that sells "smart" teddy bears leaked 800,000 user account credentials—and then hackers locked it and held it for ransom.
UPDATE, Feb. 28, 12:25 p.m. ET: After this story was published, a security researcher revealed that the stuffed animals themselves could easily be hacked

Attack on surveillance cameras a warning over security, ethics

The attack on a video surveillance startup by a hacktivist group raises questions not just over cyber security, but the use and extent of surveillance technology

By **Alex Scroxton**, Security Editor

Published: **11 Mar 2021 11:30**

A cyber attack on video surveillance startup Verkada that has seen around 150,000 video cameras, many of them in secure locations, compromised by a hacktivist collective, is prompting warnings both around basic security hygiene, and the ethics of surveillance technology.

Perché ??

Perché ??


"If everything is connected,
everything can be hacked."
— Ursula von der Leyen, President of the European Commission,
in her 2021 State of the Union Address on Sept. 15, 2021

Perché ??

Qualsiasi "cosa" connessa a Internet può essere attaccata…

… e lo sarà certamente …

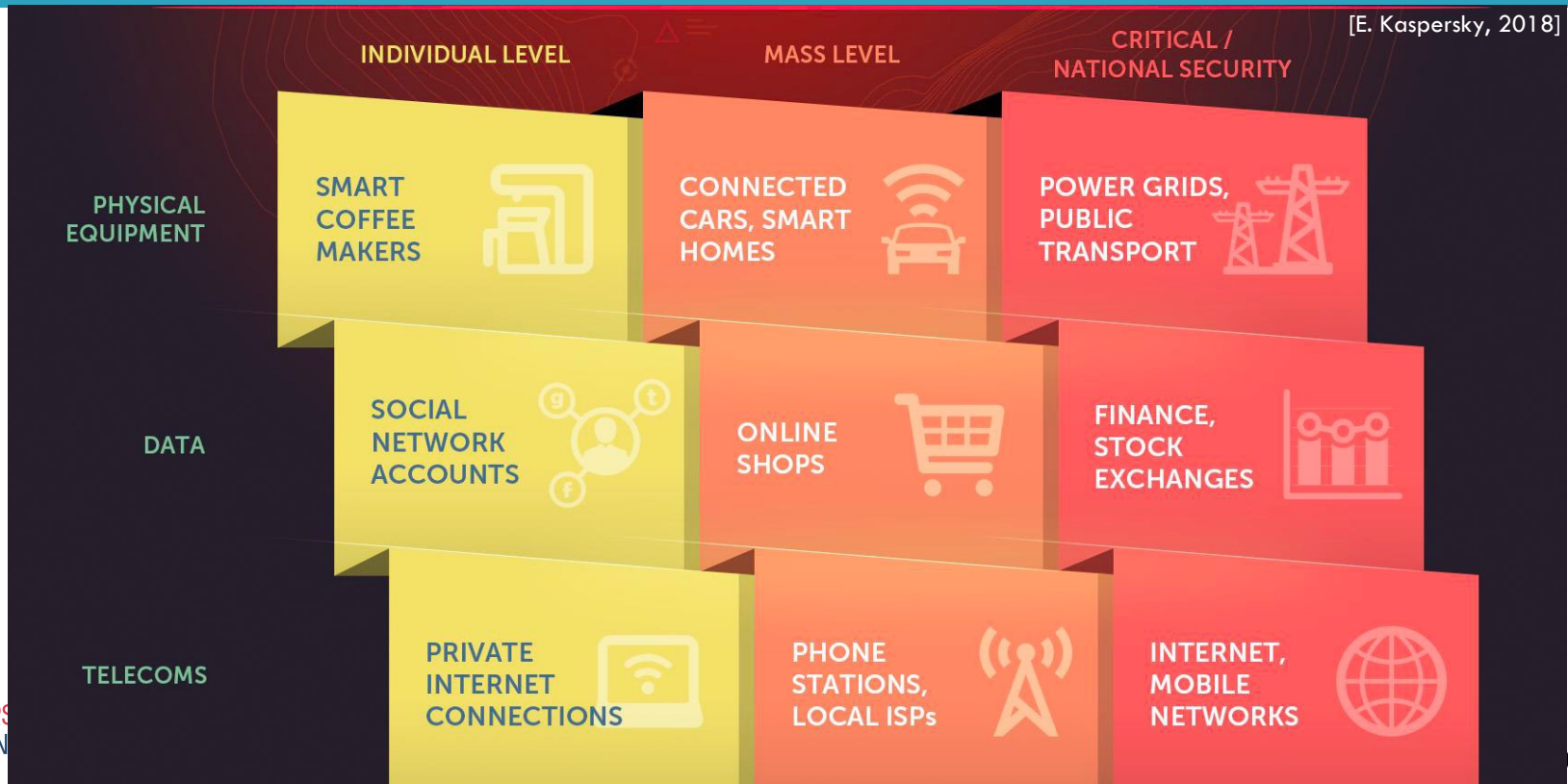
ualsiasi “cosa” connessa
a Internet può essere
attaccata…

… e lo s

Non SE,
ma QUANDO …

osa" connessa
può essere
ccata…

Tutto è sotto attacco



… sempre …

- *Cyber Attack Map*: mappe in tempo reale:
  - https://threatmap.checkpoint.com
  - https://cybermap.kaspersky.com
  - …
- Le più popolari sono riassunte qui:
  - https://norse-corp.com/map/

Check Point
SOFTWARE TECHNOLOGIES LTD.
THREATCLOUD

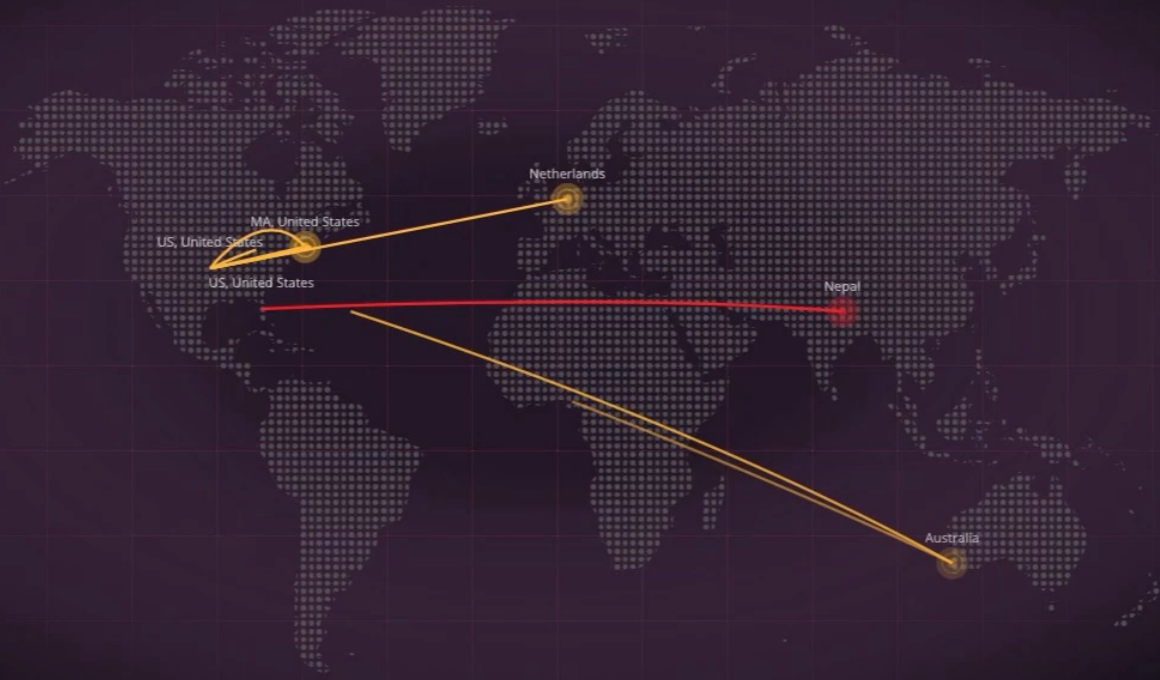
LIVE CYBER THREAT MAP

24,968,652 ATTACKS ON THIS DAY

RECENT DAILY ATTACKS

ATTACKS Current rate − 4 +

- Content Protection Violation
  17:22:53 US, United States → Netherlands
- Content Protection Violation
  17:22:52 US, United States → MA, United S...
- Content Protection Violation
  17:22:52 US, United States → MA, United S...
- Content Protection Violation
  17:22:52 US, United States → MA, United S...
- Content Protection Violation
  17:22:52 US, United States → MA, United S...
- Content Protection Violation
  17:22:51 US, United States → Netherlands
- REP.TC.abemqb
  17:22:51 US, United States → Nepal



Malware Phishing Exploit

TOP TARGETED COUNTRIES

Highest rate of attacks per organization in the last day.

- Nepal
- Mongolia
- Georgia
- Bolivia
- Indonesia

TOP TARGETED INDUSTRIES

Highest rate of attacks per organization in the last day.

- Education
- Government
- ISP/MSP

TOP MALWARE TYPES

Malware types with the highest global impact in the last day.

- Botnet
- Phishing
- Backdoor

Classificazione

- Le organizzazioni e le aziende si dividono in 2 categorie:

Classificazione

- Le organizzazioni e le aziende si dividono in 2 categorie:

  Quelle che sono state attaccate

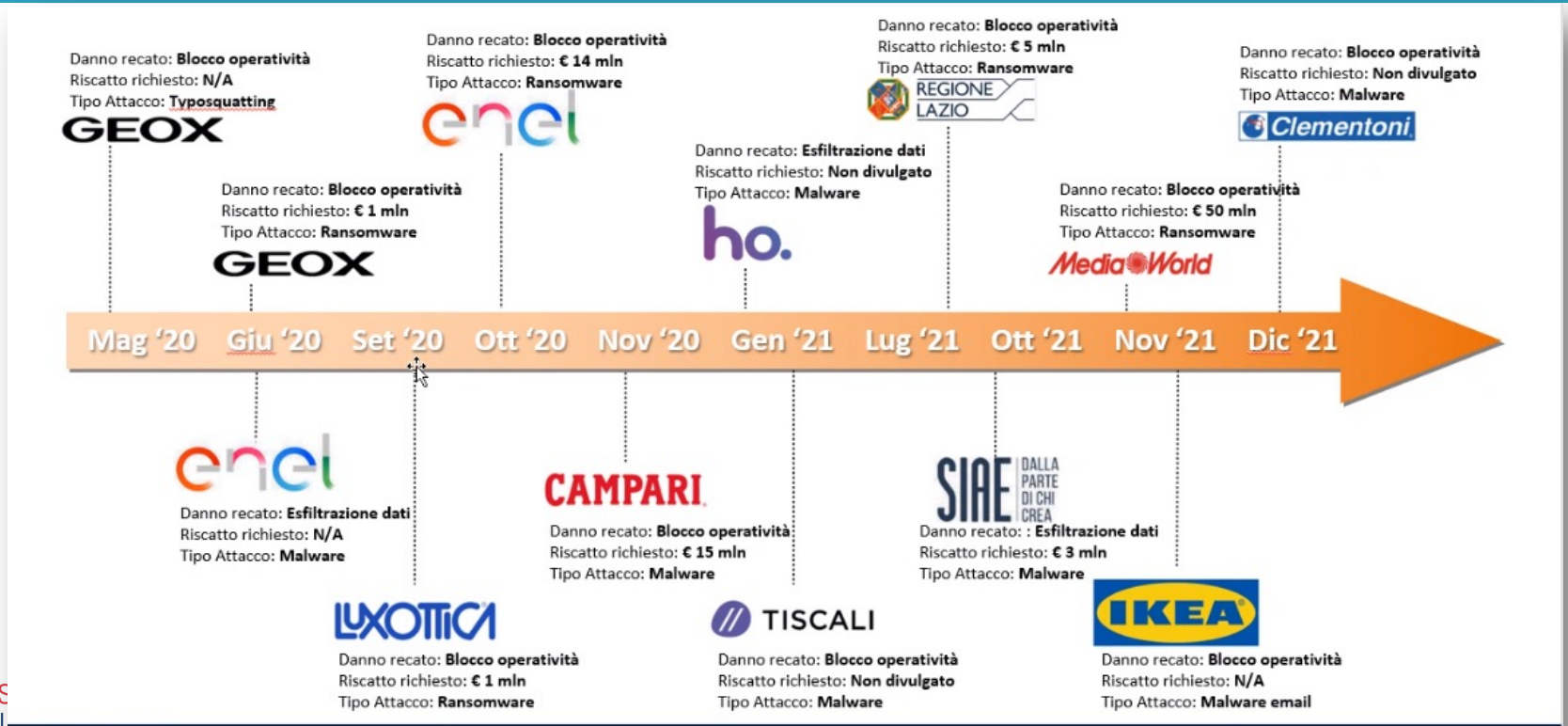
Classificazione

- Le organizzazioni e le aziende si dividono in 2 categorie:

Quelle che sono state attaccate

Quelle che non sanno di essere state attaccate

Alcuni attacchi significativi



In Italia

- *“Il numero di attacchi infomatici in Italia nei primi 6 mesi del 2020 (lockdown, etc) è aumentato del 389% rispetto ai corrispondenti 6 mesi del 2019”*

[Gen. Nunzia CIARDI – Direttrice del Servizio Polizia Postale e delle Comunicazioni -- attualmente Vice-direttrice generale ACN]

L’impatto del Covid-19

- Il Keynote Speech della Gen. Nunzia CIARDI alla conferenza ITASEC21 sull’*Epidemia da Covid-19 e il suo impatto sugli scenari del cybercrime* è scaricabile a questo indirizzo:
  - https://2021.itasec.it/stakeholder-space/keynote-speech-nunzia-ciardi-epidemia-covid19-cybercrime/

L'impatto del Covid-19

- Il Keynote
  conferenz
  suo impat
  a questo ir
  - https://20
    nunzia-cia

Keynote Speech Nunzia CIARDI
L'Epidemia da Covid-19 ed il suo impatto sugli scenari del cybercrime

Session moderator: Sonia MONTEGIOVE

Cybersicurezza – Chi ne è toccato

- Un problema da affrontare a TUTTI i livelli:
  - *Individuo*
  - *Organizzazione*
  - *Sistema Paese*
  - *Sovranazionale*

Cybersicurezza – Chi ne è toccato

- Un problema da affrontare a TUTTI i livelli:
  - *Individuo*
  - *Organizzazione*
  - *Sistema Paese*
  - *Sovranazionale*
- I vari livelli saranno analizzati nel dettaglio nelle lezioni della sezione *CS_04 - Incremento della Resilienza*

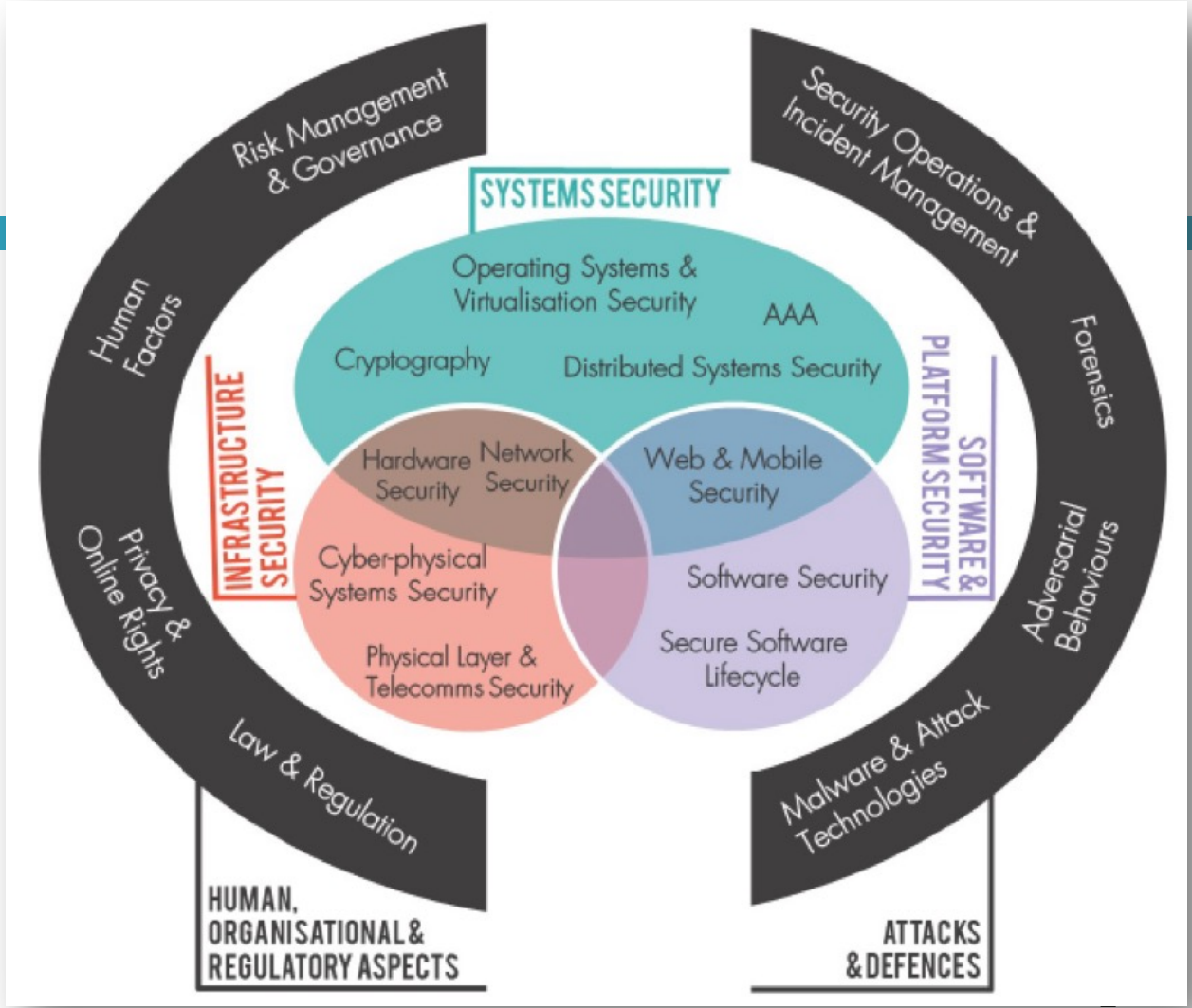
Cybersicurezza – Tassonomie

- La Cybersicurezza sta diventando un elemento importante nella vita quotidiana
- Tuttavia, le conoscenze fondamentali su cui si sta sviluppando sono frammentate e, di conseguenza, può essere difficile raccapezzarcisi.
- Alcune tassonomie particolarmente rilevanti sono riassunte nell'Approfindimento #2

The Cyber Security Body of Knowledge (CyBOK)

- Una tassonomia particolarmente valida è quella presentata in
  - CyBOK Version Version 1.1.0 - 31st July 2021, https://www.cybok.org/

CyBOK: categorie



Cybersicurezza – Glossari

- Alcuni Glossari particolarmente rilevanti sono presentati nell'Approfondimento #3.

Cybersicurezza – Carenza di forza lavoro

[https://cyber-nyc.com]

Cybersicurezza – Carenza di forza lavoro

[https://cyber-nyc.com]

Workforce shortage in EU

[https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy]

Paolo PRINETTO

Director
CINI Cybersecurity
National Lab

Paolo.Prinetto@polito.it
Paolo.Prinetto@imtlucca.it

Mob. +39 335 227529

CYBERSECURITY
NATIONAL LAB

https://cybersecnatlab.it

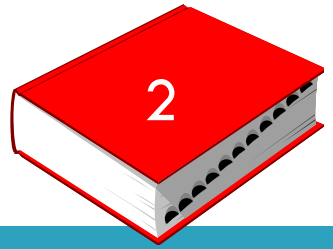
Approfondimento #1 – Definizioni addizionali di Cybersecurity

Cybersecurity

- Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

[CNSSI 4009-2015 (NSPD-54/HSPD-23)
NISTIR 7621 Rev. 1 under Cybersecurity (CNSSI 4009-2015)]

Cybersecurity



- The prevention of damage to, unauthorized use of, exploitation of, and - if needed - the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems.

[NISTIR 8074 Vol. 2 under Cybersecurity]

Cybersecurity

- The process of protecting information by preventing, detecting, and responding to attacks.

[NISTIR 8183 under Cybersecurity (Framework for Improving Critical Infrastructure Cybersecurity, version 1.0]

Cybersecurity

- Refers to the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.

[HM Government, UK, “National cyber security strategy 2016–2021,” 2016. https://www.gov.uk/government/publications/national-cyber-security- strategy-2016-to-2021]

Approfondimento #2 – Tassonomie della Cybersicurezza

Tassonomie della Cybersicurezza

- Tra le tassonomie più rilevani vanno ricordate:
  - *The Cyber Security Body of Knowledge (CyBOK)*
  - *The European Cybersecurity Centres of Expertise Map*
  - *ENISA Research Directions for Digital Strategic Autonomy*

Tassonomie della Cybersicurezza

- Tra le tassonomie più rilevani vanno ricordate:
  - *The Cyber Security Body of Knowledge (CyBOK)*
  - *The European Cybersecurity Centres of Expertise Map*
  - *ENISA Research Directions for Digital Strategic Autonomy*

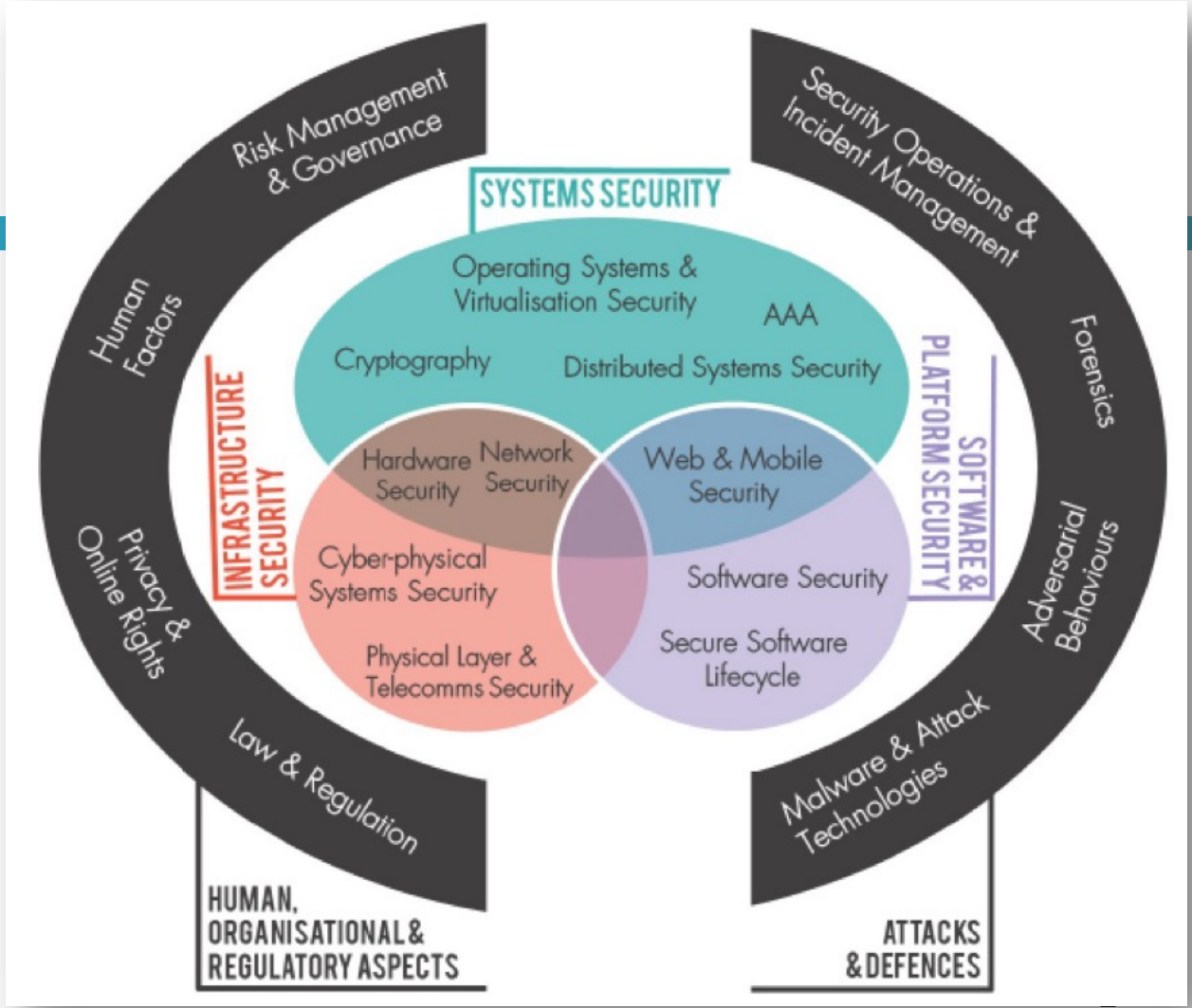
The Cyber Security Body of Knowledge (CyBOK)

- Una tassonomia particolarmente valida è quella presentata in
  - CyBOK Version Version 1.1.0 - 31st July 2021, https://www.cybok.org/

The Cyber Security Body of Knowledge (CyBOK)

- Il CyBOK è suddiviso in 19 aree di conoscenza di alto livello (Knowledge Areas), raggruppate in 5 categorie:
  - *Human, Organisational, and Regulatory Aspects*
  - *Attacks and Defences*
  - *Systems Security*
  - *Software and Platform Security*
  - *Infrastructure Security*

CyBOK: categorie



The Cyber Security Body of Knowledge (CyBOK)

- Il CyBOK è suddiviso in 19 aree di conoscenza di alto livello (Knowledge Areas), raggruppate in 5 categorie:
  - *Human, Organisational, and Regulatory Aspects*
  - *Attacks and Defences*
  - *Systems Security*
  - *Software and Platform Security*
  - *Infrastructure Security*

CyBOK Categories

	Human, Organisational, and Regulatory Aspects
Risk Management & Governance	Security management systems and organisational security controls, including standards, best practices, and approaches to risk assessment and mitigation.
Law & Regulation	International and national statutory and regulatory requirements, compliance obligations, and security ethics, including data protection and developing doctrines on cyber warfare.
Human Factors	Usable security, social & behavioural factors impacting security, security culture and awareness as well as the impact of security controls on user behaviours.
Privacy & Online Rights	Techniques for protecting personal information, including communications, applications, and inferences from databases and data processing. It also includes other systems supporting online rights touching on censorship and circumvention, covertness, electronic elections, and privacy in payment and identity systems.

Go to page 45

CyBOK Categories

Attacks and Defences	
Malware & Attack Technologies	Technical details of exploits and distributed malicious systems, together with associated discovery and analysis approaches.
Adversarial Behaviours	The motivations, behaviours, & methods used by attackers, including malware supply chains, attack vectors, and money transfers.
Security Operations & Incident Management	The configuration, operation and maintenance of secure systems including the detection of and response to security incidents and the collection and use of threat intelligence.
Forensics	The collection, analysis, & reporting of digital evidence in support of incidents or criminal events.

CyBOK Categories

Systems Security	
Cryptography	Core primitives of cryptography as presently practised & emerging algorithms, techniques for analysis of these, and the protocols that use them.
Operating Systems & Virtualisation Security	Operating systems protection mechanisms, implementing secure abstraction of hardware, and sharing of resources, including isolation in multiuser systems, secure virtualisation, and security in database systems.
Distributed Systems Security	Security mechanisms relating to larger-scale coordinated distributed systems, including aspects of secure consensus, time, event systems, peer-to-peer systems, clouds, multitenant data centres, & distributed ledgers.
Authentication, Authorisation, & Accountability	All aspects of identity management and authentication technologies, and architectures and tools to support authorisation and accountability in both isolated and distributed systems.

CyBOK Categories

	Software and Platform Security
Software Security	Known categories of programming errors resulting in security bugs, & techniques for avoiding these errors—both through coding practice and improved language design—and tools, techniques, and methods for detection of such errors in existing systems.
Web & Mobile Security	Issues related to web applications and services distributed across devices and frameworks, including the diverse programming paradigms and protection models.
Secure Software Lifecycle	The application of security software engineering techniques in the whole systems development lifecycle resulting in software that is secure by default.

CyBOK Categories

	Infrastructure Security
Network Security	Security aspects of networking & telecommunication protocols, including the security of routing, network security elements, and specific cryptographic protocols used for network security.
Hardware Security	Security in the design, implementation, & deployment of general-purpose and specialist hardware, including trusted computing technologies and sources of randomness.
Cyber-Physical Systems Security	Security challenges in cyber-physical systems, such as the Internet of Things & industrial control systems, attacker models, safe-secure designs, and security of large-scale infrastructures.
Physical Layer & Telecommunications Security	Security concerns and limitations of the physical layer including aspects of radio frequency encodings and transmission techniques, unintended radiation, and interference.

Tassonomie della Cybersicurezza

- Tra le tassonomie più rilevani vanno ricordate:
  - *The Cyber Security Body of Knowledge (CyBOK)*
  - *The European Cybersecurity Centres of Expertise Map*
  - *ENISA Research Directions for Digital Strategic Autonomy*

- [https://publications.jrc.ec.europa.eu/repository/handle/JRC111441]

Tassonomie della Cybersicurezza

- Tra le tassonomie più rilevani vanno ricordate:
  - *The Cyber Security Body of Knowledge (CyBOK)*
  - *The European Cybersecurity Centres of Expertise Map*
  - *ENISA Research Directions for Digital Strategic Autonomy*

- [https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy]

Approfondimento #3 – Glossari della Cybersicurezza

NIST

https://csrc.nist.gov/Glossary]

DIS

[https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/04/Cyberbook.pdf]

DIS


SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA
a protezione degli interessi politici, militari, economici, scientifici ed industriali dell'Italia
CHI SIAMO
COSA FACCIAMO
CULTURA DELLA SICUREZZA
IL MONDO DELL'INTELLIGENCE
PER LE IMPRESE
DOCUMENTAZIONE
COMUNICAZIONE
Home » Archivio notizie » Nuova edizione del Glossario intelligence
Nuova edizione del Glossario intelligence
13 Giugno 2019
GLOSSARIO
Intelligence
Il Glossario intelligence (ed. aggiornata – PDF 1,1 MB)
Scarica
Documenti
» Il Glossario intelligence (ed. aggiornata – PDF 1,1 MB)
Articoli recenti
» Geodiritto e Intelligence, la forza del Nomos
» Sicurezza Nazionale e Cybersecurity
» Cyber: collaborazione tra Intelligenc Forze di Polizia e Forze Armate
» Cyber Security: avvio delle attività CSIRT
» CSIRT: al via i lavori del team p notifiche e la gestione degli in


CYBERBOOK
Il glossario di sicurezza cibernetica
www.sicurezzanazionale.gov.it
www.beaware bedigital.gov.it

azio

04/C