

Cybersecurity

«come difendersi dai pericoli del Web»

Centro Bartolomeo Garelli – 14 maggio 2024



Umberto Torelli - Corriere della Sera

la domanda è

IL WEB SA TUTTO SU DI TE.
TU SAI TUTTO SUL WEB?

generazione #



Le 3+1 evoluzioni (rivoluzioni) di Internet

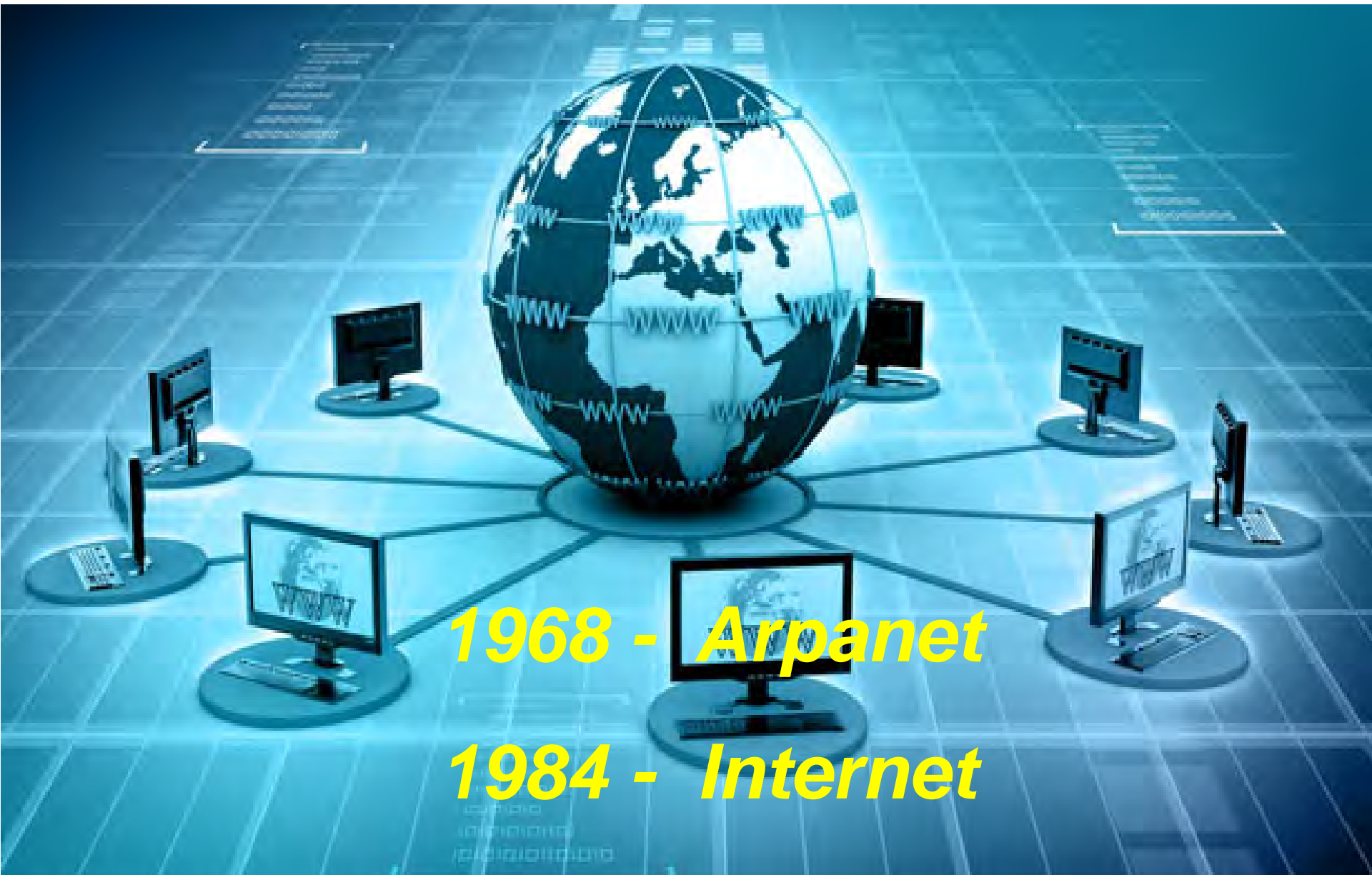
Web 1.0 - Internet dei computer (1990-2000)

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



1968 - Arpanet

1984 - Internet

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»



INTERNET OF THINGS

lot: «*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»



A person wearing a dark hoodie is seen from the side, holding a laptop. The background is a blurred digital interface with various text and icons. Overlaid on the image are several terms related to cybersecurity: 'spoofing' in orange, 'TROJAN' in yellow, 'Spam' in black, 'Phishing' in yellow, and 'Ransomware' in white.

spoofing

TROJAN

Spam

Phishing

Ransomware

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



un video vale più di mille parole



Come sta il suo strappo muscolare ?



0:56 / 2:14



l'iceberg del Web



4%

SURFACE WEB

indicizzato e facilmente consultabile

90%

DEEP WEB

non indicizzato, ricerca più complessa

6%

DARK WEB

oscurato, difficile da scoprire

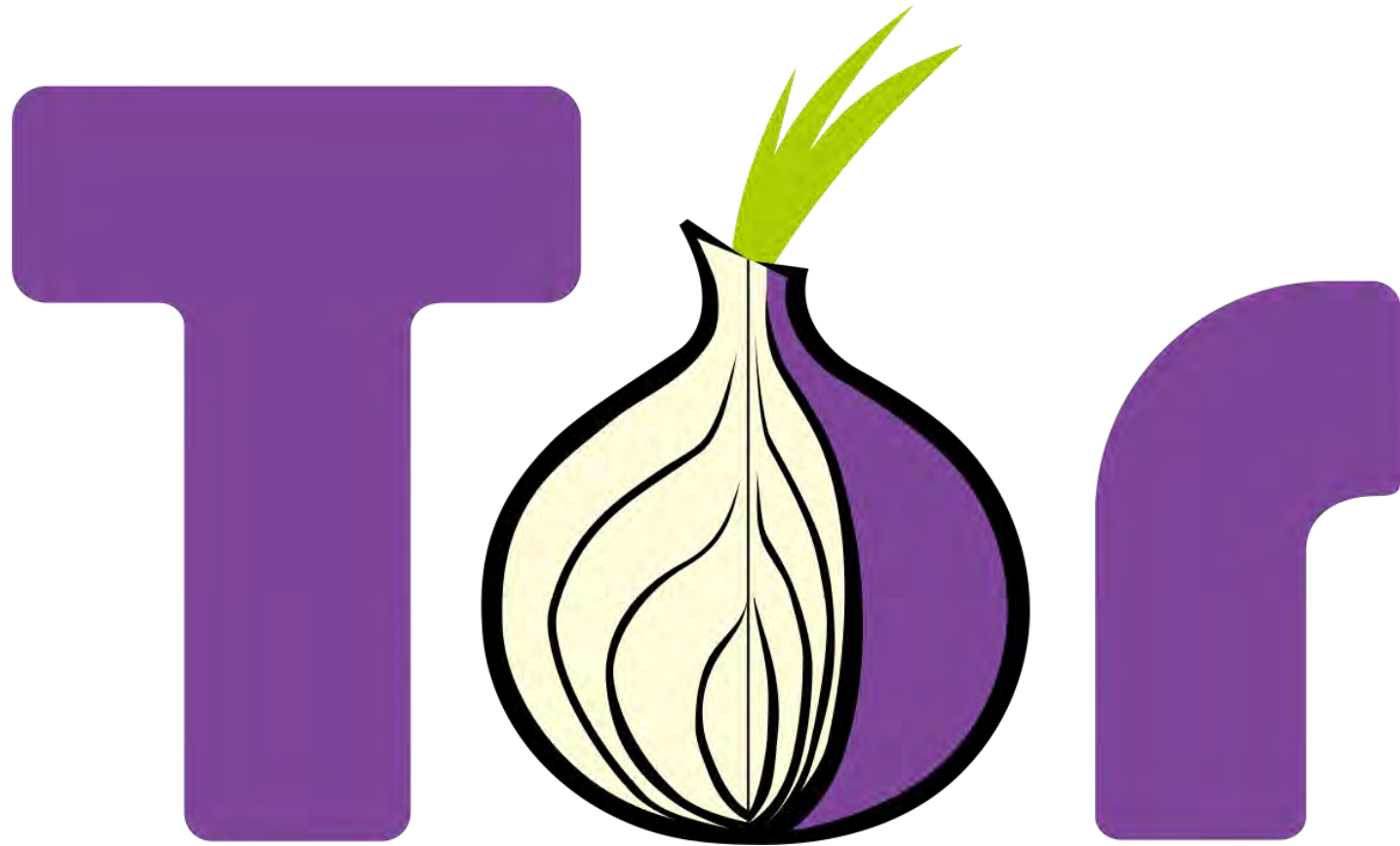
le tre Web-zone

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

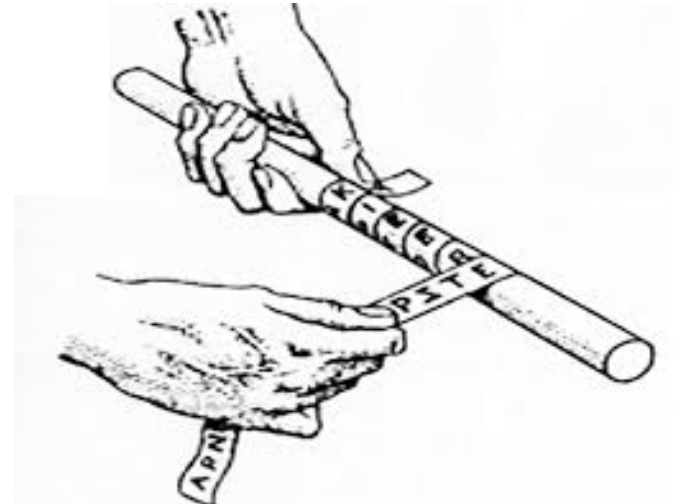
DARK WEB (6%): la **parte oscura** di Internet, con vendita di armi, siti terroristici e pedopornografici, inaccessibile senza software dedicati

come si naviga nel Dark-Web?
The Onion Router

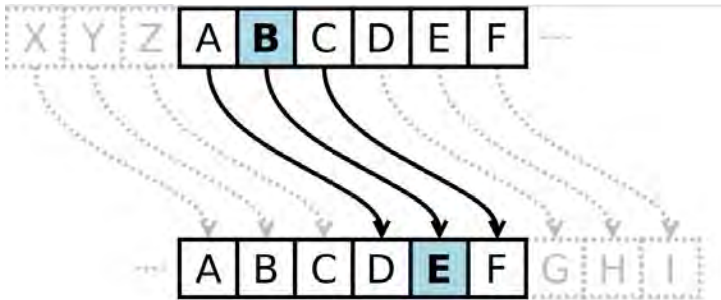


DIFESA 1

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

©2019 Paolo Bonavoglia



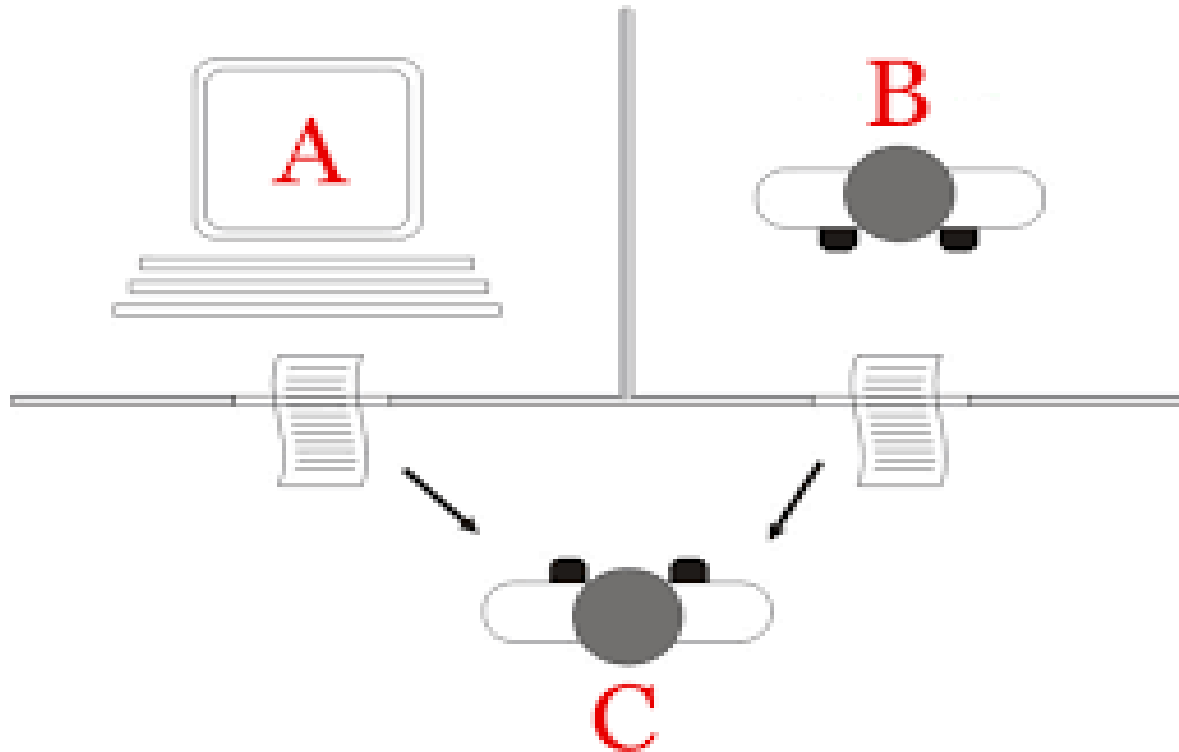
Alan Turing & Enigma



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



"THE BEST BRITISH FILM OF THE YEAR"



BENEDICT CUMBERBATCH **THE** KEIRA KNIGHTLEY
IMITATION GAME 2014



BASED ON THE INCREDIBLE
TRUE STORY OF ALAN TURING

STUDIOCANAL

DIFESA 2

*i cyber-poliziotti dei SOC
Security Operation Center*



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

 Yuri Sergeyevich Andrienko	 Sergey Vladimirovich Detistov	 Pavel Valeryevich Prolov
 Anatoliy Sergeyevich Kovalev	 Artem Valeryevich Oshchenko	 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, Yuri Sergeyevich Andrienko, Sergey Vladimirovich Detistov, Pavel Valeryevich Prolov, Anatoliy Sergeyevich Kovalev, Artem Valeryevich Oshchenko, 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

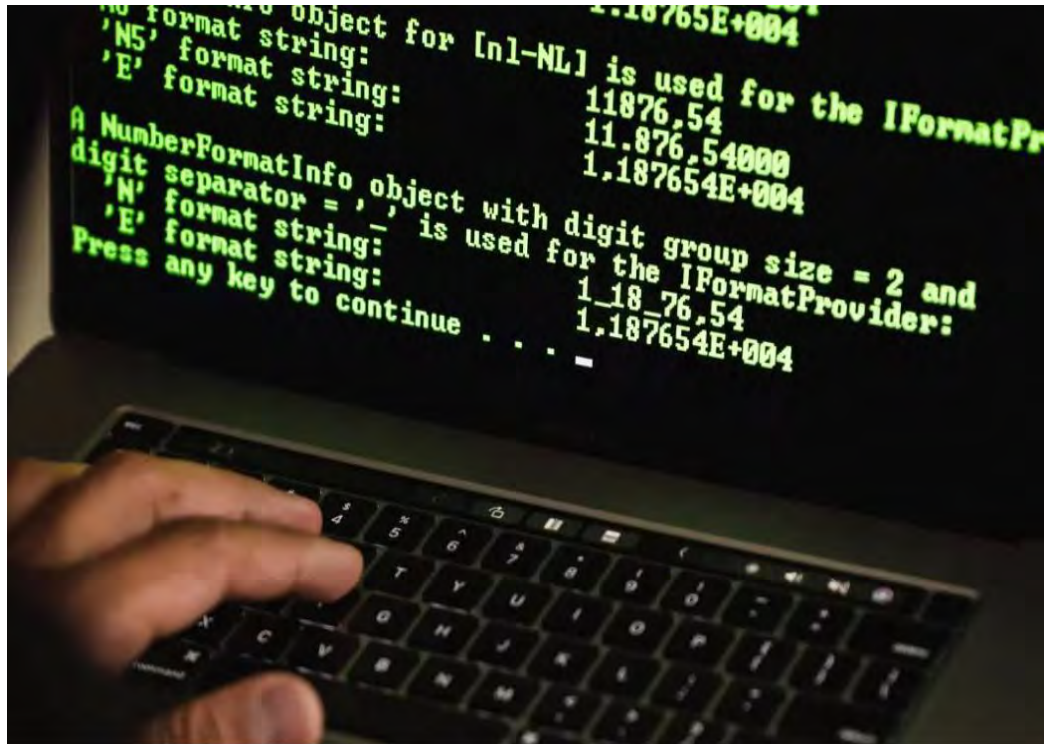
Telebots
/Voodoo Bear



Sednit
Fancy
Bear/APT28

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

The screenshot displays a software interface for credit card market analysis. At the top, logos for VISA, MASTERCARD, AMEX, and DISCOVER are visible. Below them is a section titled "CARD RESULTS" which contains a table of card data. The table has several columns: a selection checkbox, "CARD TYPE", "BII", a card number, two "YES" status indicators, a description of the card, and a price. A mouse cursor is pointing at the checkbox for the fourth row.

<input type="checkbox"/>	CARD TYPE	BII					
<input type="checkbox"/>	VISA	48165	YES	YES	Have CW2		\$10.00
<input checked="" type="checkbox"/>	VISA	496	90022	YES	YES	Have CW2	\$10.00
<input checked="" type="checkbox"/>	VISA	483	79761	YES	YES	Have CW2	\$10.00
<input checked="" type="checkbox"/>	VISA	486	50273	YES	YES	Have CW2	\$10.00
<input type="checkbox"/>	VISA	420	07076	YES	YES	Have CW2	\$10.00
<input type="checkbox"/>	VISA	406	11220	YES	YES	Have CW2	\$10.00
<input type="checkbox"/>	VISA	483	32714	YES	YES	Have CW2	\$10.00
<input type="checkbox"/>	VISA	483	11214	YES	YES	Have CW2	\$10.00
<input type="checkbox"/>	VISA	441					\$1.50
<input type="checkbox"/>	VISA	4641					

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



& 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...»

1 Durante la navigazione Internet lasci tracce dei siti visitati: restano sul cloud anche cancellando la cronologia

2 In caso di atti illeciti, la polizia può accedere a documenti, foto e filmati presenti sull'hard disk

53%
i genitori
che non sanno
che cosa fanno i figli online

@
4 Se entri in siti a «luci rosse», puoi ricevere virus che s'installano nella memoria di computer e cellulari

3 Non è praticamente possibile rimuovere foto e filmati, una volta postati

5 Non chattare con sconosciuti o lasciare numeri di telefono e indirizzi. I malintenzionati possono fingersi coetanei

6 Le informazioni personali lasciate sui social network possono essere viste da insegnanti e aziende (quando cercherai lavoro)



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

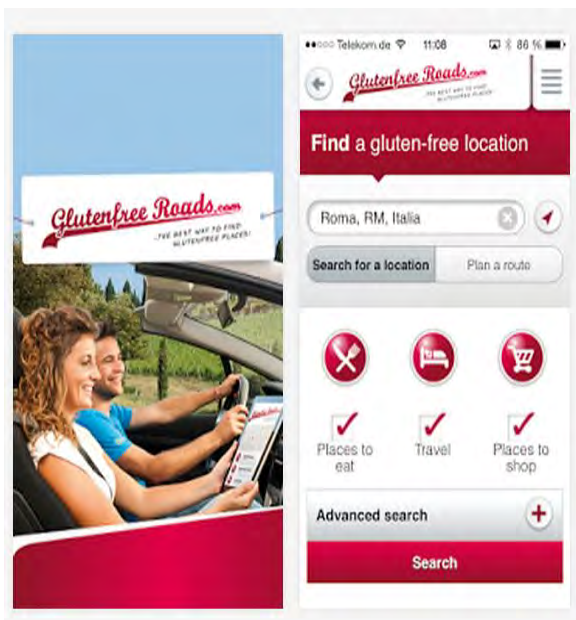
FILTERS

Out the irrelevant



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

ma ecco la sorpresa! 



La versione 1.0.0 può accedere a:

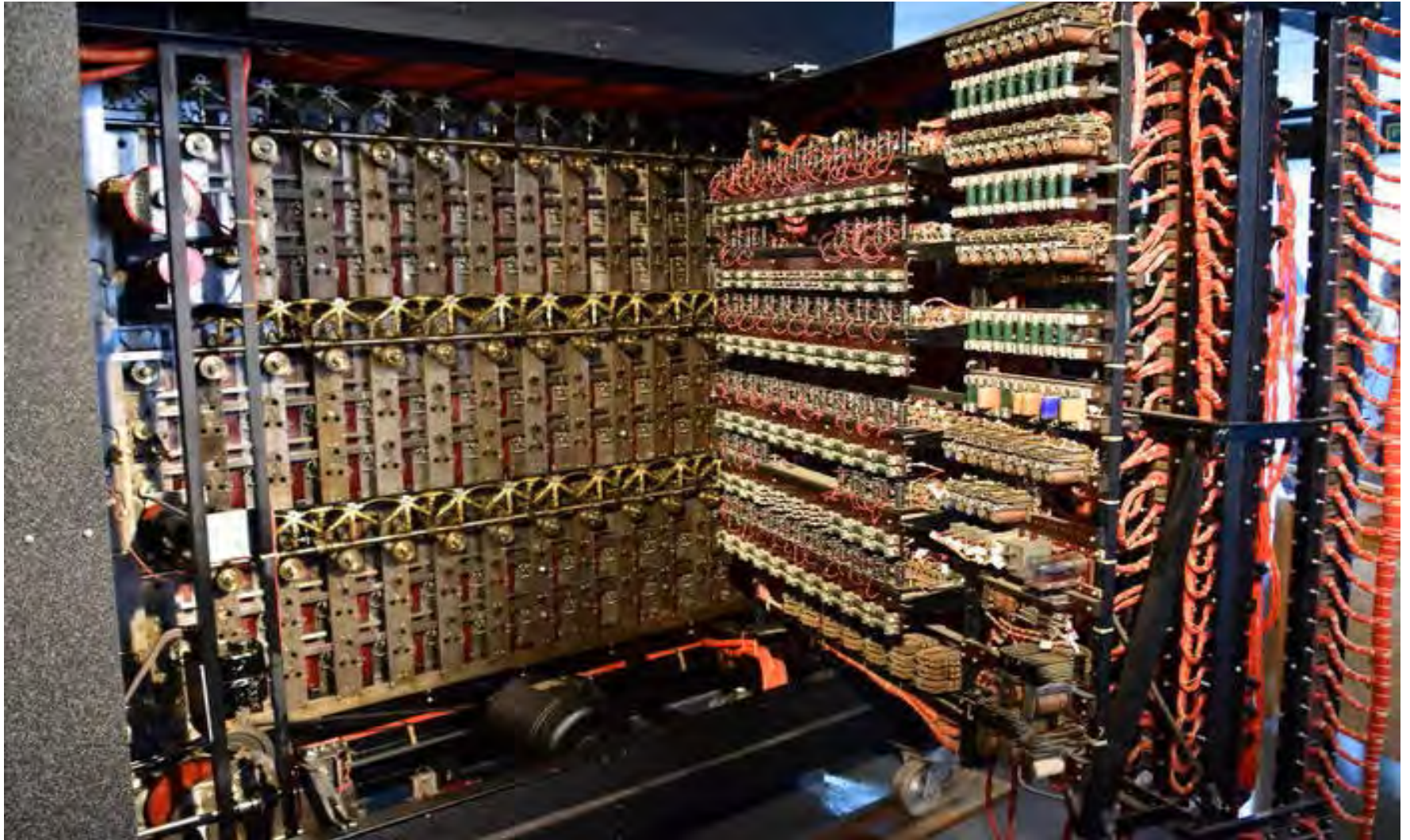
- Identità**
 - individuazione account sul dispositivo
- Contatti**
 - lettura contatti personali
 - modifica dei contatti personali
- Posizione**
 - posizione approssimativa (basata sulla rete)
 - posizione precisa (GPS e basata sulla rete)

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](https://www.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*