FORUM 2025
CYBER 4.0

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Con il patrocinio di:

Sotto l'alto patrocinio
del Parlamento europeo

Ministero delle Imprese
e del Made in Italy

Finanziato
dall'Unione europea
NextGenerationEU

Alleati e Avversari: Intelligenza Artificiale e Cybersecurity Reale

Relatore

Roberto DE FINIS

Direttore Generale, Sistemi & Automazione

Hosted by:

ROMA TRE
UNIVERSITÀ DEGLI STUDI

S&A
SISTEMI & AUTOMAZIONE

Forum Cyber 4.0
Roma Tre - 5 giugno 2025

Ing. Roberto De Finis - COO @ S&A

Alleati e Avversari:
Intelligenza Artificiale e Cybersecurity Reale

L’Intelligenza Artificiale come risorsa per ogni PMI

L'AI offre ai sistemi potenzialità fino ad ora impossibili

L’AI consente alle PMI di accelerare lo sviluppo software, migliorando **sicurezza e controllo fin dalle prime fasi del processo**. Automatizzando le attività, queste imprese **possono ridurre i costi e ottimizzare i tempi**, elevando la qualità del prodotto.

Implementazione Code review e Secure by Design

Approccio che integra la revisione del codice con i principi di sicurezza fin dall'inizio dello sviluppo, rendendo la sicurezza una parte fondamentale del ciclo di vita del software.

L'uso crescente dell'intelligenza artificiale rende il processo più efficace e proattivo.

Superare i limiti dei tradizionali LLM

Sfruttare le potenzialità della

Retrieval-Augmented Generation

(RAG)

INTEGRARE FONTI MULTIPLE

Raccolta da documenti, contenuti sui social media, ecc.

CONTESTUALIZ-ZARE LE INFORMAZIONI

Recupero dei dati più rilevanti per una query specifica.

GENERARE ANALISI APPROFONDITE

Risposte basate su dati reali e verificati, eliminando ambiguità.

Benefici di questo approccio per l'intelligence:

- **Velocità**
- **Accuratezza**
- **Scalabilità**
- **Efficienza**

Punti Chiave per IA

1

Cyber Threat Intelligence (CTI)

Raccolta e analisi mirata di dati per identificare, monitorare e rispondere alle campagne Cyber malevole.

2

Graph Analysis

Utilizzo di grafi per mappare le connessioni tra entità coinvolte nella attività organizzata e identificare nodi centrali.

3

Dis-informazione

Con contenuti verificati per correggere le false informazioni e ripristinare la fiducia.

4

Educazione e Consapevolezza Pubblica

Promozione alfabetizzazione digitale e consapevolezza sulle metodologie e tecniche di disinformazione.

SPOTLIGHT

Strumento avanzato di supporto alla cybersecurity, utile **per rilevare, analizzare e visualizzare disinformazione in tempo reale**, promuovendo **consapevolezza pubblica** e *normative autoregolative*.

R.G.O.

Lo strumento di **Cyber Threat Intelligence** che permette:

- L'integrazione Dati Eterogenei
- Il rilevamento e la Classificazione Anomalie
- La visualizzazione e l'interrogazione Grafo

FORUM 2025
CYBER 4.0

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Con il patrocinio di:

Sotto l'alto patrocinio
del Parlamento europeo

Ministero delle Imprese
e del Made in Italy

ACN

Finanziato
dall'Unione europea
NextGenerationEU

Alleati e Avversari: Intelligenza Artificiale e Cybersecurity Reale

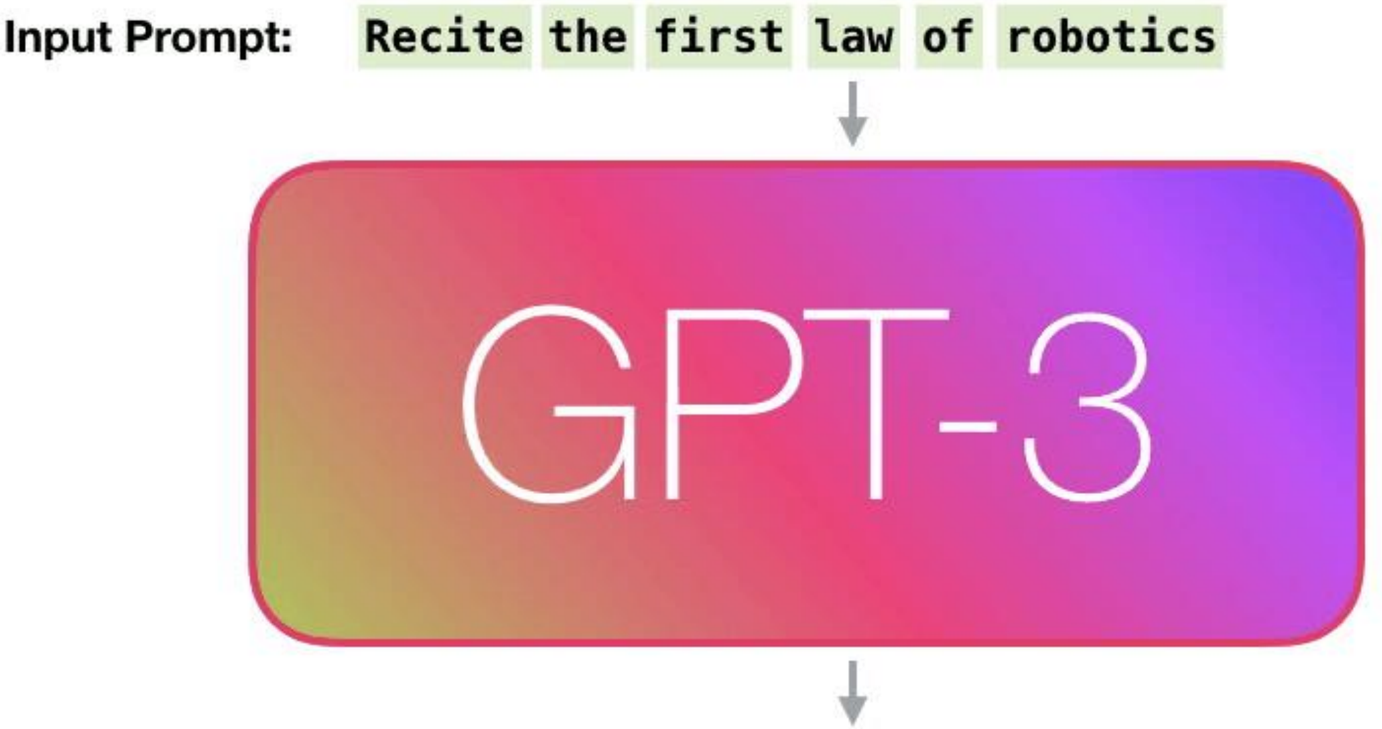
Relatore

Fabrizio SILVESTRI

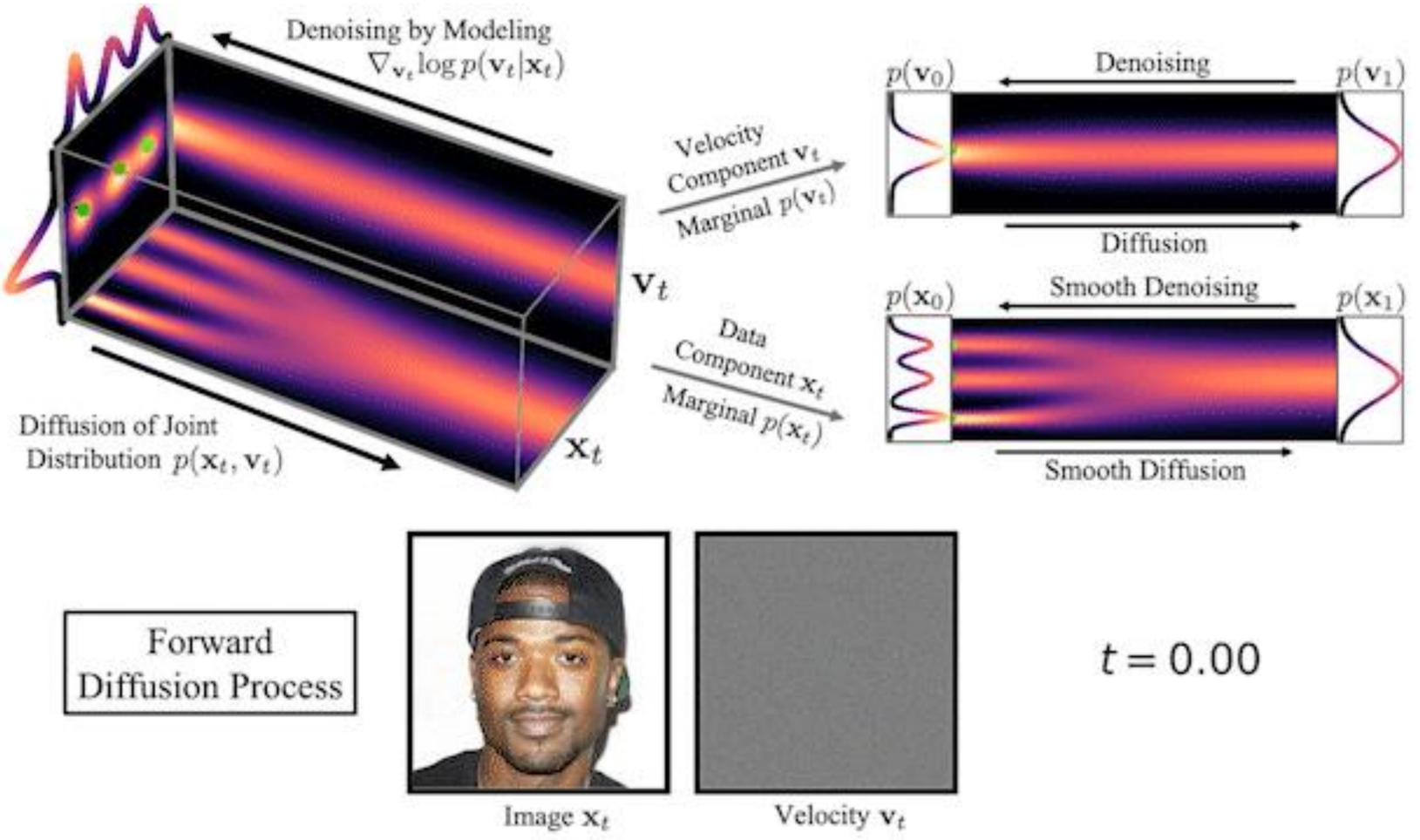
Full Professor and the coordinator of the Ph.D. in Data Science, Università Sapienza

Hosted by:

ROMA TRE
UNIVERSITÀ DEGLI STUDI



Source: https://jalammar.github.io/how-gpt3-works-visualizations-animations/



Source: https://developer.nvidia.com/blog/improving-diffusion-models-as-an-alternative-to-gans-part-2/

fanpage.it

“Mio figlio si è ucciso dopo una mail, dentro c’era sua foto nudo fatta con l’IA”: la storia di John

Source: https://www.fanpage.it/innovazione/tecnologia/mio-figlio-si-e-ucciso-dopo-una-mail-dentro-cera-sua-foto-nudo-fatta-con-lia-la-storia-di-john/

RSTLESS

SAPIENZA UNIVERSITÀ DI ROMA

How South-East Asia's pig butchering scammers are using artificial intelligence technology

By Will Jackson

Corporate Crimes

Wed 15 May 2024

South-East Asia's scam operations are making use of increasingly sophisticated AI tools. *(ABC News: Cordelia Brown)*

Source: https://www.abc.net.au/news/2024-05-16/pig-butchering-scams-artificial-intelligence-ai-face-swapping-/1(

Source: https://www.youtube.com/watch?v=x7G8ECJ_0l4&t=25s

AI Detection Companies: The New Scam

Gurbaksh Chahal
Founder @ VeerOne | AI Technology, Enterprise

May 20, 2024

Originally appeared on: https://epiphany-ai.com/2024/05/20/ai-detection-companies-the-new-scam/

Source: https://www.linkedin.com/pulse/ai-detection-companies-new-scam-gurbaksh-chahal-kryuc/

Researchers secretly experimented on Reddit users with AI-generated comments

University of Zurich researchers used bot accounts to post in r/changemyview.

Karissa Bell
Senior Editor
Updated Tue, Apr 29, 2025 · 4 min read

5

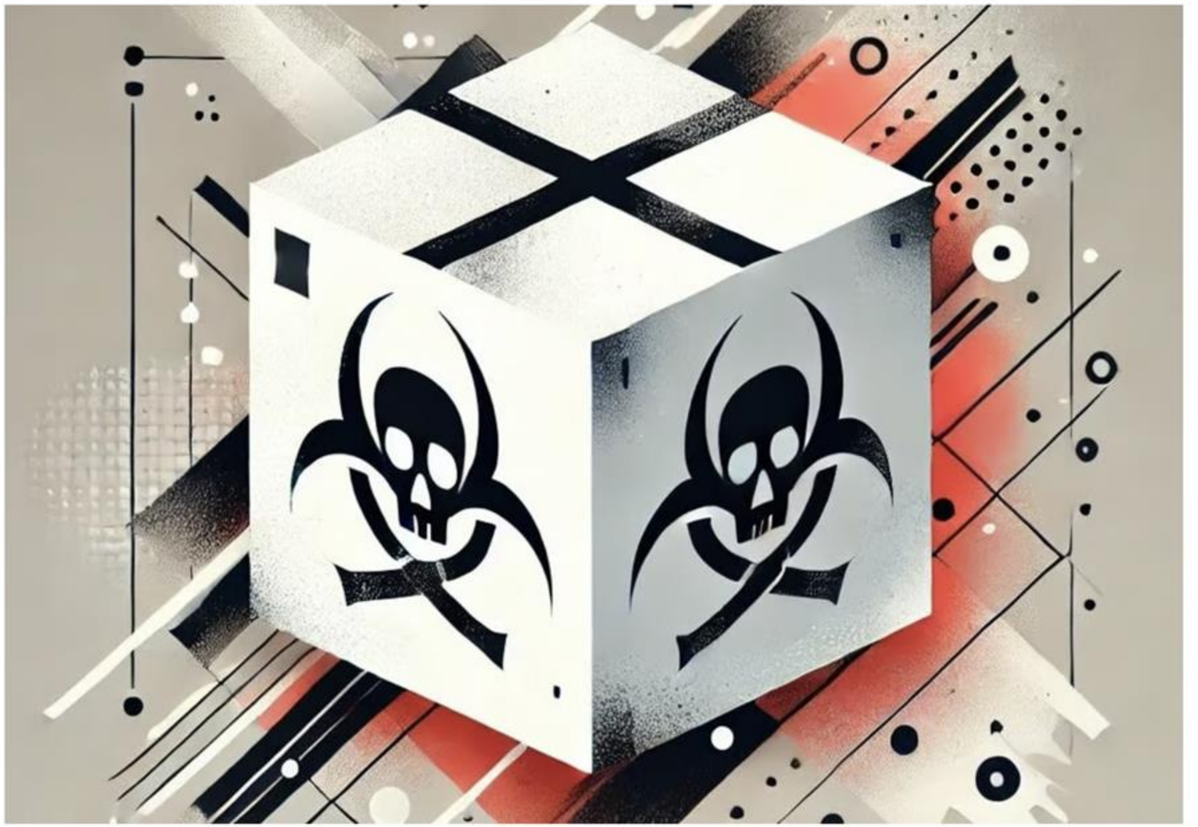
Source: https://www.engadget.com/ai/researchers-secretly-experimented-on-reddit-users-with-ai-generated-comments-194328026.html

RSTLESS

SAPIENZA UNIVERSITÀ DI ROMA

RAG Poisoning: All You Need is One Document

Tamir Ishay Sharbat
August 03, 2024



Source: https://labs.zenity.io/p/rag-poisoning-need-one-document

RSTLESS

SAPIENZA
UNIVERSITÀ DI ROMA

FORUM 2025
CYBER 4.0

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Con il patrocinio di:

Sotto l'alto patrocinio
del Parlamento europeo

Ministero delle Imprese
e del Made in Italy

ACN

Finanziato
dall'Unione europea
NextGenerationEU

Alleati e Avversari: Intelligenza Artificiale e Cybersecurity Reale

Relatore

Mirko LEANZA

CISO e responsabile della BU Cybersecurity & Governance, Teleconsys

Hosted by:

ROMA TRE
UNIVERSITÀ DEGLI STUDI

REGOLAMENTAZIONE: AI ACT

L'Unione Europea tramite **l'emanazione dell'AI Act** ha introdotto dei **requisiti stringenti** per la gestione dei **rischi** legati all'intelligenza artificiale, ponendo nuove sfide per le organizzazioni in termini di cybersecurity e conformità normativa

Il Regolamento stabilisce:

- **Regole** armonizzate per l'**immissione sul mercato**, **messa in servizio** e **uso** dei sistemi di IA
- **Divieti di pratiche** di **IA legate a : Manipolazione e Inganno, sfruttamenti di vulnerabilità, classificazione sociale**
- **Requisiti specifici** per **sistemi di IA ad alto rischio** e **obblighi per gli operatori** di tali sistemi
- Regole di **trasparenza** (sanitizzazione degli input, certezza sulle modalità di addestramento)
- Misure a **sostegno** dell'**innovazione**
- Struttura di governance **multilivello**

AI ACT| ROADMAP

Approvazione AI Act
Marzo 2024

Pubblicazione in Gazzetta Ufficiale
Maggio 2024

Entrata in vigore
Giugno 2024

Vietate pratiche IA ad alto rischio
Dicembre 2024

Codici di condotta volontari
Giugno 2025

Applicazione obblighi per IA ad alto rischio
Giugno 2026

REGOLAMENTAZIONE: AI ACT

Il Regolamento sull'intelligenza artificiale si basa sull'approccio al RISCHIO distinguendo **quattro categorie** di sistemi di IA:

RISCHIO INACCETTABILE	Sistemi di IA che contravvengono ai valori dell'Unione europea perchè violano i diritti fondamentali (manipolazione cognitivo-comportamentale di persone o di specifici, social scoring, identificazione biometrica e categorizzazione delle persone, sistemi di identificazione biometrica remota in tempo reale)
RISCHIO ALTO	Sistemi di IA che hanno un impatto negativo sulla sicurezza delle persone o sui loro diritti fondamentali
RISCHIO LIMITATO	Sistemi di IA a cui vengono imposti obblighi di trasparenza per una maggiore consapevolezza da parte degli utenti
RISCHIO MINIMO	Sistemi di IA che non necessitano di adempiere a specifici obblighi legislativi

ISO42001 | STRUMENTO PER LA COMPLIANCE

Contestualmente all’emanazione dell’AI ACT ISO/IEC ha messo a disposizione un framework per una gestione conforme dei sistemi di AI (SGAI) per supportare le aziende nel percorso di compliance

✅ Allineamento diretto ai requisiti dell’AI Act:
- Gestione rischi, trasparenza, tracciabilità, sorveglianza umana

✅ Sistema certificabile e verificabile:
- Prove documentate di conformità per sistemi ad alto rischio

✅ Dimostrazione di accountability e due diligence:
- Governance, gestione fornitori, controlli etici

✅ Integrazione con altri standard ISO:
- Compatibile con ISO 27001, 9001, 31000, 23894

✅ Pronti all’evoluzione normativa:
- Struttura flessibile e aggiornabile in base agli sviluppi UE

ISO/IEC 42001:2023

La norma ISO/IEC 42001 si rivolge a entità impegnate nell'utilizzo o nell'offerta di prodotti/servizi basati sull'IA, supportando tali organizzazioni nel raggiungimento della **compliance** con normative locali e internazionali e assicurando che l'IA venga utilizzata in modo **etico** e **sicuro**

OBIETTIVI	**Trasparenza nei modelli IA**: promuove chiarezza dei processi decisionali automatizzati **Gestione del rischio**: fornisce linee guida per identificare, valutare e mitigare i rischi associati all'uso dell'IA
PRINCIPI	**Accountability**: assicura che le organizzazioni siano responsabili delle decisioni prese dai sistemi IA, stabilendo chiare responsabilità **Mitigazione della disinformazione:** aiuta a prevenire l'uso improprio dell'IA per la diffusione di contenuti manipolati o falsi

ZEUS | La piattaforma applicativa per la 42001

Dashboard - Reportistica