



REPORT TECNICO

PROMPT PER CHATGPT

Redatto da: *Nicolò Calì Cybersecurity Student*

Data: 08/01/2026

1. Introduzione

1.1 Obiettivo dell'Attività

Lo scopo dell'attività di oggi è quello di imparare al meglio l'utilizzo di un AI inserendo al suo interno un prompt molto dettagliato e contestualizzato in modo da avere una risposta precisa e minuziosa

Le ricerche da svolgere saranno relative ai seguenti argomenti:

- *Comprendere il Social Engineering e le strategie di difesa*
- *Lista di CVE relative ad un software o un servizio e le sue possibili soluzioni*

2. Ambiente di Lavoro e Strumenti

Per la nostra esercitazione utilizzeremo semplicemente un Intelligenza Artificiale, nel nostro caso useremo ChatGPT.

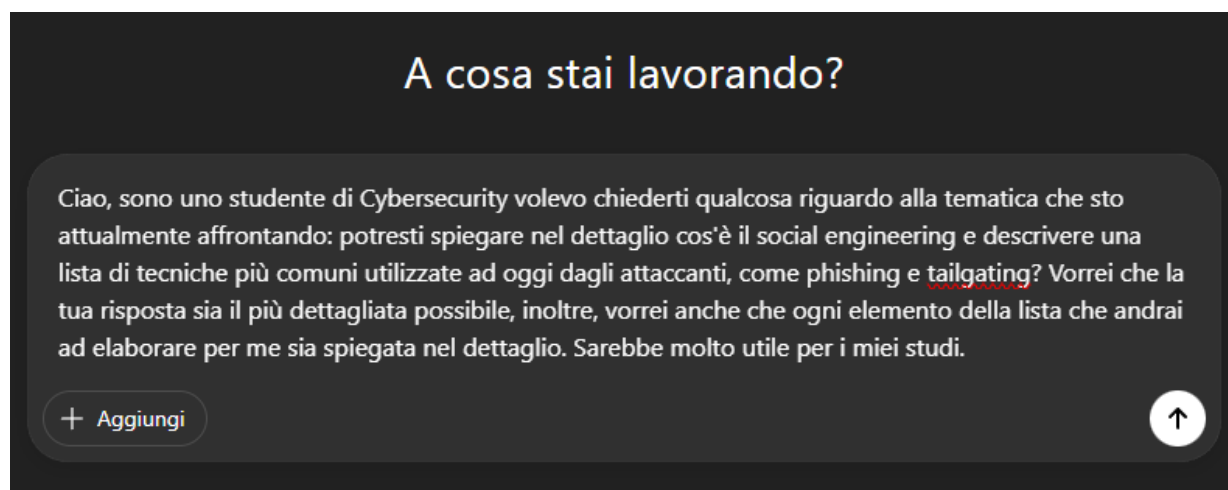
Cosa è ChatGPT?

Si tratta di un **Large Language Model (LLM)** della famiglia **GPT (Generative Pre-trained Transformer)**, addestrato da OpenAI.

3. Attività Tecnica e Metodologia

3.1 Prima Ricerca: Social Engineering e strategie di ricerca

In questa prima fase elaboriamo un prompt per ottenere una risposta esauriente su che cosa è il social engineering e quali sono le tecniche più comuni utilizzate attualmente. Userò il seguente prompt:



Come possiamo vedere, trattandosi di argomenti abbastanza “delicati” ho fatto attenzione a specificare nel modo più chiaro possibile che non ho alcuna intenzione malevola **contestualizzando** la mia richiesta.

Cos'è il Social Engineering

Il social engineering è un insieme di tecniche di attacco psicologico utilizzate per manipolare le persone inducendole a compiere azioni che compromettono la sicurezza, come:

- rivelare informazioni sensibili (password, PIN, dati personali)
- cliccare su link malevoli
- installare software dannoso
- concedere accesso fisico o logico a sistemi protetti

● **Punto chiave:**

A differenza degli attacchi puramente tecnici (exploit, malware, vulnerabilità software), il social engineering non attacca il sistema, ma la mente della vittima.

Gli attaccanti sfruttano:

- fiducia
- paura
- urgenza
- curiosità
- autorità
- ignoranza o disattenzione

Le fasi tipiche di un attacco di Social Engineering

1. Raccolta di informazioni (Reconnaissance)

- social network (LinkedIn, Facebook, Instagram)
- siti aziendali
- data breach precedenti

2. Costruzione del pretesto (Pretexting)

- creazione di una storia credibile

3. Interazione con la vittima

- email, telefono, messaggi, di persona

4. Sfruttamento

- ottenimento dell'obiettivo (accesso, dati, denaro)
-

Tecniche di Social Engineering più comuni (spiegate nel dettaglio)

1. Phishing

Il phishing è la tecnica di social engineering più diffusa e pericolosa.

Cos'è

Consiste nell'inviare comunicazioni fraudolente (email, SMS, messaggi) che imitano entità legittime per indurre la vittima a:

- cliccare su link malevoli
- inserire credenziali
- scaricare malware

Caratteristiche tipiche

- loghi e grafica ufficiale
- indirizzi simili a quelli reali (typosquatting)
- messaggi di urgenza ("account bloccato", "azione richiesta")

Esempio

"Il tuo account bancario è stato sospeso. Accedi subito per verificare."

👉 Il link porta a una pagina fake che ruba le credenziali.

2. Spear Phishing

Cos'è

È una versione mirata del phishing.

Differenza dal phishing classico

- phishing → attacco di massa
- spear phishing → bersaglio specifico

L'attaccante studia la vittima (ruolo, colleghi, interessi).

Esempio

Un'email apparentemente inviata dal responsabile IT a un dipendente:

"Ciao Marco, ho bisogno che tu verifichi questo documento urgente."

📎 Allegato contenente malware.

3. Whaling

Cos'è

Una forma di spear phishing rivolta a figure di alto livello:

- CEO
- CFO
- dirigenti
- amministratori

Obiettivo

- frodi finanziarie
- accesso a dati critici
- autorizzazioni privilegiate

Esempio

Email falsa al CFO che richiede un bonifico urgente verso un conto controllato dall'attaccante.

4. Vishing (Voice Phishing)

Cos'è

Attacco di social engineering tramite telefono.

Tecniche utilizzate

- spoofing del numero (sembra quello ufficiale)
- tono autoritario o rassicurante
- pressione psicologica

Esempio

“Sono dell'assistenza della banca, c'è un problema sul tuo conto. Mi serve il codice OTP.”

⚠ Le banche non chiedono mai queste informazioni.

5. Smishing (SMS Phishing)

Cos'è

Phishing tramite SMS o app di messaggistica (WhatsApp, Telegram).

Perché è efficace

- SMS percepiti come più “personali”
- schermi piccoli → meno attenzione ai dettagli

Esempio

“Pacco in giacenza. Conferma l'indirizzo: [link]”

6. Pretexting

Cos'è

L'attaccante crea un pretesto credibile per ottenere informazioni.

Elementi chiave

- storia coerente
- ruolo credibile (IT, HR, fornitore)
- linguaggio tecnico appropriato

Esempio

“Sono del reparto IT, stiamo verificando un problema di accesso. Puoi confermarci la tua password temporanea?”

7. Tailgating (o Piggybacking)

Cos'è

Tecnica di social engineering fisico.

Come funziona

Un attaccante segue una persona autorizzata per entrare in un'area protetta senza badge o credenziali.

Sfrutta

- educazione
- gentilezza
- pressione sociale

Esempio

Una persona con le mani occupate chiede:

“Puoi tenermi la porta?”

 Accesso non autorizzato ottenuto.

8. Baiting

Cos'è

L'attaccante offre qualcosa di allettante per attirare la vittima.

Esempi comuni

- chiavette USB infette lasciate in giro
- download “gratuiti”
- software crackati

Esempio

USB con etichetta:

“Stipendi 2025”

Quando viene inserita → malware eseguito.

9. Quid Pro Quo

Cos'è

Simile al baiting, ma prevede uno scambio diretto.

Esempio

“Sono del supporto tecnico, ti aiuto a risolvere un problema se mi dai accesso remoto.”

10. Impersonation

Cos'è

L'attaccante si finge una persona reale:

- collega
- fornitore
- tecnico
- autorità

Può avvenire:

- online
 - telefonicamente
 - di persona
-

Perché il Social Engineering è così efficace

- Le persone non sono patchabili
- Le emozioni superano la razionalità
- La tecnologia può essere sicura, ma l'utente no

📌 Statistica importante (concetto chiave per l'esame):
La maggior parte delle violazioni di sicurezza inizia da un attacco di social engineering.

Contromisure (accenno utile per lo studio)

- formazione del personale
 - awareness e simulazioni di phishing
 - policy chiare
 - principio del least privilege
 - MFA (Multi-Factor Authentication)
-

Se vuoi, nel prossimo messaggio posso:

- collegare queste tecniche a casi reali
- spiegarti come vengono testate nei penetration test
- aiutarti a preparare appunti da esame
- confrontare social engineering e attacchi tecnici

Dimmi tu 👍

Come possiamo vedere abbiamo ottenuto una risposta davvero esauriente, piena di tutte le informazioni che avevamo richiesto.

Adesso procederò con quest'altro prompt per avere delle ulteriori informazioni riguardo alcune strategie efficaci per contrastare gli attacchi di social engineering.

Tuttavia, questa volta il mio prompt sarà molto più semplificato perché, scrivendo sulla stessa chat di poco fa, l'AI dovrebbe aver già compreso che cerco informazioni utili per il mio percorso scolastico in Cybersecurity

Molto bene, potresti elencare e spiegare alcune strategie efficaci per difendersi dagli attacchi di social engineering che mi hai elencato poco fa? soffermati SOLO sulle strategie di difesa.

+ Aggiungi



ChatGPT può commettere errori. Assicurati di verificare le informazioni importanti. Vedi [Preferenze sui cookie](#).

1. Security Awareness & Formazione continua

Descrizione

La formazione degli utenti è la prima e più importante linea di difesa contro il social engineering.

Perché è cruciale

- Gli attacchi sfruttano comportamenti umani
- Le tecnologie da sole non bastano
- Un utente consapevole può bloccare l'attacco sul nascere

Elementi chiave di una buona formazione

- riconoscimento di email, chiamate e messaggi sospetti
- comprensione delle tecniche psicologiche (urgenza, paura, autorità)
- simulazioni pratiche (phishing simulation)
- aggiornamenti periodici (non formazione "una tantum")

Benefici

- riduzione drastica del click rate
- miglioramento della capacità di segnalazione
- creazione di una cultura della sicurezza

2. Policy di sicurezza chiare e applicate

Descrizione

Le policy definiscono cosa è consentito e cosa no, eliminando ambiguità sfruttabili dagli attaccanti.

Esempi di policy efficaci

- mai condividere password o OTP
- procedure standard per richieste sensibili
- verifica dell'identità su canali separati
- divieto di collegare dispositivi USB non autorizzati

Perché funzionano

- riducono il potere del pretesto

- standardizzano le risposte
 - rendono l'ingegneria sociale meno credibile
-

3. Multi-Factor Authentication (MFA)

Descrizione

L'MFA richiede più fattori di autenticazione:

- qualcosa che sai (password)
- qualcosa che hai (token, app)
- qualcosa che sei (biometria)

Impatto sulla difesa

- anche se le credenziali vengono rubate, non sono sufficienti
- blocca la maggior parte degli attacchi di phishing
- riduce drasticamente l'impatto degli errori umani

Best practice

- MFA ovunque possibile
 - evitare SMS quando possibile (SIM swapping)
 - preferire app di autenticazione o hardware token
-

4. Verifica dell'identità (Out-of-Band Verification)

Descrizione

Consiste nel verificare una richiesta tramite un canale diverso da quello originale.

Esempio

- richiesta via email → verifica telefonica
- chiamata sospetta → richiamare un numero ufficiale

Perché è efficace

- rompe il controllo dell'attaccante sulla comunicazione
 - smaschera impersonation e pretexting
 - semplice, ma potentissimo
-

5. Email Security & Anti-Phishing Technologies

Descrizione

Sistemi tecnici che analizzano e filtrano i messaggi prima che raggiungano l'utente.

Tecnologie principali

- filtri antispam avanzati
- analisi comportamentale
- sandbox per allegati
- URL rewriting e scanning
- DMARC, SPF, DKIM

Limiti (importante per lo studio)

- nessun filtro è perfetto
- attacchi mirati possono passare
 - ➔ devono sempre essere affiancati alla formazione

6. Principle of Least Privilege (PoLP)

Descrizione

Ogni utente deve avere solo i privilegi strettamente necessari.

Benefici contro il social engineering

- limita i danni se un account viene compromesso
- riduce la superficie di attacco
- rende meno efficaci attacchi mirati a utenti comuni

Applicazioni pratiche

- account amministrativi separati
- accessi temporanei
- revisione periodica dei privilegi

7. Segregation of Duties (SoD)

Descrizione

Le operazioni critiche richiedono più persone o più livelli di approvazione.

Esempio

- una persona richiede un pagamento
- un'altra lo autorizza

Perché funziona

- impedisce frodi basate su impersonation
 - riduce l'efficacia del whaling
 - introduce controlli incrociati
-

8. Controlli di sicurezza fisica

Descrizione

Difese contro social engineering in presenza (es. tailgating).

Contromisure

- badge personali e non condivisibili
- tornelli
- accessi separati
- policy “no tailgating”
- formazione del personale di reception

Aspetto culturale

- rendere socialmente accettabile chiedere il badge
 - eliminare l'imbarazzo come fattore di rischio
-

9. Disabilitazione e controllo dei supporti rimovibili

Descrizione

Difesa contro baiting e malware fisici.

Strategie

- disabilitare USB non autorizzate
 - allowlist dei dispositivi
 - endpoint protection
 - sensibilizzazione sull'uso dei supporti rimovibili
-

10. Incident Reporting & Response

Descrizione

Una difesa efficace prevede che l'errore umano sia previsto, non punito.

Elementi fondamentali

- canali chiari per segnalare incidenti
- risposta rapida del SOC o IT
- assenza di colpevolizzazione
- feedback agli utenti

Perché è cruciale

- riduce il dwell time dell'attaccante
- limita i danni
- migliora il sistema nel tempo

11. Logging, Monitoring & Anomaly Detection

Descrizione

Monitoraggio continuo delle attività per individuare comportamenti anomali.

Utilità contro il social engineering

- rileva accessi sospetti post-phishing
- identifica escalation di privilegi
- consente risposta rapida

Strumenti tipici

- SIEM
- UEBA
- EDR/XDR

Concetto chiave da ricordare (molto importante per lo studio)

Il social engineering non si elimina, si gestisce.

La difesa efficace nasce dall'integrazione di:

- persone formate
- processi chiari

- tecnologie adeguate

Se vuoi, posso:

- collegare ogni difesa a uno specifico attacco
- aiutarti a costruire una mappa concettuale
- trasformare questa risposta in appunti da esame
- simulare domande d'esame o colloquio tecnico

Dimmi pure come vuoi proseguire 🙌

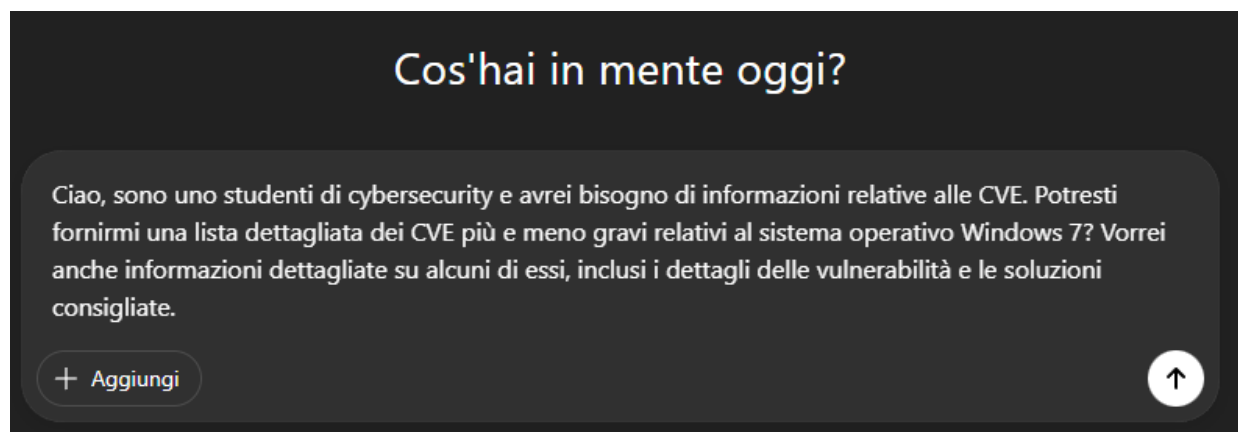
Nonostante abbia inserito un prompt abbastanza semplice ChatGPT mi ha fornito una risposta più che esauriente fornendomi una lista di 11 punti su “Come evitare attacchi di **Social Engineering**”.

3.2 Seconda Ricerca: Esplorazione dei CVE e possibili soluzioni

Per effettuare questa ricerca inserirò un unico prompt ben strutturato in modo da avere la risposta più dettagliata possibile.

Nel mio caso chiederò una lista di tutte le CVE più importanti del SO Windows 7.

Prompt utilizzato:



🔥 CVE molto gravi che hanno colpito Windows 7

1) CVE-2019-0708 “BlueKeep” – Esecuzione remota di codice (RCE)

📌 **Tipo di vuln:** Remote Code Execution (wormable)

🔍 **Descrizione:** questa vulnerabilità nel servizio **Remote Desktop Protocol (RDP)** permette ad un attaccante non autenticato di eseguire codice arbitrario tramite pacchetti RDP appositamente progettati. Si tratta di un difetto di convalida degli input, **pre-auth** e senza bisogno di interazione utente. [Wikipedia+1](#)

🚨 **Perché è critica:** può essere usata per creare worm automatizzati (come WannaCry), capaci di *spostarsi lateralmente* in una rete senza password o credenziali. [Wikipedia](#)

🔧 **Soluzione/mitigazione:**

- Applicare subito l'aggiornamento Microsoft rilasciato a maggio 2019 anche per Windows 7 (patch disponibile nel Microsoft Update Catalog). [Tenable®](#)
- Disabilitare RDP o limitare l'accesso alla porta 3389 tramite firewall.
- Abilitare il **Network Level Authentication (NLA)** per ridurre potenziali exploit anche se vulnerabili.

🔍 **Rilevanza:** una delle vulnerabilità più pericolose mai divulgate per Windows 7, tuttora citata in liste di vulnerabilità sfruttate. [Wikipedia](#)

2) CVE-2017-0144 “EternalBlue” – SMBv1 Remote Code Execution

📌 **Tipo di vuln:** Remote Code Execution (wormable)

🔍 **Descrizione:** falla nel protocollo **SMBv1** che permette l'esecuzione remota di codice da parte di un attaccante senza autenticazione sfruttando una gestione errata della memoria. [Wikipedia](#)

🚨 **Impatto storico:** ampiamente usata per i ransomware **WannaCry** e **NotPetya**, generando infezioni su scala globale grazie proprio alla sua natura “wormable”. [Wikipedia](#)

🔧 **Soluzione/mitigazione:**

- Installare la patch MS17-010 rilasciata nel marzo 2017 da Microsoft. [Wikipedia](#)

- Disattivare **SMBv1** (sostituendo con SMBv2/v3) e bloccare il traffico SMB dal perimetro.

⚠ **Nota importante:** EternalBlue nelle reti non aggiornate resta un vettore di lateral movement anche se non più sfruttato ampiamente come nel 2017.

3) CVE-2021-34527 “PrintNightmare” – Windows Print Spooler RCE/LPE

📌 **Tipo di vuln:** sia **Remote Code Execution** che **Local Privilege Escalation**

🕸 **Descrizione:** vulnerabilità critica nel servizio **Print Spooler** che può consentire ad un attaccante autenticato o locale di eseguire codice al livello SISTEMA o elevare privilegi. [Wikipedia](#)

🔧 **Soluzione/mitigazione:**

- Applicare gli aggiornamenti cumulativi relativi a PrintNightmare (usciti nell'estate 2021). [Microsoft](#)
- Disabilitare permanentemente il servizio Print Spooler su sistemi che non richiedono funzionalità di stampa.

📌 Anche in questo caso Microsoft ha dovuto rilasciare patch **anche per Windows 7**, nonostante fosse fuori supporto, proprio per la gravità del bug. [Wikipedia](#)

🇮🇹 CVE di gravità minore o storica ma comunque notevole

Queste CVE non sono necessariamente tra le più critiche rispetto alle precedenti, ma sono comunque esempi **interessanti per uno studente di cybersecurity**:

CVE	Tipo	Note
WinShock / MS14-066	Remote Code Execution	Bug storico nell'SChannel che affliggeva tutte le versioni Windows, incluso 7. Wikipedia
CVE-2017-0056	Privilege Escalation	Elevazione di privilegi locale con score CVSS 7.8/10. CVE Vulnerabilities Database

Queste non sono tra le più “wormable” né le più sfruttate in exploit automatici come BlueKeep o EternalBlue, ma mostrano come anche funzioni di basso livello (es. crittografia di canale o gestione dei privilegi) possano essere vettori importanti.

📌 Cosa considerare sul contesto Windows 7

! **End of Support:** Microsoft ha ufficialmente terminato il supporto nel gennaio 2020, quindi non rilascia più patch regolari. Tuttavia, per alcune vulnerabilità molto gravi (come PrintNightmare o BlueKeep) ha pubblicato **aggiornamenti straordinari** anche per Win7. [WindowsBlogItalia](#)

📌 Patch e gestione:

- Usa sempre il **Microsoft Update Catalog** o WSUS per recuperare patch legacy.
- Se possibile, disattiva servizi non necessari (es. RDP, Print Spooler) su sistemi Win7 non più in produzione.
- Inserisci sistemi non più supportati in segmenti di rete isolati o in DMZ.

■ Suggerimenti per lo studio

✓ Per ogni CVE che studi:

1. Identifica il **tipo di vulnerabilità** (RCE, LPE, DoS, ecc.).
2. Trova il **punteggio CVSS** e cosa significa (es. quali fattori incidono sul punteggio).
3. Cerca informazioni su **metodi di sfruttamento reali o PoC disponibili**.
4. Analizza le **patch e mitigazioni**: qual è la soluzione tecnica proposta?

✓ Toolkit utili per analisi pratiche:

- **NVD / MITRE CVE database** → per dettagli ufficiali dei CVE.
- **Exploit frameworks** (es. Metasploit) → per capire come gli exploit vengono codificati.
- **Scanner di vulnerabilità** (Nessus, OpenVAS) → per rilevare queste CVE nei sistemi target.

Se vuoi, posso anche prepararti **un elenco aggiornato di CVE recenti con exploit pubblici e proof-of-concept**, oppure mostrarti **come**

interpretare e usare i database NVD/MITRE in un workflow di penetration testing. Vuoi?

La risposta che abbiamo ottenuto è abbastanza approfondita e potrebbe essere ampliata con grande facilità inserendo altri Prompt.

La risposta presenta una breve lista delle più importanti CVE ad oggi conosciute conosciute vediamoli:

- **BlueKeep:** È una vulnerabilità critica del servizio Desktop Remoto (RDP). È molto pericolosa perché permette a un attaccante di eseguire comandi dannosi senza bisogno di password e senza che l'utente faccia nulla; può inoltre diffondersi automaticamente ad altri computer della rete (è "wormable")
- **EternalBlue:** Riguarda un difetto nel protocollo usato per condividere file. È famosa per essere stata sfruttata dal ransomware WannaCry e permette a un hacker di prendere il controllo del sistema da remoto senza alcuna autenticazione.
- **PrintNightmare:** È una falla nel servizio che gestisce la coda di stampa. Permette a un malintenzionato di ottenere i privilegi di amministratore o di eseguire codice dannoso, costringendo Microsoft a rilasciare aggiornamenti anche per il vecchio Windows 7.

5. Conclusioni

L'attività svolta ha evidenziato come l'AI, e nello specifico gli LLM come ChatGPT, rappresenti uno strumento di supporto estremamente potente per lo studio e l'analisi in ambito Cybersecurity. Tuttavia, il report dimostra chiaramente che la qualità delle informazioni ottenute non dipende solo dalla potenza del modello, ma soprattutto dalla capacità dell'utente di formulare richieste precise.

L'adozione di **prompt dettagliati e contestualizzati** si è rivelata determinante. Come osservato durante le ricerche sul Social Engineering e sulle vulnerabilità CVE, specificare il proprio ruolo ("sono uno studente") e l'obiettivo dell'analisi ha permesso di ottenere risposte tecniche, minuziose e prive di blocchi etici.

In sintesi, l'esercizio conferma che saper strutturare un input chiaro è oggi una competenza imprescindibile: **la precisione dell'output dell'AI è direttamente proporzionale alla specificità del contesto fornito dall'operatore.**

