Tesi di laurea magistrale

# Un framework di CTI per l'analisi semantica di campagne di disinformazione

Anno Accademico 2024/2025

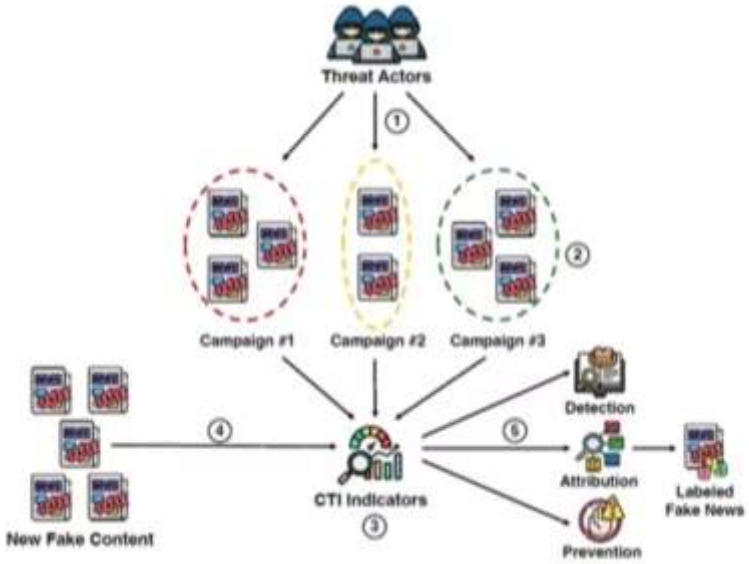
**Relatore**
Ch.mo Prof. Roberto Natella

**Correlatore**
Ing. Vittorio Orbinato

**Candidato**
Francesca Di Martino
Matr. M63001478

# Le Campagne di Disinformazione

*Una campagna di disinformazione è un'operazione coordinata e sistematica progettata per diffondere informazioni false o fuorvianti attraverso molteplici canali e piattaforme, con obiettivi strategici specifici.*




## Caratteristiche critiche

- Velocità di propagazione
- Amplificazione algoritmica
- Coordinazione strategica tra piattaforme
- Persistenza narrativa

## Limiti degli approcci tradizionali

- Fact-checking reattivo
- Analisi isolata dei contenuti
- Mancanza di attribuzione
- Difficoltà nel riconoscere pattern coordinati

# Contributi Innovativi della Tesi

1

**Adattamento del framework CTI al dominio della disinformazione**

Prima applicazione sistematica di STIX/OpenCTI al dominio narrativo per campagne di disinformazione.

2

**Framework per l’estrazione e classificazione semantica**

Prototipazione pipeline per estrazione automatica di triple semantiche e classificatore ibrido.

3

**Validazione Sperimentale**

Testing multi-dataset su fake news reali e articoli generati artificialmente per validazione empirica.

# Dalla Disinformazione Caotica all'Intelligence Navigabile: Il Knowledge Graph

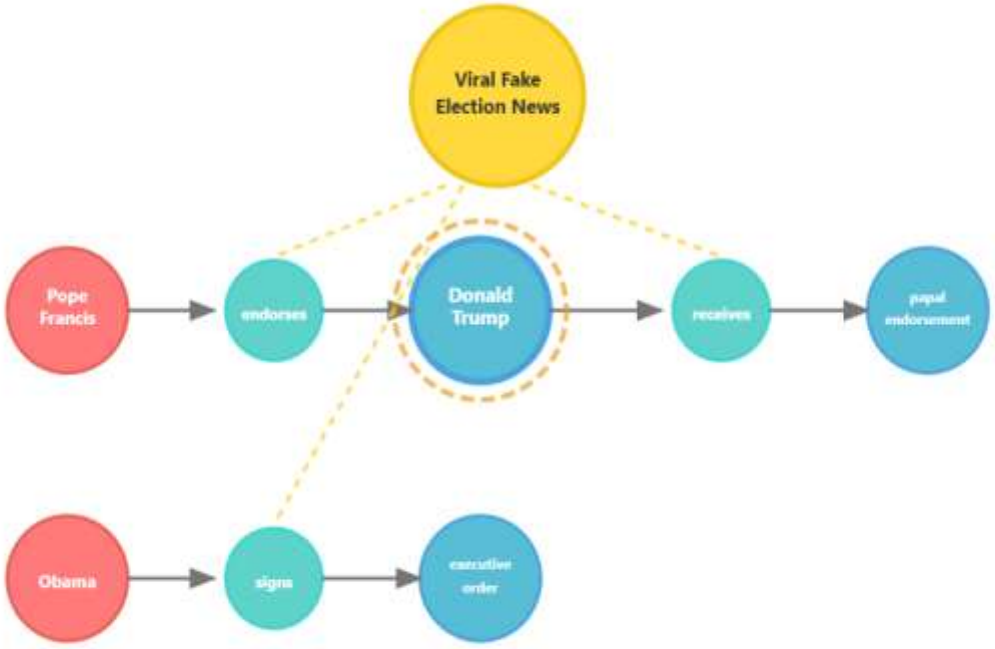
Campagna di Disinformazione: "Viral Fake Election News"

### Articoli Esemplificativi

"Pope Francis Shocks World, Endorses Donald Trump for President, Releases Statement"

### Triple Semantiche Estratte

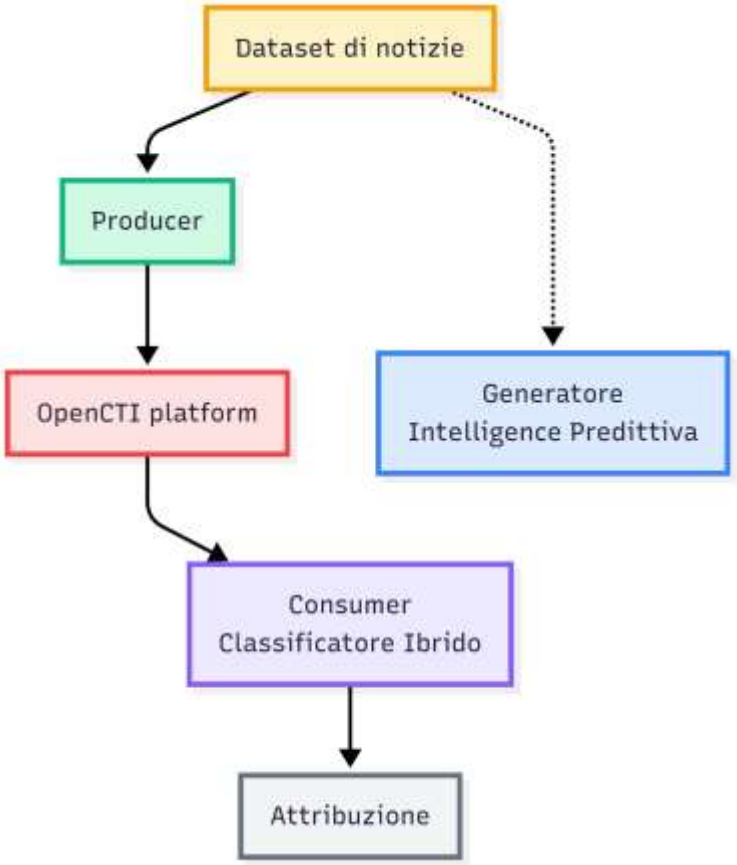
- <Pope Francis, endorses, Donald Trump>
- <Donald Trump, receives, papal endorsement>




### Capacità Operative del Knowledge Graph

- Navigazione Interattiva
- Query Semantiche Avanzate
- Graph traversal automatico
- Entity Resolution Intelligente

# Architettura Modulare




**1. Ingestion**
Articoli → LLM → Triple

**2. Storage**
Triple → STIX → OpenCTI

**3. Classificazione**
Nuovi contenuti → Attribuzione

**4. Intelligence**
Pattern → Predizione

# Dataset e Sperimentazione

## FakeCTI Dataset

- 12.155 articoli di fake news
- 43 campagne di disinformazione
- ID, URL, Title, Source, Text, Campaign, Threat Actor, Type
- Attribuzione esplicita campagna-articolo

## Setup Sperimentale

- Stack: OpenCTI 6.5.10 + Elasticsearch + Redis + Docker
- Split: 90/10 training/test stratificato per campagna

1

### Pipeline CTI Standard

Baseline performance su dati autentici

2

### Pipeline CTI Enhanced

Test robustezza su contenuti artificiali generati

3

### Confronto State-of-the-Art

Valutazione comparativa con FakeBERT

# Estrazione Semantica con LLM: Analisi Comparativa

1

**LLaMA-3-8B**
Precision-first con alta coerenza semantica

2

**DeepSeek-Coder-6.7B**
Completeness-first con elevata copertura

| Metrica | LLaMA-3-8B | DeepSeek-Coder-6.7B |
|---|---|---|
| **Triple per Articolo** | ~3.2 in media | ~8.7 in media |
| **Context Window** | 2048 token (~8000 caratteri) | ~16.000 token |
| **Velocità Processing** | Baseline | Circa 3x più veloce |
| **Limitazioni** | Ridotta scalabilità su testi lunghi | Possibili falsi positivi |

# Pipeline CTI Standard

*Sistema distribuito Producer-Consumer per l'attribuzione automatica di fake news mediante intelligence CTI condivisa*

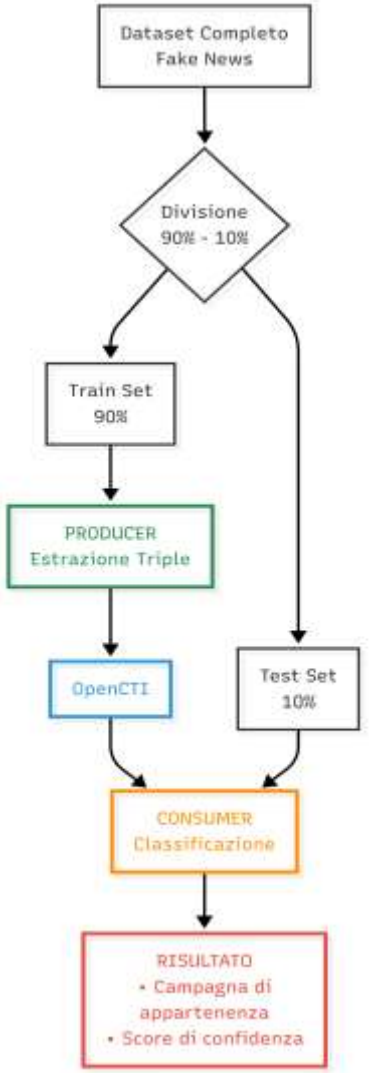
**82,76%**
**Accuracy**

**82,8%**
**Recall Media**

**78,2%**
**Precision Media**

**80,1%**
**F1-Score**

| Categoria | Recall | Precision |
|---|---|---|
| **Russian Troll** | 100% | 80% |
| **American Action News** | 85,7% | 100% |
| **Climate Change** | 83,3% | 100% |
| **Viral Election News** | 78,6% | 91,7% |



# Pipeline CTI Enhanced

**Modulo Generatore**

Trasforma la pipeline originale sostituendo il test set reale con contenuti di disinformazione artificiali generati

**Processo**

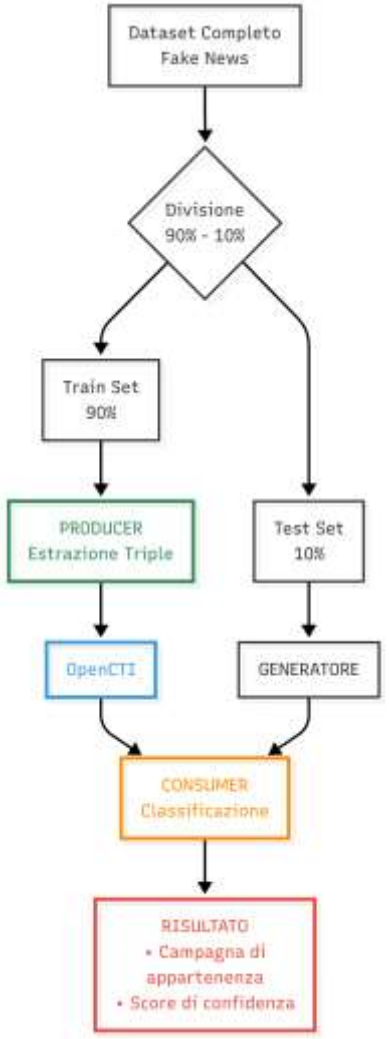
1. Selezione campagne (≥2 articoli, <2000 occorrenze)
2. Partizionamento in example list e comparison list
3. Generazione guidata di  nuovi articoli fake

**Risultati**

Accuracy: 75,86% (44/58 classificazioni)

Precision: 75,9% | Recall: 76,1%

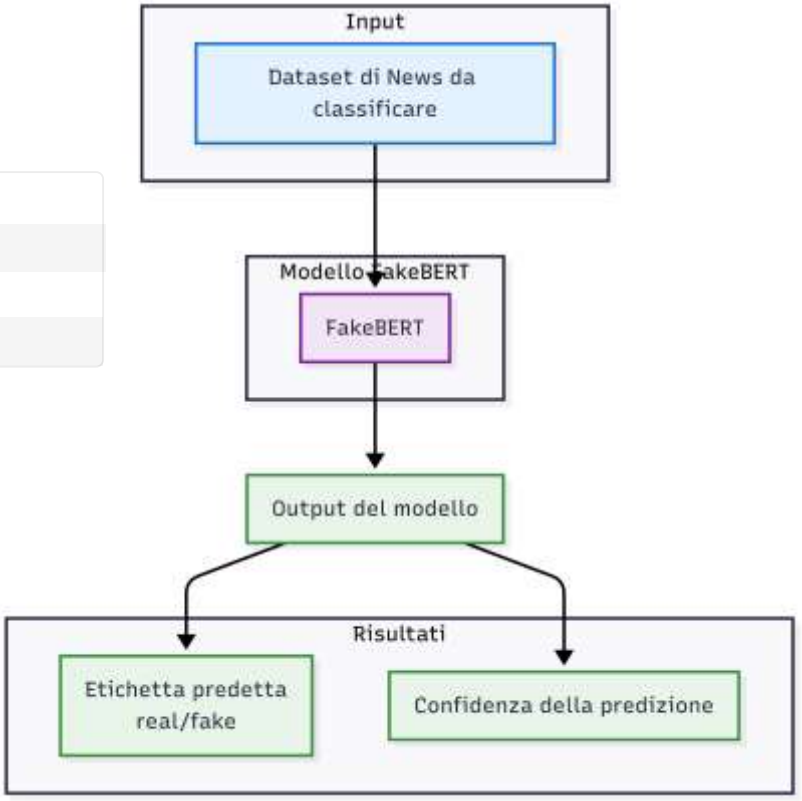
Differenza: -6,90% rispetto ai dati reali



# Confronto con detector di Fake News

FakeBERT: Modello BERT Fine-tuned

| Metrica | FakeBERT | Sistema CTI | Differenza |
|---|---|---|---|
| **Accuratezza** | 37,9% (22/58) | 82,76% (48/58) | +44,86% |
| **Errori di Classificazione** | 62,1% (36/58) | 17,24% (10/58) | -44,86% |
| **Attribution (Campagna)** | NO | 82,76% | Gap funzionale |




## Limitazioni

- Pattern matching superficiale
- Domain-specific
- Analisi isolata
- Output limitato: probabilità binaria.

## Contributi Operativi del Framework CTI

### Supporto al Fact-checking
Confronto automatico di nuovi articoli con contenuti già verificati

### Analisi Longitudinale
Tracciamento dell'evoluzione delle campagne disinformative nel tempo

### Ricerca Accademica
Database interrogabile con correlazioni semantiche pre-calcolate

### Condivisione Intelligence
Formato STIX per condivisione standardizzata tra enti diversi

## Sviluppi Futuri

- Estensione Multimodale: analisi di video e audio
- Monitoraggio in Tempo Reale: controllo 24/7 dei social media con alert immediati