Cybersecurity

«come difendersi dai pericoli del Web»

Centro Bartolomeo Garelli – 14 maggio2024

Umberto Torelli - ***Corriere della Sera***

la domanda è

Le 3+1 evoluzioni (rivoluzioni) di Internet

Web 1.0 ***-*** *Internet dei* ***computer*** *(1990-2000)*

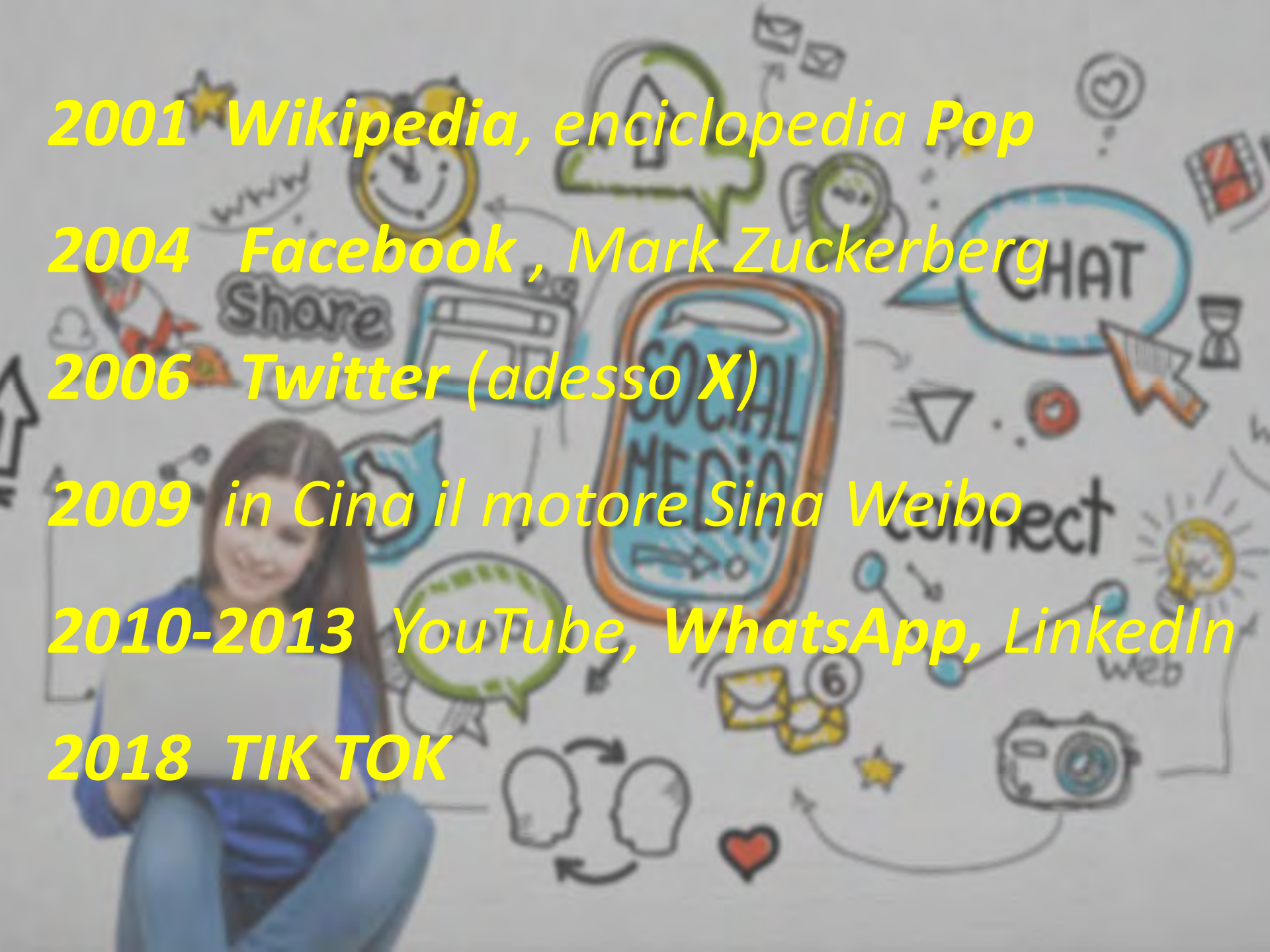
Web 2.0 ***-*** *Internet delle* ***persone*** *(2000-2010)*

Web 3.0 ***-*** *Internet delle* ***cose*** *(2010-2020)*

Intelligenza Artificiale (AI) *(dal 2020 a domani)*

Web 1.0 *- Internet dei* ***computer***

Web 2.0 *- Internet delle* ***Persone***
*nasce il mondo «**Social**»*



2001 Wikipedia**, enciclopedia **Pop

***2004 Facebook**, Mark Zuckerberg*

***2006 Twitter** (adesso **X**)*

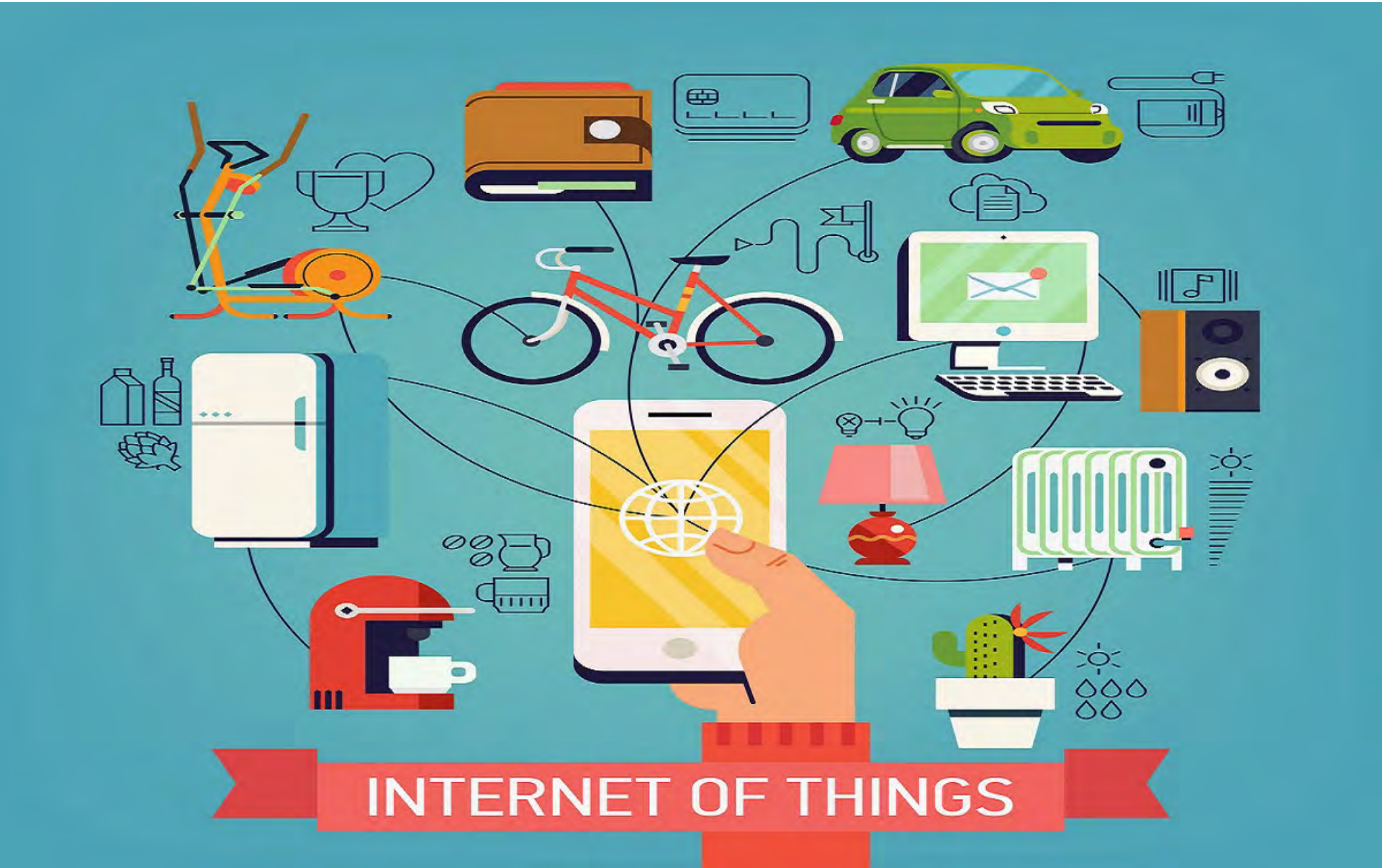
***2009** in Cina il motore Sina Weibo*

***2010-2013** YouTube, **WhatsApp**, LinkedIn*

2018 TIK TOK

WEB 3.0 Internet of Things (Iot)

«la nuova era digitale»



***Iot**: «come cambia il mondo»*

*«tutti **taggati** nello IoT»*

*ma tutto questo ha un prezzo: «la **SECURITY**»*

il «bidet rosa» di Alexa e Siri

Social + App: *«porte aperte ai pericoli del Web»*


spoofing
TROJAN
Spam
Phishing
Ransomware

e il nuovo paradigma ***«dell'Internet of me»***

il risultato di questa ***abboffata*** di dati?

- seminiamo il Web *con informazioni personali, foto, filmati, indirizzi, appuntamenti,*

- ma anche transazioni di ecommerce e home banking

- senza renderci conto che la tracce digitali rimangono per sempre nel ***cloud****, ahimè* ***anche da morti***

così ci comportiamo come ***Pollicino***
che lascia le tracce nel bosco

*un **video** vale più di mille parole*

l'iceberg del Web

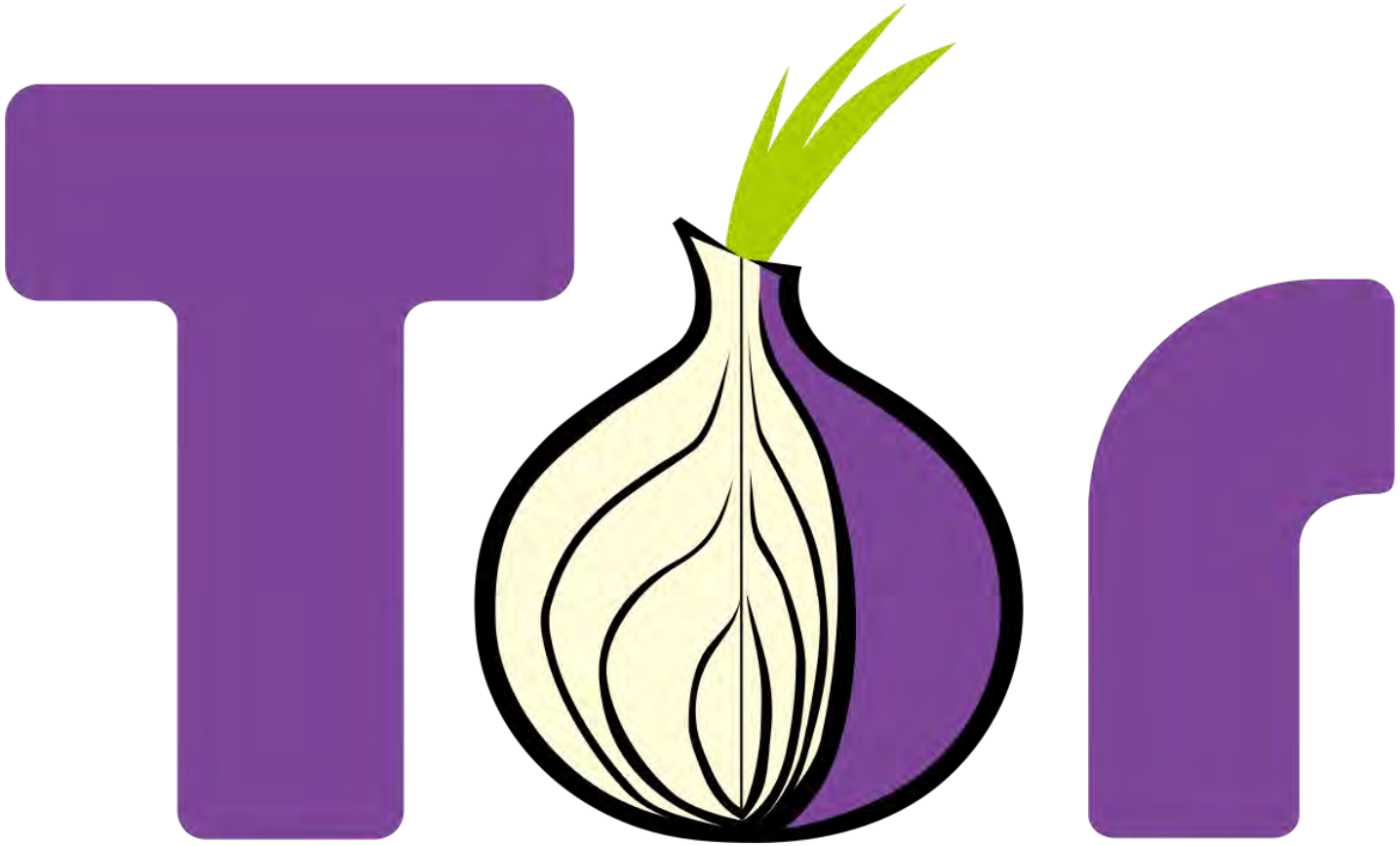
*le **tre** Web-zone*

***SURFACE WEB (4%)**: circa **2 miliardi** di siti in chiaro, consultabili con browser su computer e telefonini*

***DEEP WEB (90%):** siti **non visibili**, per accedere ai dati occorrono password, accessi riservati, identificazioni personali etc etc*

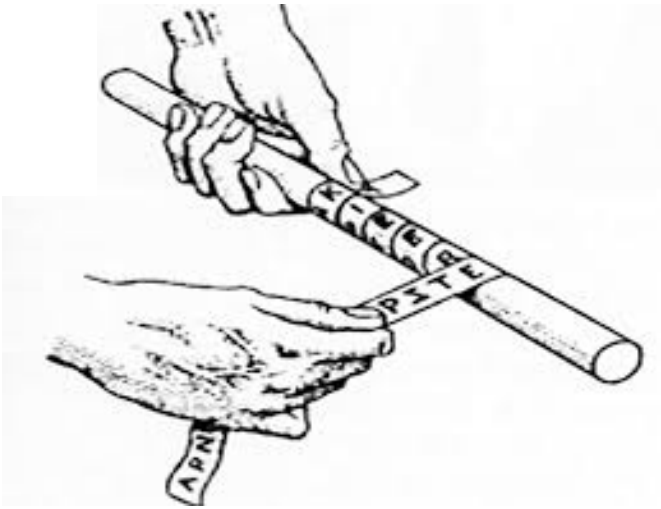
***DARK WEB (6%)**: la **parte oscura** di Internet, con vendita di armi, siti terroristici e pedopornografici, inaccessibile senza software dedicati*

*come si **naviga** nel Dark-Web?*
The Onion Router

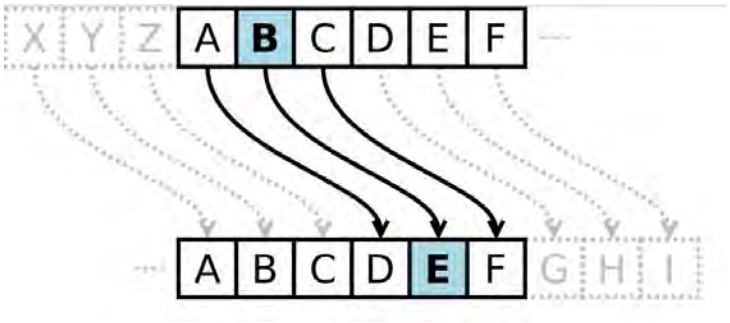


DIFESA 1

Crittografia: *«l'arte della scrittura nascosta»*



Crittografia: «l'arte della scrittura nascosta»



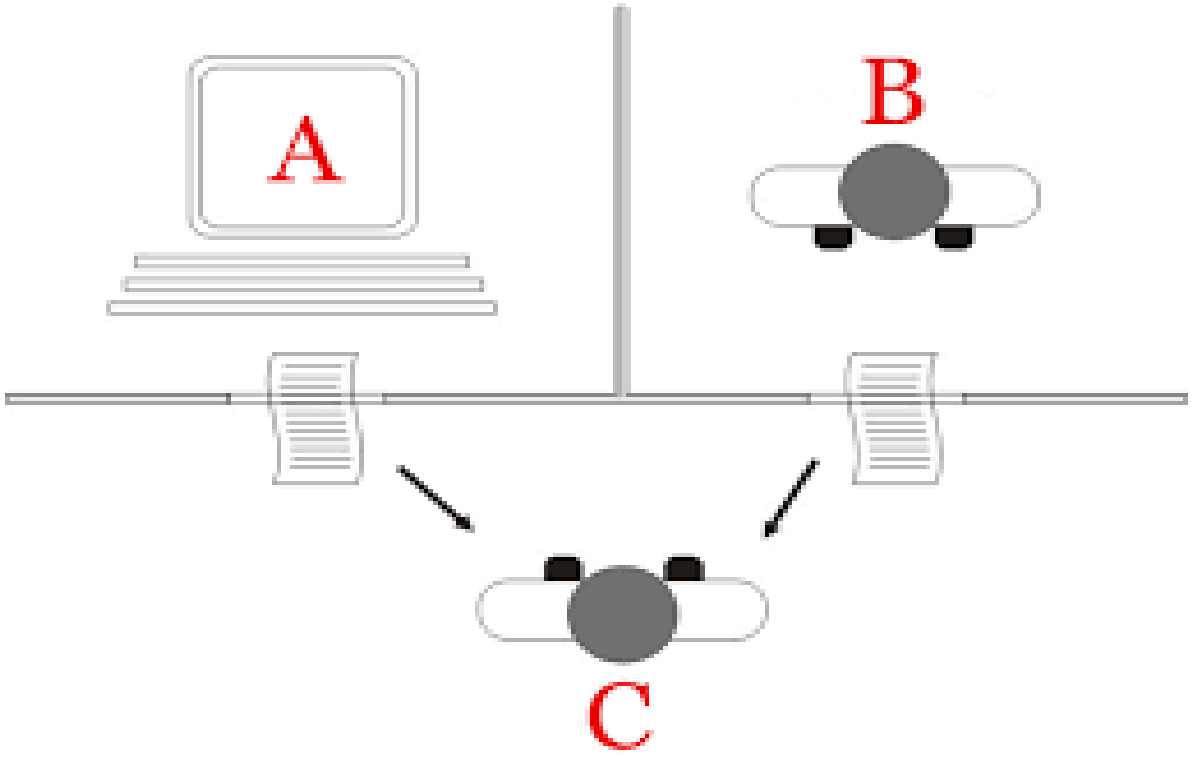
	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X
A	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X
B	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	A
C	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	A	B
D	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	A	B	C
E	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	A	B	C	D
F	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	A	B	C	D	E
G	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	A	B	C	D	E	F
H	H	I	L	M	N	O	P	Q	R	S	T	V	X	A	B	C	D	E	F	G
I	I	L	M	N	O	P	Q	R	S	T	V	X	A	B	C	D	E	F	G	H
L	L	M	N	O	P	Q	R	S	T	V	X	A	B	C	D	E	F	G	H	I
M	M	N	O	P	Q	R	S	T	V	X	A	B	C	D	E	F	G	H	I	L
N	N	O	P	Q	R	S	T	V	X	A	B	C	D	E	F	G	H	I	L	M
O	O	P	Q	R	S	T	V	X	A	B	C	D	E	F	G	H	I	L	M	N
P	P	Q	R	S	T	V	X	A	B	C	D	E	F	G	H	I	L	M	N	O
Q	Q	R	S	T	V	X	A	B	C	D	E	F	G	H	I	L	M	N	O	P
R	R	S	T	V	X	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q
S	S	T	V	X	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R
T	T	V	X	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S
V	V	X	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T
X	X	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V

Alan Turing & Enigma

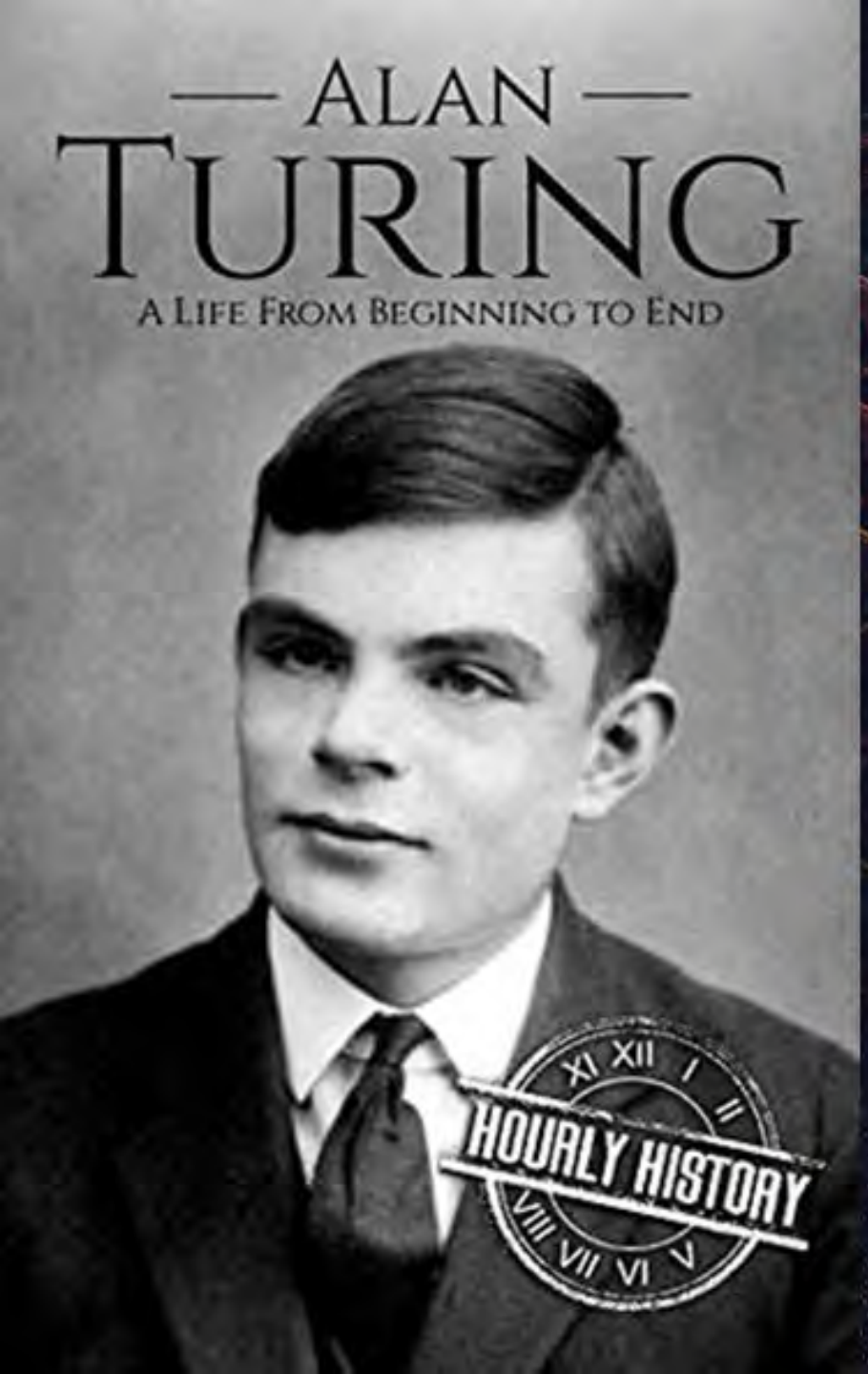
ALAN TURING

(1912-1954) matematico e crittografo tra i padri del computer, durante la Seconda Guerra Mondiale decifrò ***Enigma***. Ma nel 1954 venne condannato per omosessualità e si suicidò. Fu lui ad avere ideato l'omonimo Test

Test di Turing



l'uomo C pone le stesse domande ad A e B.
C sarà in grado di stabilire chi è il computer?


ALAN
TURING
A LIFE FROM BEGINNING TO END
HOURLY HISTORY


"THE BEST BRITISH FILM OF THE YEAR"
★★★★★
THE INDEPENDENT
BENEDICT CUMBERBATCH
KEIRA KNIGHTLEY
THE IMITATION GAME
2014
12
12
BASED ON THE INCREDIBLE TRUE STORY OF ALAN TURING
STUDIOCANAL

DIFESA 2

i cyber-poliziotti dei SOC

Security Operation Center

Bratislava – 500 mila attacchi al giorno

Unità militare 74455 dell'ex KGB, conosciuta come Sandworm, formata da un collettivo di hacker

WANTED BY THE FBI

GRU HACKERS' DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS

Conspiracy to Commit an Offense Against the United States; False Registration of a Domain Name; Conspiracy to Commit Wire Fraud; Wire Fraud; Intentional Damage to Protected Computers; Aggravated Identity Theft

Yuriy Sergeyevich Andrienko

Sergey Vladimirovich Detistov

Pavel Valeryevich Frolov

Anatoliy Sergeyevich Kovalev

Artem Valeryevich Ochichenko

Petr Nikolayevich Pliskin

CAUTION

On October 15, 2020, a federal grand jury sitting in the Western District of Pennsylvania returned an indictment against six Russian military intelligence officers for their alleged roles in targeting and compromising computer systems worldwide, including those relating to critical infrastructure in Ukraine, a political campaign in France, and the country of Georgia; international victims of the "NotPetya" malware attacks (including critical infrastructure providers); and international victims associated with the 2018 Winter Olympic Games and investigations of nerve agent attacks that have been publicly attributed to the Russian government. The indictment charges the defendants, Yuriy Sergeyevich Andrienko, Sergey Vladimirovich Detistov, Pavel Valeryevich Frolov, Anatoliy Sergeyevich Kovalev, Artem Valeryevich Ochichenko, and Petr Nikolayevich Pliskin, with a computer hacking conspiracy intended to deploy destructive malware and take other disruptive actions, for the strategic benefit of Russia, through unauthorized access to victims' computers. The indictment also charges these defendants with false registration of a domain name, conspiracy to commit wire fraud, wire fraud, intentional damage to protected computers, aggravated identity theft, and aiding and abetting those crimes. The United States District Court for the Western District of Pennsylvania issued a federal arrest warrant for each of these defendants upon the grand jury's return of the indictment.

SHOULD BE CONSIDERED ARMED AND DANGEROUS, AN INTERNATIONAL FLIGHT RISK, AND AN ESCAPE RISK

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

www.fbi.gov

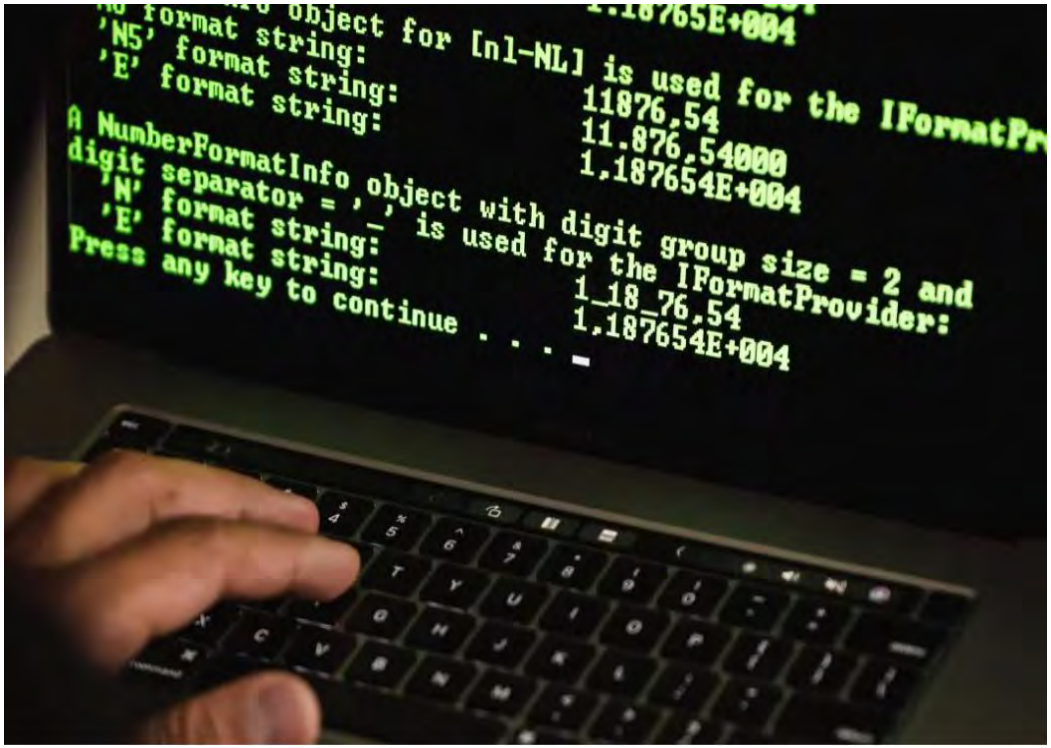
Sandworm

Telebots

/Voodoo Bear

GRU

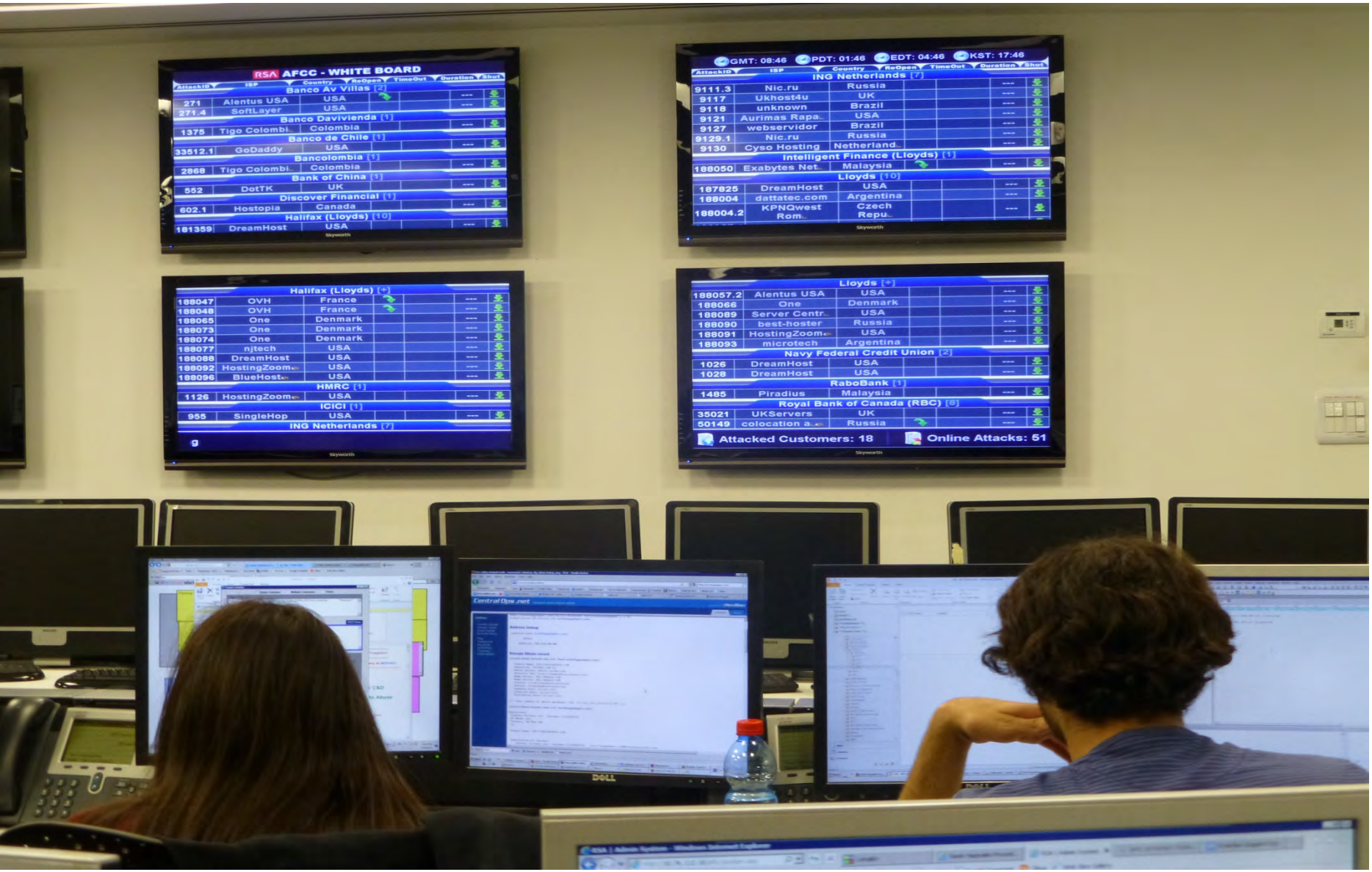
*Guerra digitale: «di recente il gruppo hacker russo **Noname57** attivo sulla propaganda pro-Putin ha violato siti istituzionali»*



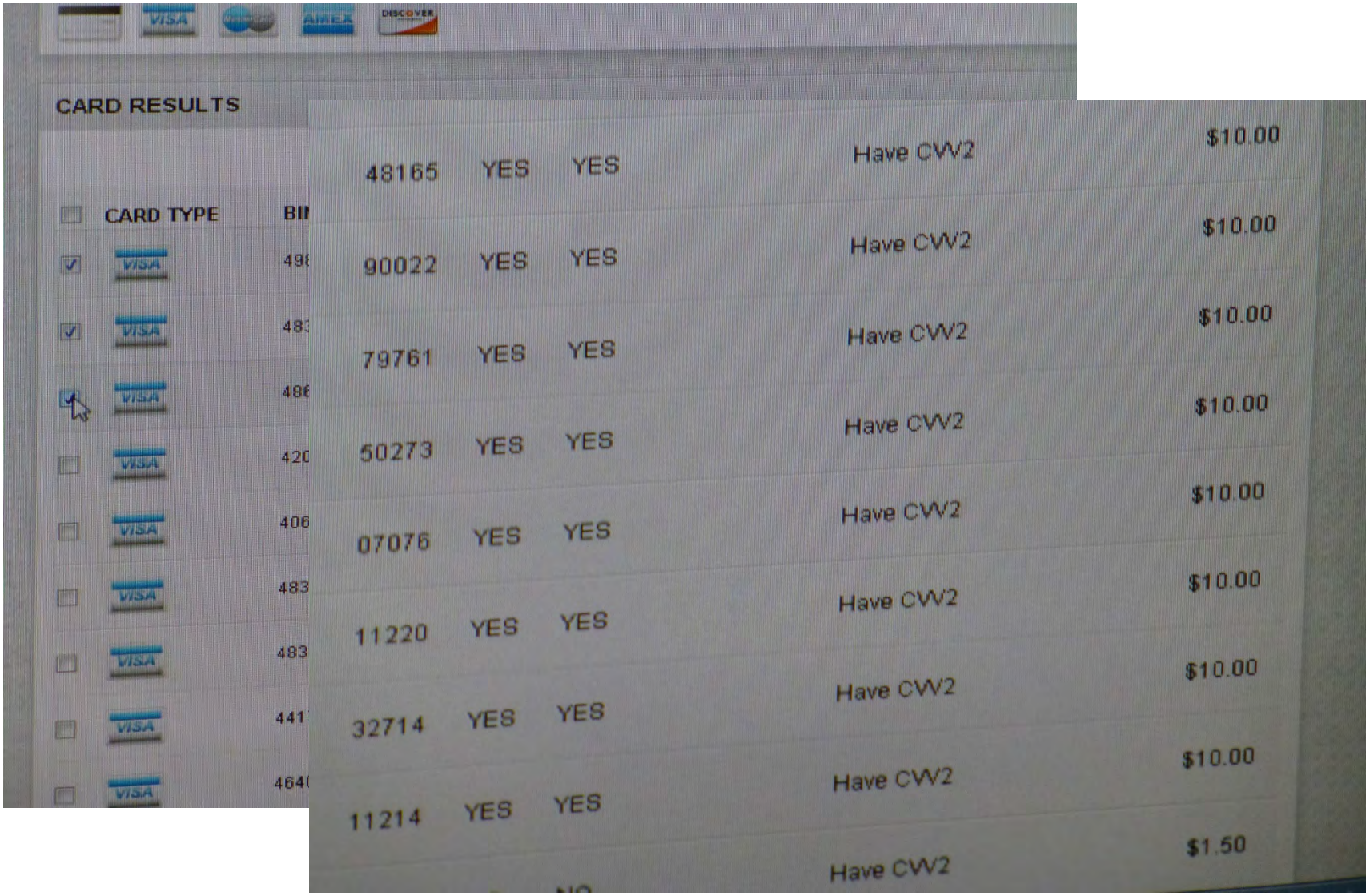
ministero Economia, Finanza e Infrastrutture

portale Gdf e dominio premier Meloni

cybersecurity in ambito ***geopolitico***



Credit Card Market



DIFESA 3


CINQUE REGOLE PER RICONOSCERE UN'EMAIL SOSPETTA
1 Codice fiscale errato su bollette, fatture e documenti bancari
2 Testo con la presenza di caratteri poco in uso come &, #, % e $
3 Email di banche, Poste ed enti con diverse gradazioni di colore
4 Link sospetti con nome accorciato
5 Indirizzo del mittente con dominio sbagliato
Web Mail
S.Franchino

& cinque consigli per combattere i cybercriminali

1) togliete la geolocalizzazione quando non serve

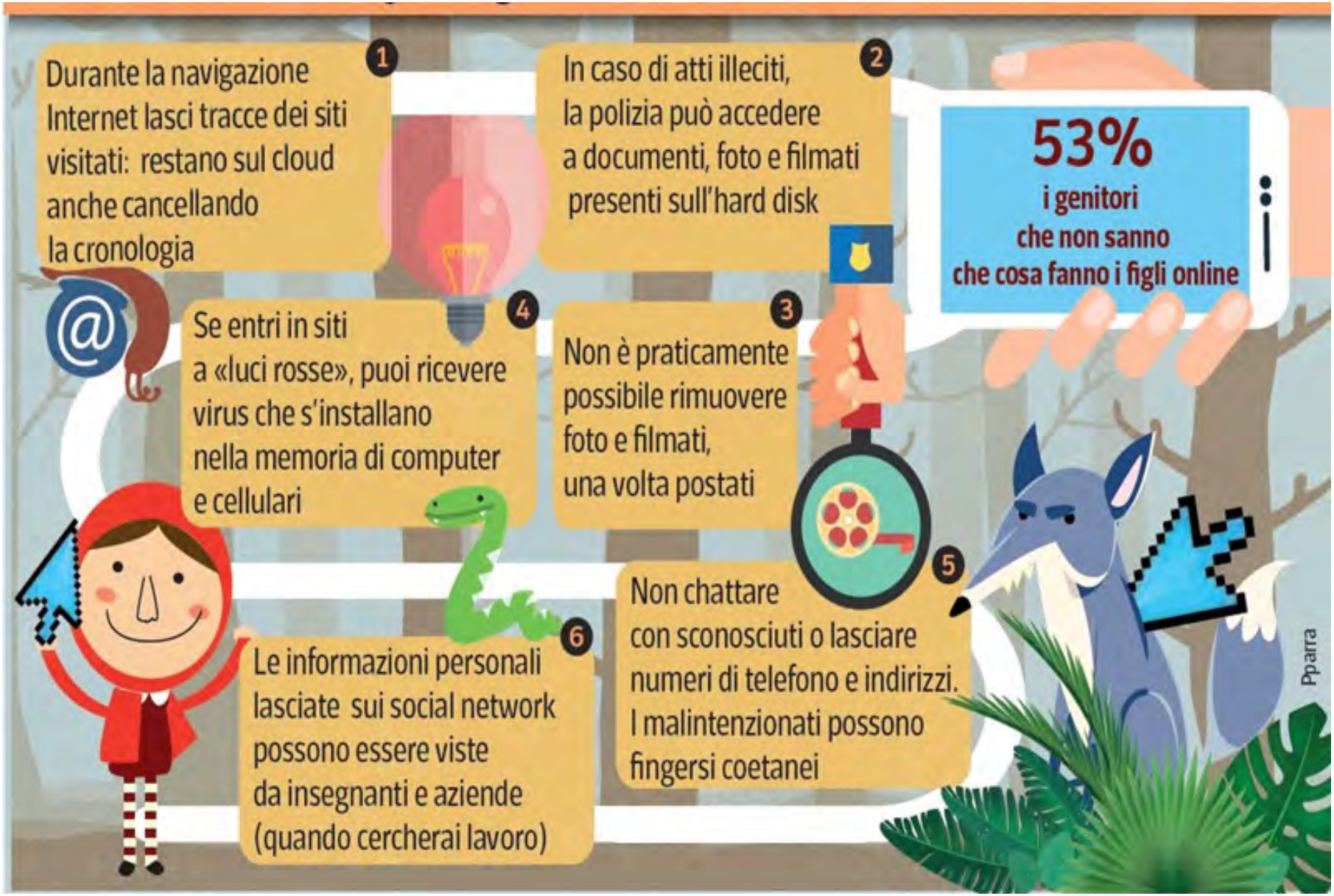
2) aggiornate sempre l'antivirus & fate un backup

3) acquisti online: «meglio usare carte prepagate»

4) ragazze: «niente tentazioni di foto intime sui Social»

5) mamme: «non mettete foto di minori in rete»

e per finire: ***«dovete sapere che…»***



www.UmbertoTorelli.com

è in arrivo «mobile personalizzato»

SENSING
Local content & service discovery

SEEING
Augmented reality UI
Map, 3D, in building navigation

INTERACTING
Connection manager

KNOWS
You and what is around you

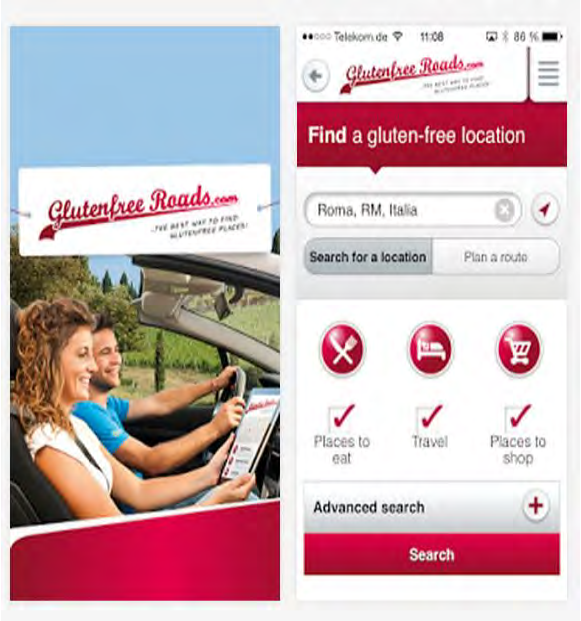
LEARNS
What you like

DISCOVERS
Things relevant to you

FILTERS
Out the irrelevant

quando le App catturano informazioni:
«un esempio che mi è capitato»

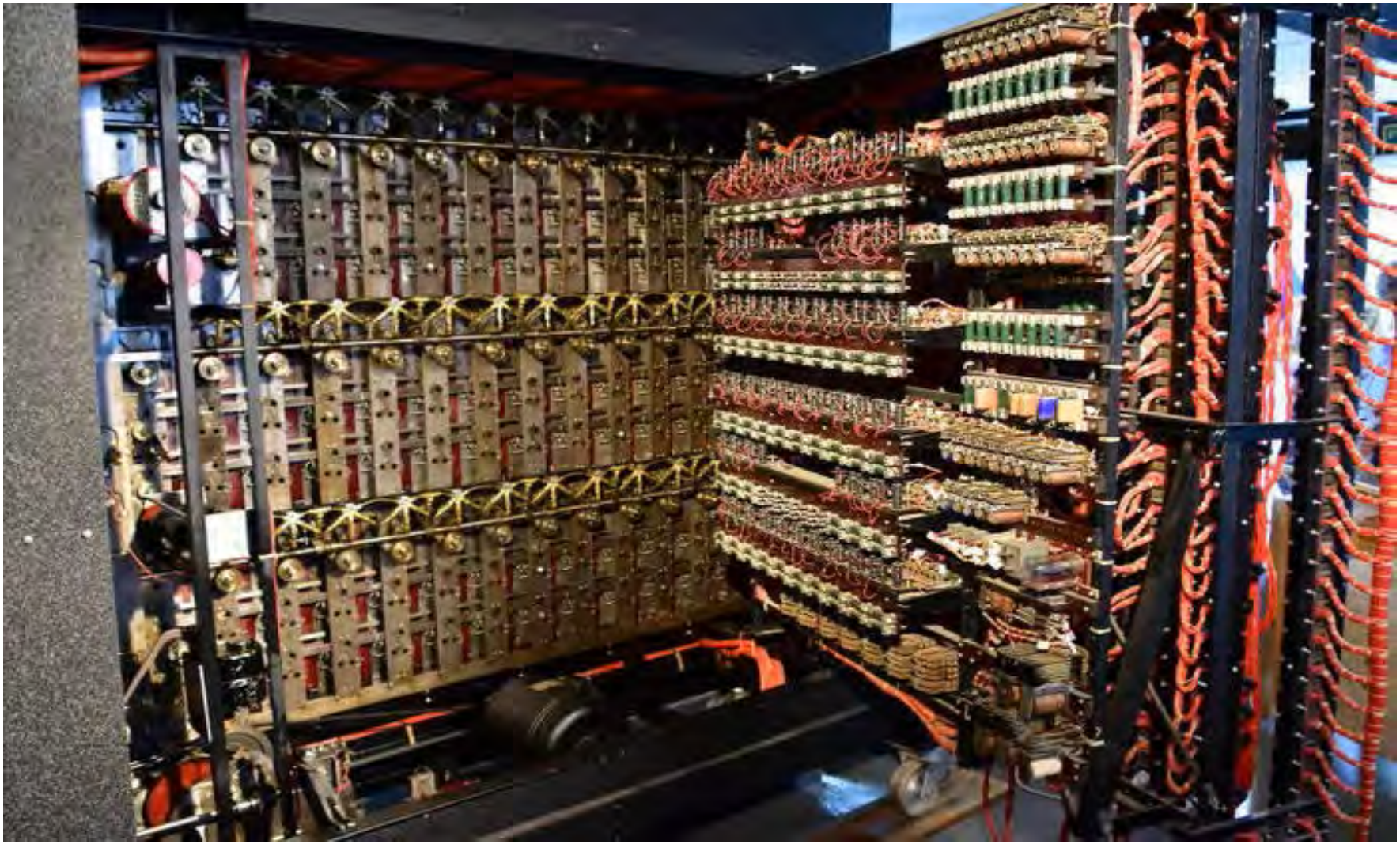
ma ecco la sorpresa!



da dove arrivano le nuove minacce Internet:
*«il **Ransomware**»*

*ecco **la bestiaccia***
come si presenta per chiedere il riscatto

Colossus (1943), prodotto in 10 esemplari elaborava 4 mila messaggi al giorno



*Social & Smartphone: «mondo **reale** & mondo **virtuale**»*

*- l'obiettivo è condividere info, foto, filmati, mettersi in mostra sulla «**piazza virtuale**»*

*- però con problemi **isolamento,** **security & privacy***

filmato

Il telefonino e Google,
conoscono tutto di noi

Non ci credete?
Facciamo la prova
con me

In ***Google.it/locationhistory*** *troviamo il diario di tutti i nostri spostamenti, giorno per giorno, ora per ora, metro per metro*

di che cosa parliamo nell'incontro

*# dal Web 1.0 ai Social**: «come è cambiato il nostro rapporto con Internet»***
 # la migliore difesa è la conoscenza dei pericoli
*# virus, trojan, spam, phishing e ransomware: «**ogni giorno ne arrivano di nuovi»***
*# noi navighiamo nei siti web conosciuti, ma poi esistono **deep web e dark web**: «che cosa sono?»*
*# parleremo anche di **crittografia** e come i nostri dati possono essere protetti*
*# ricordiamo **Alan Turing**, il matematico inglese che ha decifrato Enigma, accelerando la fine della Guerra Mondiale: «che cos' è il suo test?»*
*# **i consigli** per rendere più sicura la nostra presenza online*