

UNIVERSITÀ POLITECNICA DELLE MARCHE
FACOLTÀ DI INGEGNERIA
Dipartimento di Ingegneria dell'Informazione
Corso di Laurea Magistrale in Ingegneria Informatica e dell'Automazione



PROJECT MANAGEMENT E BUSINESS INTELLIGENCE

**Applicazione di tecniche di Business Intelligence per la costruzione
di dashboard strategiche a supporto dell'analisi della minaccia
terroristica globale e dei processi decisionali in ambito Difesa e
Sicurezza**

**Application of Business Intelligence techniques to build strategic
dashboards to support global terrorist threat analysis and
decision-making processes in the Defense and Security sectors**

Relatori

Prof. Domenico Ursino
Prof.ssa Federica Parlapiano

Candidati

Antonio D'Amelio
Luca Diomedi
Enrico Straccialini
Davide Traini

Sommario

Negli ultimi anni la Data Analytics e la Business Intelligence hanno assunto un ruolo sempre più centrale nei processi decisionali in ambito strategico, in particolare nei settori della Difesa e della Sicurezza. La capacità di analizzare grandi volumi di dati relativi a eventi di violenza politica e terrorismo consente di individuare pattern ricorrenti, monitorare l'evoluzione dei gruppi armati e valutare il livello di instabilità nelle diverse aree geografiche.

In questa tesi sono stati analizzati dati storici relativi alla minaccia terroristica globale. In particolare, è stata realizzata una fase di ETL (Extract, Transform and Load) finalizzata alla pulizia, integrazione e strutturazione del dataset, seguita da un'analisi descrittiva e dalla costruzione di dashboard interattive per la visualizzazione dei principali indicatori. L'obiettivo è fornire uno strumento di supporto alle decisioni capace di trasformare dati complessi in informazioni strategiche utili per il decision-making in ambito Difesa e Sicurezza.

Keyword: Data Analytics, Business Intelligence, Risk Management, Extract Trasform and Load, Qlik, Tableau, Power BI

Introduzione	1
0.1 Approfondimento del Dataset Global Terrorism Database (GTD)	1
0.1.1 Qualità dei Dati e Preparazione (ETL)	3
0.1.2 Preprocessing dei Dati in Python	4
1 Qlik	6
1.1 Analisi descrittiva	6
1.2 Caricamento dei dati su Qlik	6
1.2.1 Data Analysis Dataset Global Terrorism Database	7
1.3 Analisi della distribuzione geopolitica delle minacce	8
1.3.1 Utente	8
1.3.2 Obiettivo	9
1.3.3 Filtri ed esempi di utilizzo	9
1.4 Analisi delle tattiche di attacco e armamenti	13
1.4.1 Utente	13
1.4.2 Obiettivo	14
1.4.3 Filtri ed esempi di utilizzo	14
2 Tableau	18
2.1 Introduzione	18
2.2 Metodologia di Analisi	18
2.3 Strategia di Visualizzazione	19
2.4 Gestione della Qualità dei Dati	19
2.5 Panoramica delle Dashboard Realizzate	19
2.5.1 Dashboard 1: Analisi Temporale degli Attacchi e delle Vittime	20
2.5.2 Dashboard 2: Analisi e Previsione della Letalità per Regione	21
2.5.3 Dashboard 3: Previsione dei Bersagli (Target) per Regione	23
2.5.4 Dashboard 4: Analisi degli Esiti dell'Attacco (Successo vs Fallimento)	25
3 Power PI	28
3.1 Seguire pdf esempio	28
Sitografia	29

Elenco delle figure

1.1	Creazione dell'applicazione	7
1.2	Upload del Dataset	7
1.3	Analisi della distribuzione geopolitica delle minacce	9
1.4	Analisi della distribuzione geopolitica delle minacce filtrando per Anno . . .	10
1.5	Analisi della distribuzione geopolitica delle minacce filtrando per Anno e Regione	10
1.6	Analisi della distribuzione geopolitica delle minacce filtrando per Anno (2000-2010)	11
1.7	Analisi della distribuzione geopolitica delle minacce filtrando per Anno (2000-2010) e Regione (<i>Middle East & North Africa, Sub-Saharan Africa</i>)	11
1.8	Analisi della distribuzione geopolitica delle minacce filtrando per Anno, Regione e Criticità	12
1.9	Analisi delle tattiche di attacco e armamenti	13
1.10	Analisi delle tattiche di attacco e armamenti: filtro suicidio	15
1.11	Analisi delle tattiche di attacco e armamenti: filtro Bersaglio	15
1.12	Analisi delle tattiche di attacco e armamenti: filtro Bersaglio Cittadini	16
1.13	Analisi delle tattiche di attacco e armamenti: filtro Bersaglio Turisti	16
1.14	Dettaglio operativo su <i>Educational Institutions</i> : KPI e tattiche in presenza di attacchi suicidi	17
1.15	Dettaglio operativo su <i>Educational Institutions</i> : KPI e tattiche per attacchi convenzionali (non suicidi)	17

Elenco delle tabelle

1	Elenco completo delle 27 variabili selezionate dal GTD.	2
2.1	Confronto del tasso di letalità previsto tra South Asia e North America.	22

Introduzione

In uno scenario geopolitico caratterizzato da crescenti tensioni e conflitti asimmetrici, la minaccia terroristica evolve rapidamente nelle sue modalità operative e strategiche, sfidando la stabilità della sicurezza internazionale. In questo contesto, la presente tesina si propone di esplorare le dinamiche della violenza politica sotto molteplici prospettive: valutando l'impatto umano ed economico, l'evoluzione del *Modus Operandi* (tattiche e armamenti), l'efficacia delle azioni offensive (Successo vs Fallimento) e la distribuzione geografica delle zone di crisi a livello globale.

Nello specifico, l'indagine si basa sul dataset *Global Terrorism Database (GTD)*, sviluppato dal consorzio START dell'Università del Maryland, che raccoglie e sistematizza i dati relativi agli incidenti terroristici registrati dal 1970 ad oggi. Il dataset offre una visione granulare su variabili cruciali quali la tipologia di attacco (es. *Bombing*, *Armed Assault*, *Hijacking*), la natura del bersaglio colpito (*Target Type*: Civili, Militari, Business), i danni materiali ed economici generati e l'identità dei gruppi responsabili. Il dataset rappresenta la fonte open-source più completa e autorevole in questo dominio, presentando un elevato livello di dettaglio storico e strutturale.

Le analisi sono state condotte mediante l'utilizzo di avanzati software di *Business Intelligence* (tra cui *Qlik Sense*, *Power BI* e *Tableau*), che hanno permesso di trasformare oltre 180.000 record grezzi in *dashboard interattive*. Questo approccio metodologico ha consentito di simulare un processo di *Intelligence Analysis* orientato ai dati (*Data-Driven Intelligence*), fornendo risposte concrete a specifiche domande strategiche e identificando pattern temporali e spaziali non rilevabili tramite una semplice analisi tabellare.

0.1 Approfondimento del Dataset Global Terrorism Database (GTD)

Da modificare prima e dopo pulizia

Il dataset selezionato per questo progetto rappresenta la risorsa più completa e autorevole a livello mondiale per l'analisi quantitativa del terrorismo. Esso si compone di oltre 180.000 *record*, ciascuno rappresentante un singolo evento terroristico unico, e copre un arco temporale che va dal 1970 al 2017.

La struttura del dataset è stata progettata per offrire una visione olistica del fenomeno della violenza politica: non si limita a registrare l'evento spaziale, ma ne traccia le modalità tattiche (*Modus Operandi*), gli attori responsabili (Gruppi terroristici) e le conseguenze umane ed economiche.

Di seguito viene riportato il *Dizionario dei Dati* (Tabella 1), che descrive nel dettaglio il significato di ciascuna variabile utilizzata nelle successive dashboard di Business Intelligence:

Tabella 1: Elenco completo delle 27 variabili selezionate dal GTD.

Nome Colonna	Descrizione
eventid	Identificativo univoco numerico dell'evento (Chiave Primaria).
iyear	Anno in cui si è verificato l'incidente.
imonth	Mese in cui si è verificato l'incidente (0 se sconosciuto).
iday	Giorno in cui si è verificato l'incidente (0 se sconosciuto).
country_txt	Nome della Nazione in cui è avvenuto l'attacco.
region_txt	Macro-regione geografica (es. Medio Oriente, Nord America).
provstate	Nome della Provincia o dello Stato amministrativo (es. Texas, Baghdad).
city	Nome della città o del villaggio specifico.
latitude	Coordinata geografica (Latitudine) dell'evento.
longitude	Coordinata geografica (Longitudine) dell'evento.
Crit1	Indicatore binario (1/0) se l'evento è violento o minaccia di violenza.
Crit2	Indicatore binario (1/0) se l'evento è perpetrato da un gruppo non statale.
Crit3	Indicatore binario (1/0) se l'evento ha uno scopo politico, religioso, ideologico o sociale.
attacktype1_txt	Categoria principale della tattica d'attacco (es. Bombardamento).
weaptype1_txt	Categoria generale dell'arma utilizzata (es. Esplosivi).
weapsubtype1_txt	Sottocategoria specifica dell'arma (es. Dinamite, Mina terrestre).
suicide	Indicatore binario (1/0) se l'attacco è stato suicida.
success	Indicatore binario (1/0) se l'attacco ha raggiunto l'obiettivo tattico.
targtype1_txt	Categoria generale del bersaglio (es. Civili, Militari).
targsubtype1_txt	Sottocategoria specifica del bersaglio (es. Ristorante, Caserma).
corp1	Nome dell'ente, azienda o gruppo specifico colpito.
natlty1_txt	Nazionalità delle vittime colpite.
gname	Nome del gruppo terroristico responsabile o sospettato.
claimed	Indicatore binario (1/0) se l'attacco è stato rivendicato ufficialmente.
nperps	Numero di terroristi che hanno partecipato all'azione.
nkill	Numero di persone decedute (Morti).
nwound	Numero di persone ferite.
propvalue	Valore stimato del danno economico alla proprietà (in USD).

Continua nella prossima pagina...

Tabella 1 – continua dalla pagina precedente

Nome Colonna	Descrizione
ishostkid	Indicatore binario (1/0) se l'evento è un rapimento/presa ostaggi.
ransomamt	Importo del riscatto richiesto (in USD).

0.1.1 Qualità dei Dati e Preparazione (ETL)

Data la complessità e la vastità del *Global Terrorism Database* (GTD), prima di procedere con l'importazione nei software di Business Intelligence, è stata necessaria una fase strutturata di *Data Cleaning e preparazione dei dati (ETL – Extract, Transform, Load)*. L'obiettivo principale è quello di rendere i dati accessibili, puliti e strutturati, così da supportare in modo efficace le analisi.

In particolare, sono stati eseguiti i seguenti passaggi:

1. *Selezione delle colonne rilevanti*:

Dal dataset originale sono state estratte solo le colonne necessarie per l'analisi, suddivise per categorie: identificativi, dati geografici, criteri di terrorismo, tattiche e armi, obiettivi, gruppi e terroristi, impatto e vittime. Questa operazione ha permesso di ridurre il dataset ai soli dati utili, migliorando la leggibilità e le performance di calcolo nelle fasi successive.

2. *Gestione delle date incomplete*:

Alcuni record presentavano giorno o mese sconosciuti, indicati con valore "0". Per garantire la compatibilità con Qlik Sense, Tableau e Power BI, è stata creata una *colonna unificata date*, combinando anno, mese e giorno. I valori sconosciuti sono stati sostituiti con "1", evitando errori nella lettura e permettendo aggregazioni temporali coerenti.

3. *Normalizzazione dei valori numerici*:

Alcune colonne numeriche, come numero di morti, feriti, terroristi coinvolti, danni economici e riscatti richiesti, contenevano il codice "-99" a indicare valori sconosciuti. Tali valori sono stati convertiti in *NaN* (Not a Number) per distinguerli dai valori effettivamente pari a zero. Inoltre, tutte le colonne sono state convertite in formato numerico per garantire la corretta interpretazione dei dati. Questo passaggio consente di evitare distorsioni nelle analisi statistiche e nei KPI, preservando la distinzione tra dati mancanti e valori reali.

4. *Verifica della qualità dei dati*:

Il dataset è stato controllato per valori nulli e duplicati, confermando che non esistono record che possano alterare aggregazioni statistiche o analisi temporali. Anche le colonne numeriche sono state verificate per assicurare la coerenza dei formati e la precisione dei calcoli.

5. *Preparazione per l'analisi BI*:

Al termine del preprocessing, il dataset risultante è stato salvato come *CSV pulito e standardizzato*, pronto per essere importato nei software di Business Intelligence. La struttura dei dati, con colonne coerenti e valori numerici normalizzati, consente di creare dashboard affidabili e KPI precisi senza rischio di errori derivanti da dati mancanti o codifiche anomale.

Nota metodologica:

Questa fase di ETL è fondamentale per trasformare un dataset grezzo e complesso in un

formato *immediatamente utilizzabile* per analisi visive, aggregazioni temporali e comparazioni geografiche, migliorando la robustezza delle dashboard di Qlik Sense, Tableau e Power BI.

0.1.2 Preprocessing dei Dati in Python

Per preparare il dataset del *Global Terrorism Database* per l'importazione nei software di Business Intelligence, è stato utilizzato Python con la libreria pandas e numpy. Di seguito sono descritti i principali passaggi eseguiti.

- ### **1. Importazione delle librerie e caricamento del dataset:**

```
import pandas as pd
import numpy as np

file_path = "/Users/antonio/Desktop/globalterrorismdb_0718dist.csv"

columns_of_interest = [
    "eventid", "country_txt", "region_txt", "provstate", "city", "latitude",
    "longitude", "latlong", "attacktype1_txt", "weaptype1_txt", "weapsubtype1_txt", "suicide",
    "targtype1_txt", "targsubtype1_txt", "corp1", "natlty1_txt",
    "gname", "claimed", "nperps",
    "nkill", "nwound", "propvalue", "ishostkid", "ransomamt",
    "iyear", "imonth", "iday"
]
```

2. Pulizia dei valori numerici: sostituzione di -99 con NaN

```
numeric_cols_unknown = ["nkill", "nwound", "propvalue", "ransomamt", "np  
for col in numeric_cols_unknown:  
    df[col] = pd.to_numeric(df[col], errors='coerce')  
    df[col] = df[col].replace(-99, np.nan)
```

3. *Creazione di una colonna data unificata:* combinazione di anno, mese e giorno in una singola colonna date.

```
def create_date(row):
    try:
        year = int(row['iyear'])
        month = int(row['imonth']) if row['imonth'] != 0 else 1
        day = int(row['iday']) if row['iday'] != 0 else 1
        return pd.Timestamp(year=year, month=month, day=day)
    except:
        return np.nan

df['date'] = df.apply(create_date, axis=1)
df = df.drop(columns=['iyear', 'imonth', 'iday'])
```

4. *Esplorazione del dataset pulito:* visualizzazione delle prime righe per controllo.

```
df.head()
```

5. *Salvataggio del dataset pulito:* creazione di un file CSV pronto per BI.

```
output_path = "/Users/antonio/Desktop/gtd_cleaned_CORRECT.csv"
df.to_csv(output_path, index=False, encoding='utf-8')
print("Dataset corretto generato.")
```

CAPITOLO 1

Qlik

In questo capitolo viene presentata l'implementazione di una soluzione di Business Intelligence mediante l'utilizzo di Qlik Sense, piattaforma che consente un'analisi interattiva e multidimensionale dei dati grazie al suo motore associativo. L'attenzione è rivolta alla modellazione dei dati e alla realizzazione di una dashboard strategica composta da diverse visualizzazioni, progettate per supportare in modo efficace il processo decisionale in ambito cybersecurity. Fondata nel 1993, Qlik offre soluzioni di Business Intelligence che facilitano l'esplorazione autonoma dei dati, permettendo agli utenti di individuare relazioni e correlazioni in modo dinamico. A differenza degli strumenti tradizionali basati esclusivamente su interrogazioni SQL, Qlik consente un approccio analitico più flessibile e intuitivo, riducendo i tempi di analisi e accelerando l'individuazione di insight rilevanti. Nel contesto del presente progetto, Qlik Sense è stato impiegato per effettuare un'analisi descrittiva delle minacce di cybersecurity a livello globale, fornendo una visione d'insieme sull'evoluzione temporale degli attacchi, sulle tipologie di minacce più diffuse e sulle aree geografiche maggiormente colpite.

1.1 Analisi descrittiva

L'analisi descrittiva rappresenta un aspetto fondamentale della Business Intelligence (BI), focalizzandosi sull'esplorazione e l'interpretazione dei dati storici per offrire una panoramica chiara e dettagliata delle attività passate di un'organizzazione. Attraverso strumenti di aggregazione, visualizzazione e reporting, questa tipologia di analisi consente alle aziende di riconoscere pattern, trend e comportamenti rilevanti all'interno dei propri dati, trasformandoli in conoscenze pratiche e facilmente fruibili.

1.2 Caricamento dei dati su Qlik

Il caricamento dei dati in Qlik rappresenta un passaggio essenziale per importare informazioni provenienti da diverse fonti, tra cui file in formato CSV. Questo processo inizia con la corretta preparazione del file, che deve presentare un'intestazione chiara e dati coerenti.

Prima dell'importazione, è stata effettuata una fase preliminare di verifica della qualità dei dati (Data Quality Assessment).

Attraverso l'interfaccia di Qlik, si definisce l'applicazione e, successivamente, si inserisce il dataset da analizzare, come mostrato nelle figure 1.1 e 1.2.

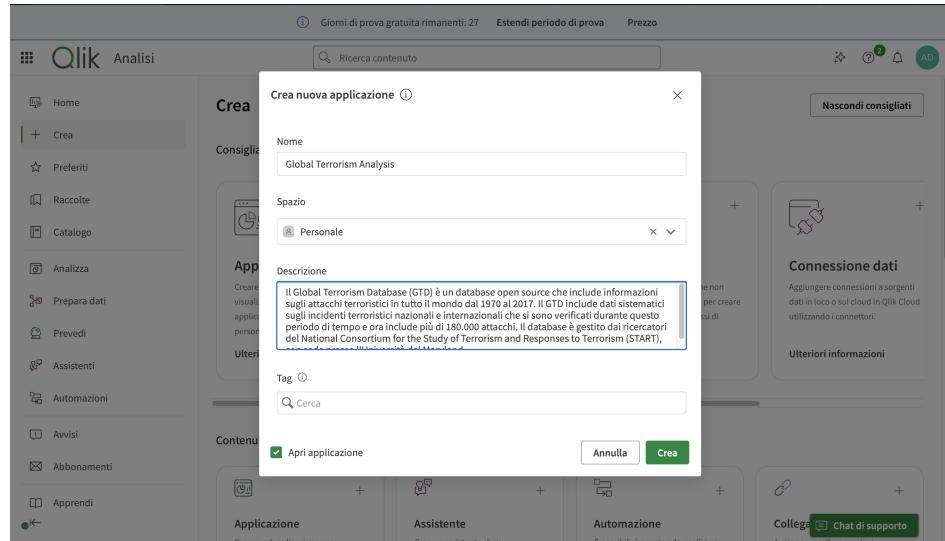


Figura 1.1: Creazione dell'applicazione

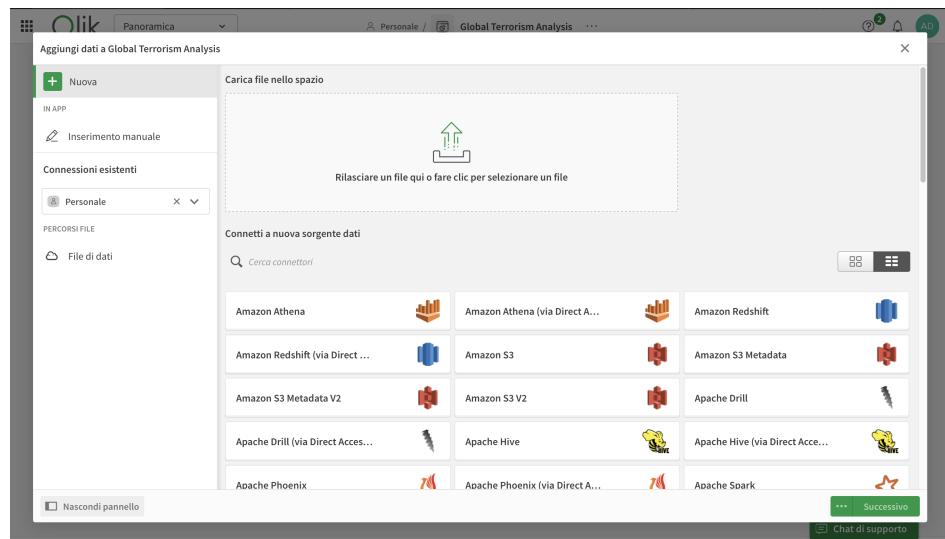


Figura 1.2: Upload del Dataset

Per questo lavoro, è stato utilizzato un singolo file CSV, pertanto non si è fatto ricorso alla funzione di "Gestione Dati" per la combinazione di più file. Tale scelta ha semplificato il flusso di lavoro, permettendo di integrare rapidamente le informazioni necessarie per le successive analisi.

1.2.1 Data Analysis Dataset Global Terrorism Database

Una volta completata la fase di caricamento e preparazione dei dati, si procede all'analisi del dataset attraverso l'utilizzo delle *dashboard*. Queste rappresentano il principale strumento di esplorazione dei dati e consentono di creare grafici interattivi, applicare filtri dinamici e utilizzare funzionalità di selezione che permettono di analizzare le informazioni da diversi punti di vista.

L'uso delle dashboard facilita l'individuazione di pattern ricorrenti, trend temporali e relazioni tra le variabili, rendendo possibile un'analisi approfondita e intuitiva del fenomeno studiato. Inoltre, grazie al modello associativo di Qlik Sense, ogni interazione effettuata su un

grafico si riflette automaticamente sugli altri, permettendo di ottenere una visione coerente e integrata dei dati e supportando il processo decisionale.

Nelle sezioni a seguire verranno esaminate nel dettaglio le diverse *dashboard* sviluppate, illustrandone le principali funzionalità, i grafici utilizzati e le analisi specifiche condotte. In particolare, l'attenzione sarà rivolta alle seguenti aree di studio:

- analisi della distribuzione geopolitica delle minacce;
- analisi delle tipologie di attacco e degli armamenti;
- analisi dell'impatto economico e danni causati;
- Analisi dell'evoluzione temporale del fenomeno del terrorismo.

1.3 Analisi della distribuzione geopolitica delle minacce

La Dashboard, mostrata in Figura 1.3, analizza lo scenario globale delle zone di crisi e la profilazione dei gruppi terroristici, focalizzandosi sulla relazione tra instabilità geografica, attori coinvolti e tipologia di obiettivi colpiti. Nel dettaglio, il sistema mostra i principali indicatori di performance (KPI) legati all'impatto complessivo degli eventi: il numero totale degli attentati, il numero delle vittime (morti) e il numero dei feriti.

La visualizzazione principale è costituita da una Mappa Geografica interattiva che identifica gli "Hotspot¹" del terrorismo globale. Ogni evento è rappresentato da un punto la cui dimensione varia in base alla letalità dell'attacco. Per facilitare l'analisi visiva, è stata applicata una formattazione condizionale "a semaforo" basata sul numero di vittime:

- il colore *Verde* identifica gli eventi a bassa letalità (0-1 vittime);
- il colore *Giallo* identifica gli eventi con impatto medio (2-10 vittime);
- il colore *Rosso* identifica le stragi o gli eventi critici (oltre 10 vittime);

Accanto alla mappa, la Treemap (Mappa ad Albero) permette di profilare i gruppi terroristici più attivi (come Taliban, ISIL o Boko Haram) e i loro bersagli prediletti (Civili, Militari, Business). Il grafico è configurato per escludere i dati classificati come "Unknown", garantendo così una visione specifica sulle gerarchie dei gruppi identificati. Sono inoltre presenti filtri per *Regione* e per *Anno*, che consentono una visione dinamica della distribuzione del terrorismo, permettendo di osservare come il fenomeno sia cambiato dagli anni '80 a oggi.

1.3.1 Utente

L'utente a cui è destinata questa dashboard è un analista specializzato nel settore della Difesa e degli Affari Esteri. Tale figura professionale utilizza lo strumento per monitorare costantemente le aree di crisi a livello globale, identificando pattern di violenza, dinamiche di conflitto e tendenze emergenti nei diversi contesti geopolitici. L'analisi fornita dalla dashboard supporta i decisori politici e militari nel comprendere quali regioni stiano attraversando processi di instabilità e quali gruppi armati stiano aumentando il proprio potere operativo o sviluppando nuove capacità tattiche. In questo modo, lo strumento contribuisce a una pianificazione strategica più informata e a interventi mirati nelle zone a rischio.

¹Nel contesto del terrorismo internazionale, un hotspot è un'area geografica caratterizzata da un'elevata concentrazione di eventi terroristici o da un livello particolarmente alto di instabilità e violenza politica in un determinato periodo di tempo.

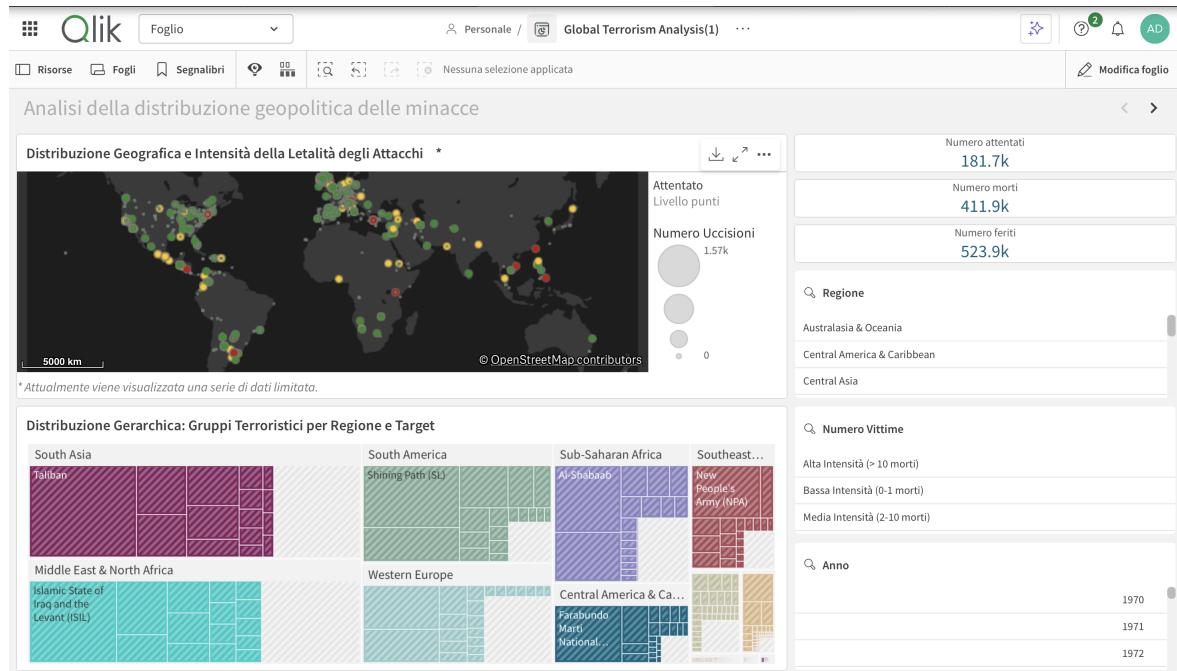


Figura 1.3: Analisi della distribuzione geopolitica delle minacce

1.3.2 Obiettivo

L’obiettivo principale di questa analisi è trasformare dati storici complessi sulla minaccia terroristica in informazioni strategiche utili. La dashboard permette di:

- Identificare pattern di letalità, distinguendo aree a bassa intensità da zone con eventi catastrofici.
- Monitorare l’evoluzione dei gruppi terroristici e la loro influenza geografica.
- Supportare il decision-making fornendo evidenze per comprendere quali attori rappresentino la minaccia maggiore.

In sintesi, l’analisi mira a svelare le dinamiche della violenza politica, andando oltre il semplice conteggio degli eventi, per prevedere potenziali aree di futura crisi.

1.3.3 Filtri ed esempi di utilizzo

L’efficacia della dashboard risiede nella sua natura dinamica: l’integrazione dei filtri permette all’analista di esplorare i dati in modo interattivo per isolare specifici fenomeni o periodi storici. Di seguito vengono riportati due esempi pratici di utilizzo che dimostrano la capacità dello strumento di estrarre informazioni mirate dal dataset.

Evoluzione degli "Hotspot" e della Matrice Ideologica (Filtro Anno e Regione)

Questo scenario risponde alle domande: "Quali nazioni sono i principali Hotspot?" e "Chi sono i gruppi più attivi?".

Utilizzando lo Slider temporale, è possibile confrontare due epoche distinte per osservare il mutamento del baricentro del terrorismo e della tipologia di violenza.

- **Scenario A (1980-1989):** La mappa evidenzia una forte concentrazione di eventi in America Latina e in Europa Occidentale, come mostrato in Figura 1.4. I KPI e le bolle rosse indicano picchi di alta letalità anche in occidente, come nel caso della strage di Bologna (85 morti). Utilizzando il filtro Regione su *Western Europe* e *South America*, la Treemap permette di isolare i principali attori (es. Sendero Luminoso, IRA, ETA), rivelando visivamente che le motivazioni dominanti del periodo erano di natura *prettamente ideologica e politica*, come mostrato in Figura 1.5

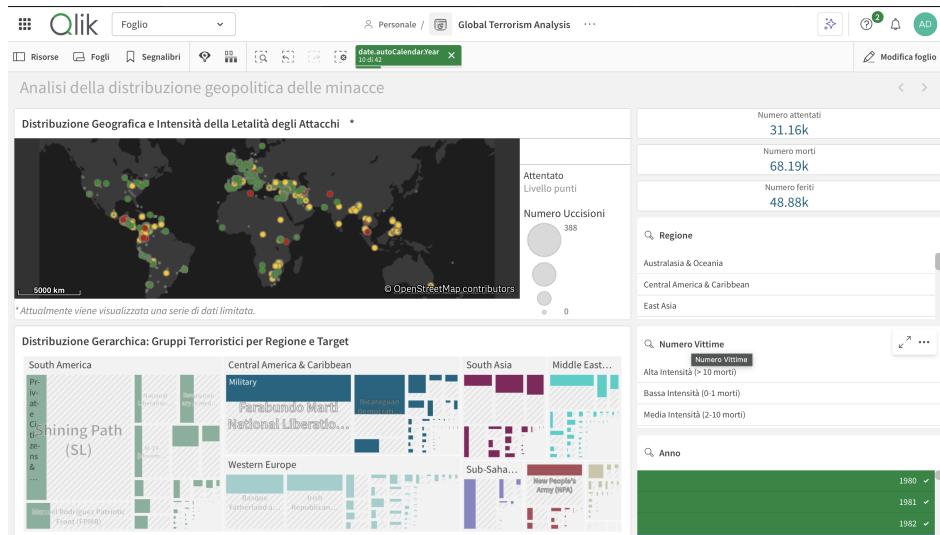


Figura 1.4: Analisi della distribuzione geopolitica delle minacce filtrando per Anno

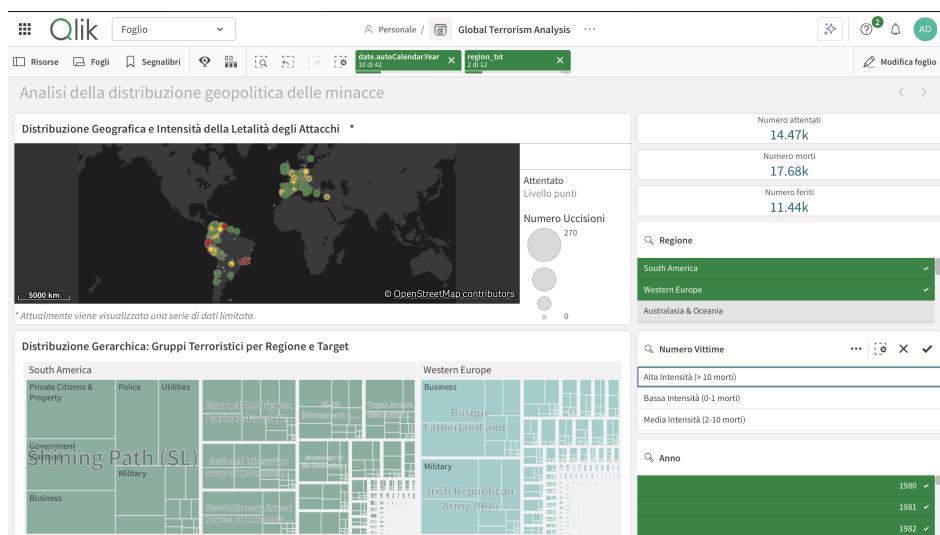


Figura 1.5: Analisi della distribuzione geopolitica delle minacce filtrando per Anno e Regione

- **Scenario B (Dal 2000 ad oggi - L'era del Fondamentalismo):** Impostando il filtro temporale a partire dall'anno 2000, la dashboard visualizza una radicale migrazione degli "Hotspot" dall'Occidente verso il Medio Oriente (Iraq, Afghanistan) e l'Africa Subsahariana (Nigeria), come mostrato in Figura 1.6. La Treemap diventa fondamentale per comprendere l'evoluzione degli attori: essa evidenzia prima la dominanza di Al-Qaida e degli estremisti islamici, come mostrato in Figura 1.7. In questo scenario, la matrice religiosa

e transnazionale sostituisce quella politica locale, caratterizzandosi per un volume di attacchi massivo e una letalità spesso elevata (bolle Rosse e Gialle diffuse).

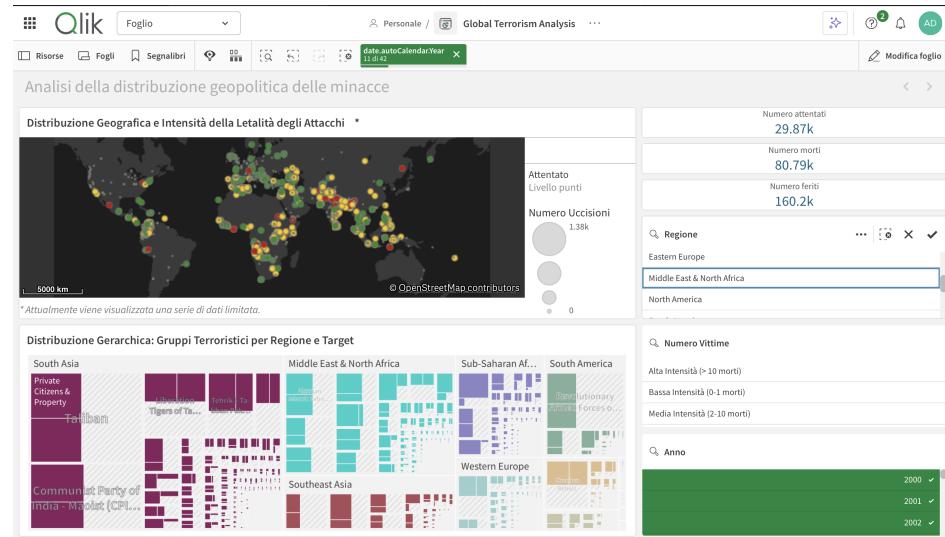


Figura 1.6: Analisi della distribuzione geopolitica delle minacce filtrando per Anno (2000-2010)

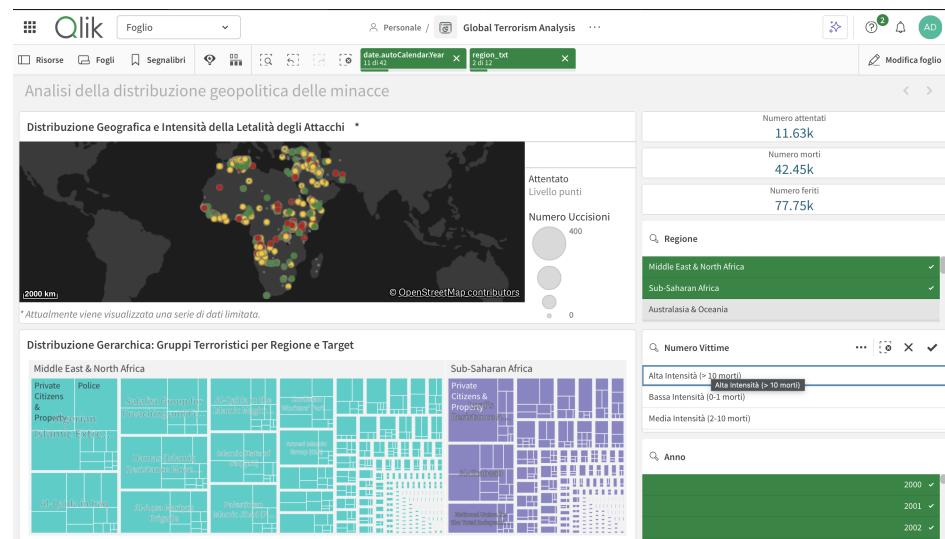


Figura 1.7: Analisi della distribuzione geopolitica delle minacce filtrando per Anno (2000-2010) e Regione (Middle East & North Africa, Sub-Saharan Africa)

Analisi della Letalità (Filtro per Criticità)

Infine, per rispondere alla domanda di ricerca: "Qual è l'impatto reale degli attacchi e come distinguere la micro-conflittualità dalle grandi stragi?", è stato implementato il filtro *Numero Vittime*.

Questo strumento permette di segmentare il dataset in base al numero di vittime (*nkill*), applicando la stessa logica "a semaforo" visibile sulla mappa:

- *Bassa Intensità (Verde - 0/1 morti)*: Isola la frequenza degli attacchi intimidatori o falliti.
- *Media Intensità (Giallo - 2/10 morti)*: Evidenzia gli scontri tattici.

- *Alta Intensità (Rosso - >10 morti)*: Permette di visualizzare esclusivamente i "Mass Casualty Events", pulendo la mappa dal "rumore di fondo" per far emergere solo le crisi umanitarie più gravi.

Impostando i filtri su Regione (North America), intervallo temporale 2000-2010 e Criticità (Alta / > 10 morti), come mostrato in Figura 1.8, la dashboard isola immediatamente l'evento più impattante della storia contemporanea.

- *Visualizzazione*: La mappa si svuota quasi completamente, lasciando emergere i punti focali su New York e Washington (Pentagono).
- *Attori e Responsabilità*: La Treemap (o l'analisi dei gruppi) identifica inequivocabilmente Al-Qaida come attore dominante e unico responsabile di questo picco di violenza.
- *Analisi dei Target*: L'analisi dei bersagli conferma la natura sistematica e coordinata dell'attacco, diretto simultaneamente contro obiettivi istituzionali (Government/Military) e civili-finanziari (Private citizens & Property), riflettendo la strategia del gruppo di colpire i simboli del potere politico ed economico.

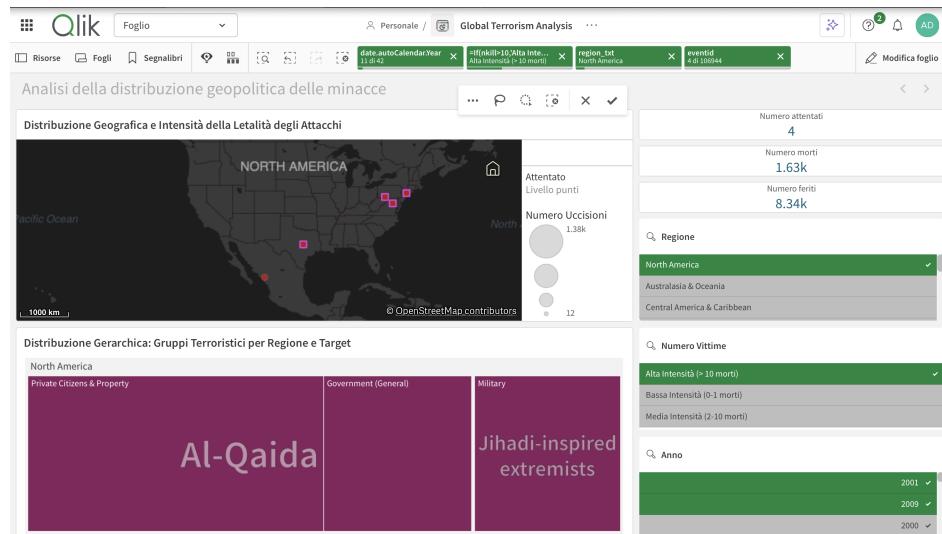


Figura 1.8: Analisi della distribuzione geopolitica delle minacce filtrando per Anno, Regione e Criticità

Questo esempio dimostra come l'uso combinato dei filtri permetta di ricostruire l'identikit completo di un attentato (Chi, Dove, Contro Chi) in pochi secondi.

1.4 Analisi delle tattiche di attacco e armamenti

La Dashboard, mostrata in Figura 1.9, analizza le strategie operative e la sofisticazione militare dei gruppi terroristici, focalizzandosi sulla relazione tra il "Modus Operandi" adottato (tipologia di attacco), gli armamenti utilizzati e la letalità risultante. Nel dettaglio, il sistema monitora i principali indicatori di performance (KPI) legati all'efficienza dell'azione: il Tasso di Successo (%) degli attacchi e il numero totale di eventi analizzati.

La visualizzazione della distribuzione tattica è costituita da un Grafico a Ciambella (Donut Chart), che ripartisce le modalità di attacco predominanti (come Bombing, Armed Assault o Hijacking). Questa vista offre una percezione immediata della composizione percentuale della minaccia, permettendo di distinguere se un gruppo predilige l'uso di esplosivi o azioni di guerriglia armata.

Accanto alla ripartizione tattica, il Grafico Combinato (Combo Chart) a doppio asse permette di confrontare la frequenza d'uso delle armi con la loro letalità effettiva. In questa configurazione:

- le *barre* indicano il volume di utilizzo di ogni arma (Frequenza);
- la *linea* sovrapposta traccia il numero totale delle vittime causate (Letalità).

Questa struttura permette di identificare le asimmetrie del conflitto, isolando le armi che, pur essendo usate raramente, causano un numero elevato di vittime. Sono inoltre presenti filtri interattivi per *Fattore Suicida (Suicide)* e *Tipo di Bersaglio (Target Type)*, che consentono una visione dinamica degli scenari operativi, permettendo di osservare come variano le tattiche in base all'obiettivo colpito.

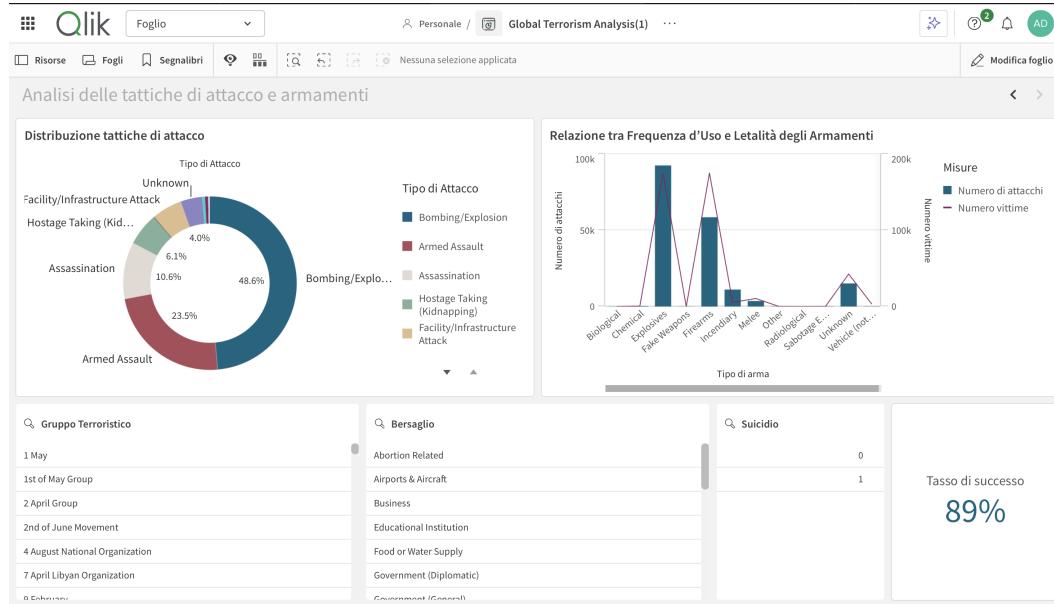


Figura 1.9: Analisi delle tattiche di attacco e armamenti

1.4.1 Utente

L'utente a cui è destinata questa dashboard è un Comandante Operativo o un Analista di Intelligence Tattica, specializzato nel contrasto alle minacce asimmetriche. Tale figura professionale utilizza lo strumento per decodificare il modus operandi delle organizzazioni ostili, valutando la sofisticazione degli armamenti e la relazione critica tra la frequenza degli

attacchi e la loro letalità effettiva. L’analisi fornita dalla dashboard supporta i responsabili della sicurezza nazionale e delle forze speciali nel distinguere tra minacce convenzionali e scenari ad alto impatto (come attentati suicidi o l’uso di esplosivi complessi). In questo modo, lo strumento contribuisce alla definizione di protocolli di ingaggio efficaci e all’ottimizzazione delle risorse di intervento, permettendo di adeguare l’equipaggiamento difensivo e le procedure di risposta alle specifiche tipologie di tattica rilevate sul campo.

1.4.2 Obiettivo

L’obiettivo principale dell’analisi è comprendere e decodificare le modalità operative nonché il livello di sofisticazione militare delle organizzazioni terroristiche. La dashboard consente di:

- identificare le tattiche di attacco predominanti, distinguendo tra minacce di tipo convenzionale (ad esempio assalti armati) e modalità caratterizzate da elevato impatto psicologico e materiale (quali attentati suicidi o utilizzo di esplosivi).
- Valutare l’efficacia degli armamenti impiegati, mettendo in relazione la frequenza d’uso delle diverse categorie di armi con il relativo tasso di letalità.
- Supportare la preparazione operativa attraverso evidenze empiriche sulle capacità offensive dei gruppi, favorendo l’adeguamento delle misure difensive in funzione della tipologia di minaccia rilevata.

In sintesi, l’analisi non si limita a contare gli eventi, ma cerca di comprendere le dinamiche operative che li caratterizzano, al fine di anticipare l’evoluzione delle minacce asimmetriche e rafforzare la resilienza dei bersagli critici.

1.4.3 Filtri ed esempi di utilizzo

L’efficacia della dashboard risiede nella sua natura dinamica: l’integrazione dei filtri permette all’analista di esplorare i dati in modo interattivo per isolare scenari complessi e verificare ipotesi investigative in tempo reale. Attraverso la selezione mirata delle variabili, è possibile rispondere a quesiti operativi specifici:

- **1. Quali sono le modalità di attacco predominanti?** L’analisi del Grafico a Ciambella evidenzia una netta prevalenza della categoria *Bombing/Explosion*, che costituisce la modalità standard per la maggioranza dei gruppi armati, seguita dagli assalti armati (*Armed Assault*). L’applicazione del filtro *Suicide* conferma e radicalizza questa tendenza: in presenza di attacchi suicidi, l’uso di *Explosives* diventa l’armamento quasi esclusivo, marginalizzando drasticamente altre modalità come gli assalti armati (*Armed Assault*). Questo dato conferma che il vettore suicida è tatticamente concepito quasi sempre come un sistema di guida umano per ordigni esplosivi.

La Figura 1.10 mostra la dashboard con il filtro applicato.

- **2. Qual è il tasso di letalità per ogni tipo di arma?** Applicando il filtro *Bersaglio = Airports & Aircraft*, il Grafico Combinato permette di isolare la minaccia specifica per il settore aviazione. L’analisi visiva evidenzia che gli *Explosives* (Esplosivi) costituiscono l’arma nettamente più utilizzata in termini di frequenza (Barra più alta). Il confronto con la linea della letalità conferma inoltre che gli esplosivi detengono il primato assoluto del tasso di mortalità per questo scenario, superando drasticamente l’impatto di altre

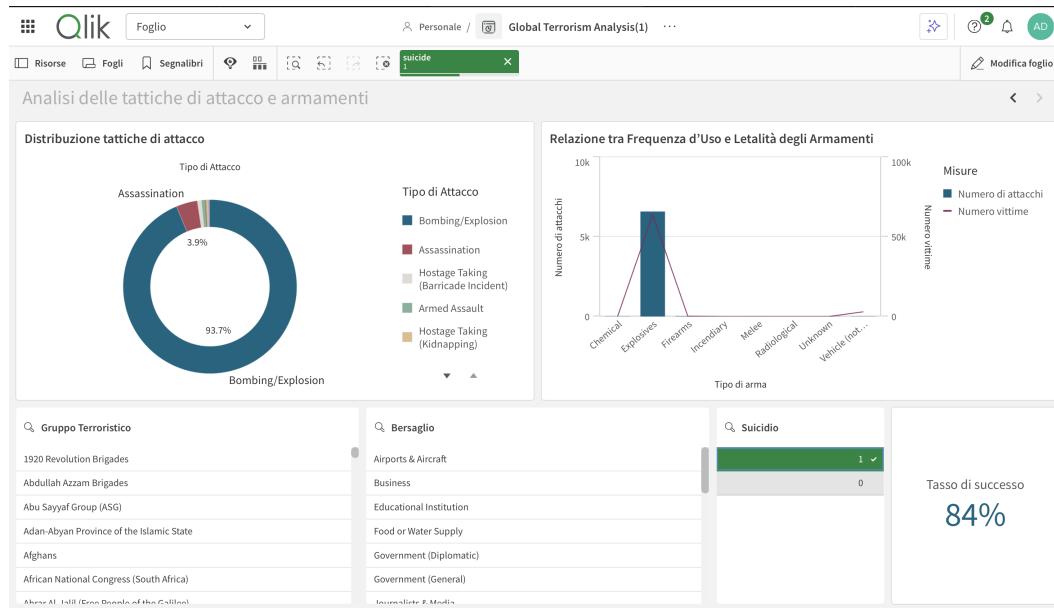


Figura 1.10: Analisi delle tattiche di attacco e armamenti: filtro suicidio

armi come *Firearms* o *Incendiary*, che pur essendo presenti, registrano livelli di letalità marginali.

La Figura 1.11 mostra la dashboard con il filtro applicato.

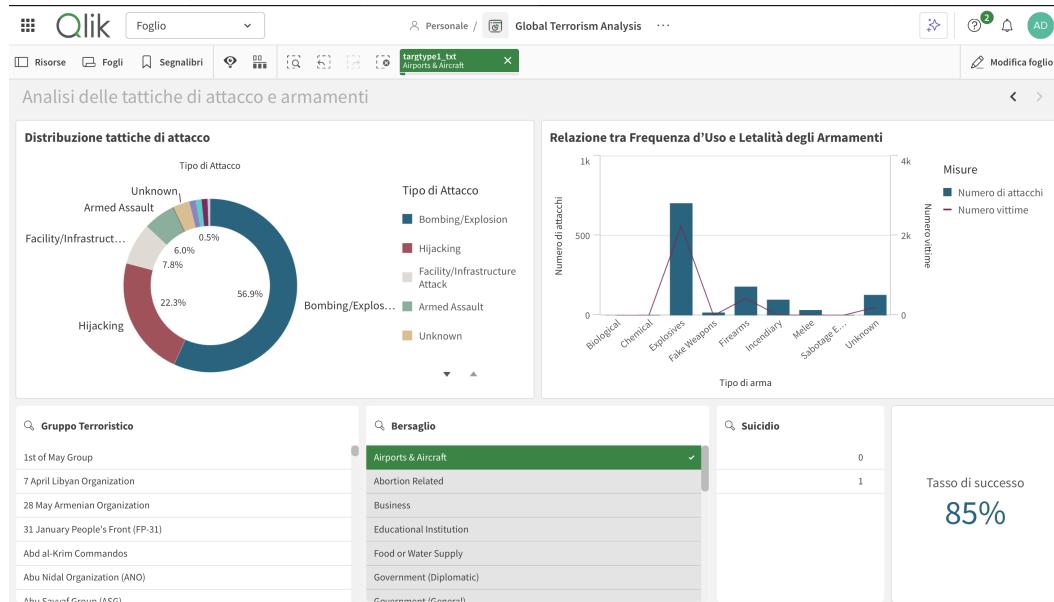


Figura 1.11: Analisi delle tattiche di attacco e armamenti: filtro Bersaglio

- **3. Adattamento Tattico al Bersaglio** Confrontando le modalità di attacco del gruppo Taliban su due categorie di vittime distinte, *Tourists* (Turisti) e *Private Citizens & Property* (Cittadini Privati), emerge una significativa variazione del *modus operandi*. Mentre contro i cittadini privati la tattica predominante è l'uso massiccio di *Bombing/Explosion* e *Armed Assault*, volto a generare intimidazione diffusa e destabilizzazione sociale, contro i turisti si osserva uno scenario tattico più composito. Sebbene emerga un'incidenza rilevante di *Hostage Taking* (Presa di Ostaggi) per il suo elevato valore negoziale e media-

tico, le modalità più convenzionali non vengono abbandonate: sia il *Bombing/Explosion* che l'*Armed Assault* registrano infatti una frequenza del 33,3% ciascuno. Ciò evidenzia una capacità strategica di differenziare l'azione operativa, alternando la violenza indiscriminata contro la popolazione locale a un mix di attacchi diretti e rapimenti mirati contro target internazionali.

Le dashboard sono mostrate nelle Figure 1.12 e 1.13

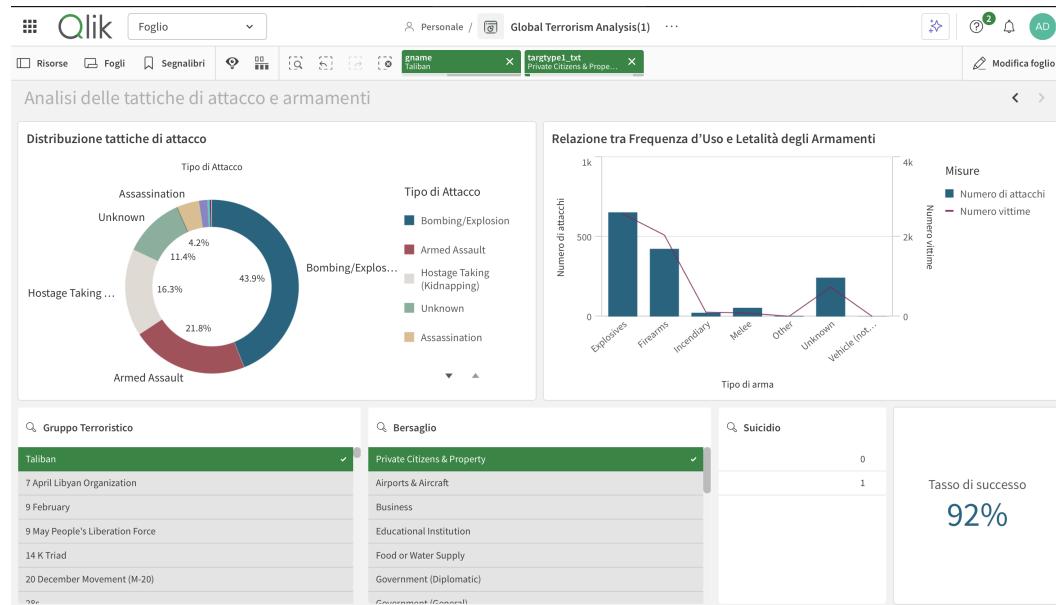


Figura 1.12: Analisi delle tattiche di attacco e armamenti: filtro Bersaglio Cittadini

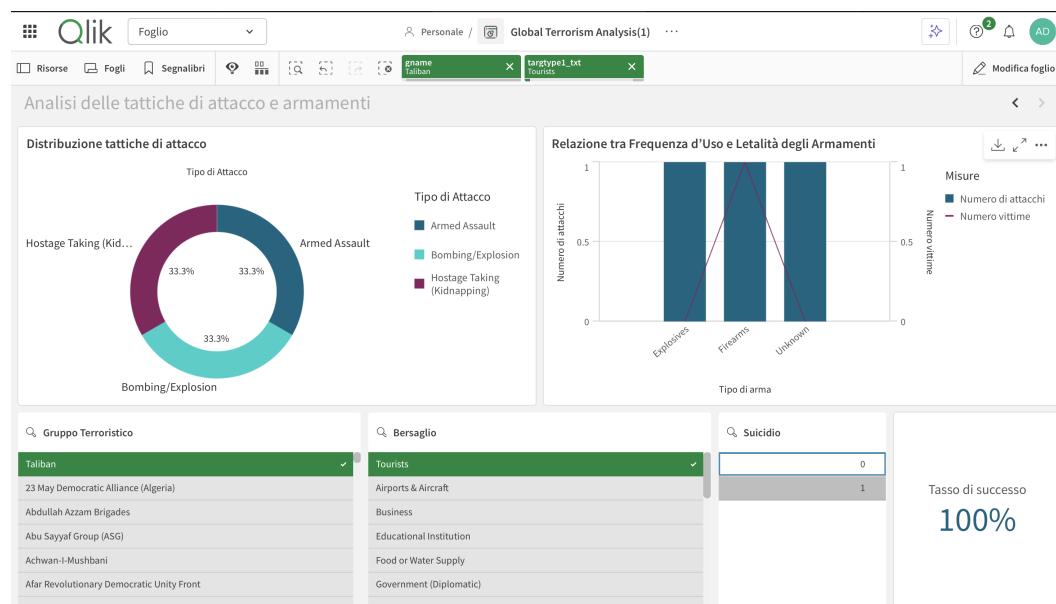


Figura 1.13: Analisi delle tattiche di attacco e armamenti: filtro Bersaglio Turisti

La dashboard, inoltre, permette verifiche puntuali su obiettivi specifici, come, ad esempio, gli *Educational Institutions* (Istituti Educativi). Confrontando le modalità di attacco tramite il KPI del *Success Rate*, emerge un risultato in controtendenza rispetto al dato globale: in questo contesto, gli attacchi suicidi (*Suicide = 1*) registrano un tasso di suc-

cesso inferiore rispetto alle modalità convenzionali, come mostrato nelle Figure 1.14 e 1.15.

Questo dato suggerisce che, mentre gli attacchi tradizionali (es. piazzamento di ordigni) risultano più difficili da prevenire in istituzioni educative accessibili, il tentativo di intrusione di un attentatore suicida viene più spesso intercettato o fallisce nella fase esecutiva.

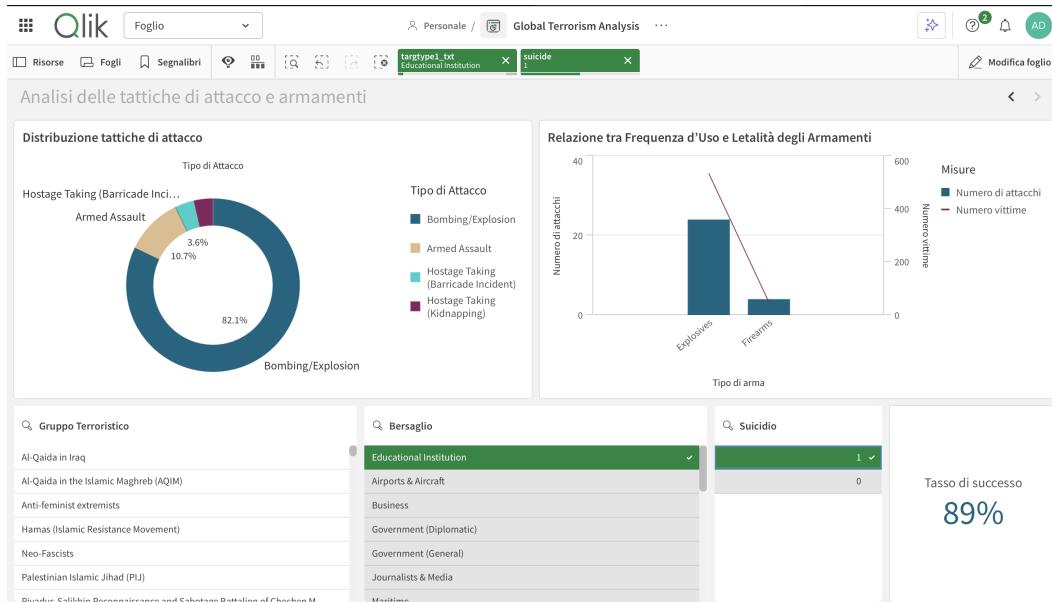


Figura 1.14: Dettaglio operativo su *Educational Institutions*: KPI e tattiche in presenza di attacchi suicidi

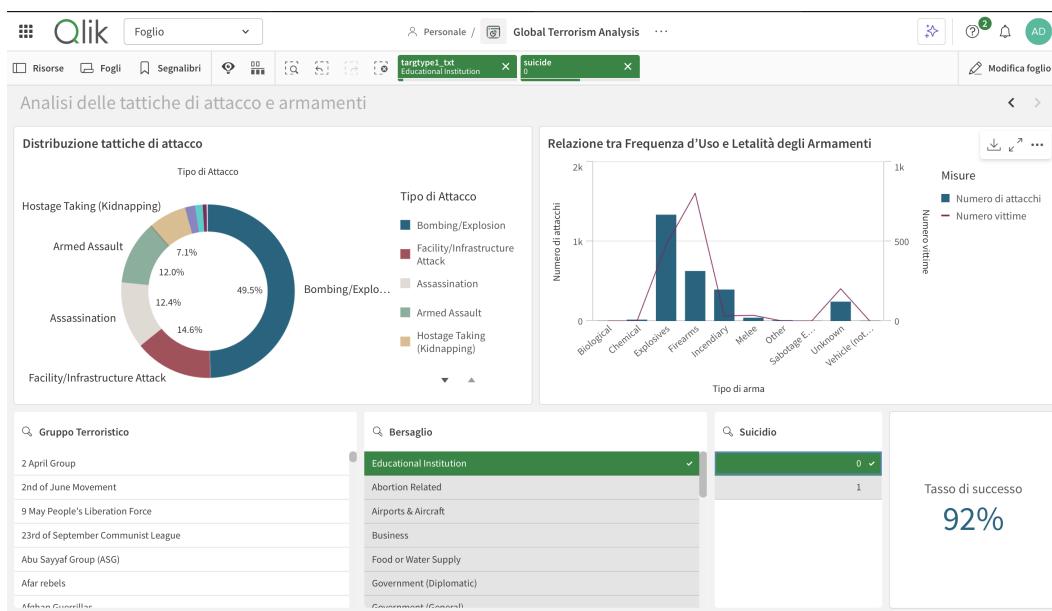


Figura 1.15: Dettaglio operativo su *Educational Institutions*: KPI e tattiche per attacchi convenzionali (non suicidi)

CAPITOLO 2

Tableau

Da scrivere

2.1 Introduzione

Il presente capitolo illustra la fase di **Data Visualization** e **Analisi Predittiva**, realizzata mediante l'utilizzo del software Tableau. La scelta di questo strumento è stata dettata dalla necessità di gestire un dataset complesso come il *Global Terrorism Database* (GTD), caratterizzato da una profonda serie storica (1970–2017) e da una natura multivariata (geografica, temporale e categorica).

L'obiettivo principale del progetto è trasformare i dati grezzi in informazioni strategiche (*Actionable Insights*). Non ci si è limitati a una rappresentazione descrittiva degli eventi passati, ma si è sfruttato il motore analitico di Tableau per implementare:

- **Modelli di Forecasting:** basati su tecniche di smussamento esponenziale per proiettare i trend futuri.
- **Clustering:** per individuare pattern nascosti e isolare anomalie all'interno dei dati.

L'analisi mira dunque a isolare le dinamiche della minaccia nel futuro immediato e a medio termine, fornendo una visione d'insieme chiara e scientificamente fondata.

2.2 Metodologia di Analisi

L'approccio analitico adottato segue un flusso logico strutturato in tre fasi distinte, necessarie per rispondere alle *Business Questions* definite in fase di progettazione:

1. **Analisi Descrittiva (Cosa è successo?):** Esplorazione dei trend storici per comprendere l'evoluzione del fenomeno, la distribuzione geografica degli attacchi e l'impatto in termini di vittime ed economia.
2. **Analisi Diagnostica (Perché è successo?):** Indagine sulle correlazioni tra variabili (es. relazione tra numero di feriti e numero di morti) e sulla segmentazione degli eventi tramite tecniche di clustering per isolare gli attacchi ad alta intensità.

3. **Analisi Predittiva (Cosa potrebbe succedere?):** Applicazione di algoritmi predittivi per stimare i volumi futuri degli attacchi, l'evoluzione della letalità e i target a rischio, fornendo supporto ai processi di pianificazione strategica e di sicurezza.

2.3 Strategia di Visualizzazione

Per garantire la massima leggibilità e interattività, le dashboard sono state progettate seguendo le *best practices* della Data Visualization. Ogni visualizzazione è stata costruita per rispondere a una specifica domanda chiave, utilizzando filtri dinamici (per Regione, Anno o Tipo di Attacco) che permettono all'utente di esplorare i dati a diversi livelli di granularità.

Sono state impiegate diverse tipologie di grafici avanzati, tra cui:

- **Dual Axis Chart:** per il confronto di metriche con scale differenti.
- **Scatter Plot:** per l'analisi di dispersione e correlazione.
- **Highlight Tables:** per la visualizzazione immediata delle densità di rischio tramite gradienti di colore.
- **Altro?**

2.4 Gestione della Qualità dei Dati

Una fase critica antecedente alla visualizzazione ha riguardato la bonifica dei campi relativi alle vittime: nkill (numero di morti) e nwound (numero di feriti). L'analisi preliminare nel Pannello Dati di Tableau ha evidenziato due problematiche strutturali:

1. **Errata Tipizzazione (Data Type Mismatch):** In fase di importazione, Tableau aveva interpretato queste colonne come stringhe. È stato necessario forzare il *Type Casting* in **Numerico Intero** per abilitare le aggregazioni matematiche (somme, medie).
2. **Gestione dei Valori Nulli (Missing Values):** Numerosi record presentavano valori vuoti. È stata applicata la funzione ZN() (*Zero Null*):

`nkill_fix = ZN([nkill])` → Se il valore è nullo, viene convertito in 0.

è stato fatto altro ?

2.5 Panoramica delle Dashboard Realizzate

Il progetto si articola in 7 Dashboard, organizzate in un percorso narrativo che parte dall'analisi storica globale per arrivare a previsioni specifiche su target e regioni:

- **Dashboard 1:** Analisi Temporale degli Attacchi e delle Vittime (Trend Storici).
- **Dashboard 2:** Analisi e Previsione della Letalità per Regione.
- **Dashboard 3:** Previsione dei Bersagli (Target) per Regione.
- **Dashboard 4:** Analisi degli Esiti dell'Attacco (Successo vs Fallimento).
- **Dashboard z:** Previsione del Volume degli Attacchi.
- **Dashboard y:** Previsione dell'Impatto Economico per Tipo di Attacco.
- **Dashboard x:** Previsione dell'Intensità (Vittime) per Tipo di Attacco e Arma.

2.5.1 Dashboard 1: Analisi Temporale degli Attacchi e delle Vittime

Obiettivo dell'Analisi

Questa dashboard rappresenta il punto di ingresso all'analisi storica, mettendo a confronto la **Frequenza** del fenomeno (Conteggio degli Attacchi – Linea Blu) con la sua **Letalità Totale** (Somma delle Vittime/nkill – Linea Rossa). L'obiettivo è verificare la correlazione tra volume di fuoco e impatto umano, rispondendo al quesito: *"L'aumento del numero di attacchi si traduce sempre in un aumento proporzionale delle vittime, o esistono periodi in cui il terrorismo diventa intrinsecamente più letale?"*.

Configurazione della Visualizzazione

È stato utilizzato un grafico **Dual Axis** (Doppio Asse) con scale indipendenti:

- **Asse Sinistro (Attacchi):** Scala adattata al volume degli eventi.
- **Asse Destro (Vittime):** Scala adattata al numero dei deceduti.

Questa scelta tecnica è cruciale: sganciando la sincronizzazione degli assi, è possibile sovrapporre visivamente i trend per confrontare la "forma" delle curve, identificando immediatamente i momenti in cui la mortalità cresce a un ritmo diverso rispetto alla frequenza degli attacchi.

Foto

Analisi del Trend (Confronto Attacchi vs Vittime)

Osservando il grafico, emergono due fasi distinte:

1. **Parallelismo (1970 – 2000):** Le due linee si muovono quasi all'unisono. Quando gli attacchi salgono, le vittime salgono in proporzione. Questo indica una letalità media costante e una "capacità distruttiva" standardizzata degli attacchi.
2. **Divergenza e Accelerazione (Post-2010):** È la fase più critica. Sebbene entrambe le curve crescano, la linea delle **Vittime** mostra un'accelerazione verticale più marcata rispetto alla linea degli **Attacchi**. Questo fenomeno suggerisce un cambiamento strutturale nel *modus operandi*: negli ultimi anni del dataset, il terrorismo è diventato più efficiente nel causare vittime (attacchi di massa, uso di esplosivi più potenti), rompendo la correlazione lineare del passato.

Validazione Statistica dei Modelli

Per confermare matematicamente l'osservazione visiva, sono state applicate **Linee di Tendenza Polinomiali di 3° grado (Cubiche)**. I parametri statistici estratti confermano la robustezza dell'analisi:

- **Significatività (P-Value):** Per entrambe le curve, il *P-Value* è $< 0,0001$. Essendo ben al di sotto della soglia di 0,05, possiamo affermare con certezza statistica che la crescita osservata non è casuale ma descrive un trend reale.
- **Confronto dei Coefficienti:**
 - La curva delle Vittime (*nkill*) ha un coefficiente cubico (x^3) di $3,92 \cdot 10^{-8}$.
 - La curva degli Attacchi ha un coefficiente cubico (x^3) di $1,76 \cdot 10^{-8}$.

Interpretazione: Il coefficiente delle vittime è più del doppio di quello degli attacchi. Matematicamente, questo conferma che la curva della mortalità è più "ripida" e cresce più velocemente.

foto dati

Conclusioni

L'analisi dimostra che il rapporto tra attacchi e vittime non è 1 : 1. L'impennata della linea rossa e i coefficienti del modello polinomiale rivelano un aggravamento della minaccia nell'ultimo decennio analizzato: il terrorismo moderno non colpisce solo più spesso, ma colpisce "più forte".

Nota Metodologica: Il "Missing Data" del 1993

I dati relativi al 1993 sono andati persi storicamente a causa di un problema durante il trasferimento degli archivi cartacei della *Pinkerton Global Intelligence Service*. In fase di *Data Cleaning*, si è scelto di mantenere il valore nullo piuttosto che interpolare artificialmente i dati, per preservare l'integrità scientifica. Tableau gestisce correttamente questa mancanza interrompendo la linea, segnalando visivamente l'assenza di informazioni per quell'anno specifico.

2.5.2 Dashboard 2: Analisi e Previsione della Letalità per Regione

Obiettivo dell'Analisi

Questa dashboard indaga la relazione tra l'intensità dell'attacco (misurata in numero di feriti, *nwound*) e la sua mortalità (numero di morti, *nkill*). L'obiettivo è duplice: verificare la correlazione tra le due variabili e prevedere l'evoluzione della letalità media, permettendo confronti geografici mirati.

Foto

1. **Analisi di Correlazione e Clustering (Scatter Plot):** La parte superiore ospita un grafico a dispersione dove ogni punto rappresenta un singolo evento.
 - **Clustering K-Means:** Tramite l'algoritmo *K-Means* di Tableau, gli attacchi sono stati raggruppati statisticamente per gravità.
 - **Legge di Potenza:** La densa "nuvola" colorata vicino all'origine rappresenta il *Cluster a Bassa-Alta Intensità*. I punti isolati (*Outliers*) rappresentano gli "Eventi Critici", rari ma devastanti.
2. **Trend Storico e Previsione (Forecast):** La parte inferiore utilizza il motore di *Exponential Smoothing* di Tableau. L'area ombreggiata attorno alla linea di previsione rappresenta l'intervallo di confidenza al 95%. Anche in questo grafico è visibile l'interruzione dei dati corrispondente all'anno 1993.
3. **Analisi Geografica (Filtro Dinamico):** L'implementazione di un filtro per regione permette di trasformare una media mondiale generica in uno strumento di *Risk Assessment* specifico per area.

Caso Studio Comparativo: South Asia vs North America

Per validare il modello, è stato eseguito un confronto diretto tra *South Asia* (area ad alta instabilità) e *North America* (area a stabilità relativa).

Foto caso studio

Analisi Qualitativa

- **South Asia:** La nuvola di punti nello *Scatter Plot* è estremamente densa, confermando che gli eventi ad alta intensità non sono eccezioni ma ricorrenze statistiche.
- **North America:** Il grafico appare quasi "vuoto". La quasi totalità degli eventi si concentra nell'origine; i casi ad alta intensità sono rari (es. 11 settembre).

Analisi Predittiva e Business Insights L'analisi del *Tasso di Letalità Previsto* (rapporto tra morti e feriti stimati) ha rivelato risultati inaspettati:

Regione	Tasso di Letalità	Caratteristica della Minaccia
South Asia	0,766	Alta frequenza, letalità "diluita" (molti feriti)
North America	0,990	Bassa frequenza, alta efficienza letale

Tabella 2.1: Confronto del tasso di letalità previsto tra South Asia e North America.

- **South Asia (0,766):** Ogni 100 feriti si registrano circa 76 decessi. La tipologia di attacchi (spesso esplosivi in aree aperte) genera un numero massiccio di feriti. La minaccia è definita dal **volume** degli eventi.
- **North America (0,990):** Il rapporto è quasi 1 : 1. Sebbene gli attacchi siano rari, mostrano una "efficienza letale" superiore, suggerendo l'uso di armi specifiche (sparatorie di massa) con esiti più frequentemente fatali.

Conclusioni Strategiche

Il confronto evidenzia due profili di rischio opposti: nel **Sud Asia**, le strutture di emergenza devono focalizzarsi sulla gestione dei grandi flussi di feriti; in **Nord America**, la prevenzione deve concentrarsi sull'anticipazione dell'evento raro, data l'altissima probabilità di decesso in caso di attacco.

Validazione Statistica del Modello Predittivo

Motore di Forecasting e Parametri di Base Per generare la proiezione futura della letalità, Tableau ha utilizzato un algoritmo di **Livellamento Esponenziale** (*Exponential Smoothing*). Il modello selezionato automaticamente è di tipo **Aggiuntivo** per il Livello, senza Trend e senza Stagionalità (Modello: *Aggiuntivo, Nessuno, Nessuno*).

L'algoritmo ha calcolato i seguenti valori per la previsione:

- **Rapporto di Letalità Iniziale previsto:** 0,864
- **Intervallo di confidenza (95%):** ±0,701

Analisi delle Metriche di Qualità Il software ha classificato la qualità della previsione come "*Scarsa*". Tale valutazione non indica un errore di modellazione, ma riflette l'estrema volatilità del fenomeno. Le metriche specifiche chiariscono il quadro:

- **RMSE (0,358) e MAE (0,245):** Misurano lo scostamento tra valori previsti e reali. Essendo contenuti, indicano che la linea di base è centrata correttamente sulla media storica.

- **MASE (0,91):** Essendo inferiore a 1, certifica che il modello ha prestazioni superiori rispetto a un modello *Naive*. Il sistema estrae dunque un pattern statistico valido.
- **MAPE (27,8%):** L'errore percentuale spiega il rating di Tableau; esiste un margine d'incertezza del 30% circa sulle previsioni.

Interpretazione Strategica del Modello Dal punto di vista dell'analisi di *intelligence*, una qualità statistica definita "scarsa" a causa dell'alta varianza è un'informazione preziosa. L'ampiezza dell'intervallo di confidenza ($\pm 0,701$) dimostra matematicamente che il terrorismo non segue un trend lineare.

Gli eventi estremi possono alterare le medie in qualsiasi momento. Il modello suggerisce che non si deve basare la pianificazione solo sulla media attesa (0,86), ma si devono preparare le risorse di emergenza per l'estremo superiore dell'intervallo di confidenza, ovvero per potenziali picchi di letalità improvvisi.

figura dati previsione

2.5.3 Dashboard 3: Previsione dei Bersagli (Target) per Regione

Obiettivo dell'Analisi (Vittimologia)

Mentre le dashboard precedenti si sono concentrate sui volumi globali e sull'impatto in termini di vite umane (letalità), questa visualizzazione sposta il focus sulla **Vittimologia**. L'obiettivo è analizzare chi viene colpito e con quale frequenza, incrociando le tipologie di bersaglio (`targtype1_txt`) con le aree geografiche (`region_txt`).

Al fine di valutare il "Rischio di essere colpiti", la metrica utilizzata non è più la somma dei decessi, ma il **Conteggio degli Eventi** (Frequenza). Questo permette di identificare quali settori sono strutturalmente più sotto tiro, indipendentemente dall'esito letale del singolo attacco. La dashboard si compone di due strumenti complementari: un'analisi dinamica temporale (a sinistra) e una mappatura statica del rischio (a destra).

foto

1. **Evoluzione Temporale e Previsione (Stacked Area Chart):** La parte sinistra della dashboard ospita un grafico ad aree impilate che mostra la composizione dei bersagli dal 1970 al 2017. I settori analizzati sono i cinque principali: *Business*, *Government (General)*, *Military*, *Police*, e *Private Citizens & Property*.

- **Analisi Storica Visiva:** Il grafico evidenzia come la distribuzione dei bersagli non sia costante. Si nota una crescita significativa a cavallo tra gli anni '80 e '90, seguita da una flessione. Tuttavia, il dato più allarmante è l'esplosione volumetrica post-2010 (anche in questo grafico è visibile il "buco" fisiologico del 1993).
- **Strategic Forecasting (Previsione a 5 anni):** Il valore aggiunto di questo grafico è la proiezione futura (2017–2021), rappresentata dall'area più chiara a destra. Questa estensione supporta i processi di *Strategic Planning* a medio termine dei governi. L'intervallo di confidenza associato si allarga progressivamente, indicando matematicamente l'aumento dell'incertezza man mano che ci si allontana dai dati storici.

2. **Matrice di Concentrazione degli Attacchi (Heatmap):** La parte destra della dashboard risponde alla necessità di localizzare geograficamente la minaccia tramite una *Highlight Table* (Tabella Termica). Incrociando le Regioni (sulle righe) con i Target (sulle colonne), l'intensità del colore mappa la densità storica degli attacchi, fungendo da vera e propria mappa di rischio statica.

- **Identificazione delle "Zone Rosse":** Analizzando i dati crudi riportati nella matrice, emergono chiaramente le combinazioni a massimo rischio globale. Le celle dal colore più intenso si trovano in *Middle East & North Africa*, dove gli attacchi ai *Private Citizens* raggiungono la cifra record di 15.257 eventi storici, seguiti dagli attacchi alla *Police* (6.893). Anche il *South Asia* mostra una densità critica, con 10.491 attacchi ai privati cittadini e 8.471 ai militari.
 - Al contrario, regioni come *Australasia & Oceania* mostrano celle chiarissime (poche decine di attacchi), confermando un profilo di rischio quasi nullo.
3. **Interattività e Risposta alle Business Questions:** Il collante dell'intera dashboard è il **Filtro Dinamico per Regione**, posizionato in alto a destra. Selezionando un'area specifica (es. *Western Europe*), sia l'*Area Chart* che la previsione si ricalcolano immediatamente. Questo permette agli analisti di rispondere a domande di business mirate, come ad esempio verificare se in Europa si stia assistendo a uno spostamento dei bersagli dalle istituzioni (*Government*) verso i mercati civili (*Business* o *Private Citizens*).

Validazione Statistica e Comportamento del Modello Predittivo

Motore di Forecasting e Orizzonte Temporale Per la proiezione a 5 anni (2017–2021) dei volumi di attacco sui diversi bersagli, il motore analitico ha utilizzato il Livellamento Esponenziale sui dati storici dal 1970 al 2016. Coerentemente con la granularità annuale del dataset, il software non ha forzato alcuna componente di stagionalità (Modello Stagione: *Nessuna*).

Il Cambiamento di Paradigma (Soft Target vs Hard Target) L'analisi dei coefficienti del modello rivela una netta spaccatura matematica tra gli obiettivi civili e quelli istituzionali, confermando l'ipotesi visiva di un cambio di strategia del terrorismo moderno:

1. **Istituzioni, Forze dell'Ordine e Business (Hard/Economic Targets):** Per categorie come *Police*, *Military*, *Government* e *Business*, il coefficiente Beta (β , che regola la pendenza del trend) è pari a 0,000. Di conseguenza, il modello prevede una stabilizzazione della minaccia: la stima di crescita per il quinquennio successivo è pari a 0 rispetto al valore iniziale.
2. **Civili e Proprietà Private (Soft Targets):** Per la categoria *Private Citizens & Property*, il coefficiente β è salito a 0,297, portando il modello a calcolare un incremento stimato impressionante di +2.084 attacchi nel quinquennio. Questo dato certifica matematicamente lo spostamento della violenza verso bersagli non difesi.

Foto dati confronto

Analisi delle Metriche di Qualità (Il significato del rating "Scarsa") Come già osservato nell'analisi della letalità (Dashboard 2), Tableau classifica la qualità complessiva di queste previsioni come *"Scarsa"*. Questa valutazione è il riflesso dell'alta volatilità geopolitica. Esaminando le metriche specifiche:

- **MAPE :** Si attesta su valori che vanno dal 27,7% per il settore *Business* fino a un picco del 50,1% per i *Private Citizens*. L'errore così alto sui civili è dovuto all'impennata anomala ed esponenziale degli attacchi nell'ultimo decennio, che rende i dati storici del passato meno affidabili per prevedere l'entità esatta della crescita futura.

- **MASE** : I valori oscillano tra 1,01 e 1,11. Essendo leggermente superiori a 1, indicano che, a causa delle brusche oscillazioni (cicli di pace seguiti da improvvise ondate di attentati), il modello di smussamento esponenziale fatica a performare significativamente meglio di una semplice "previsione Naive" (che replicherebbe linearmente l'ultimo dato noto).

Implicazioni Strategiche L'alta varianza (testimoniata dall'ampio intervallo di confidenza, es. ± 780 attacchi sui civili) e la netta distinzione dei trend modellati suggeriscono un'importante indicazione di *Intelligence*: mentre le misure di sicurezza fisiche a protezione di basi militari e palazzi governativi sembrano aver "congelato" la crescita degli attacchi contro di essi (trend piatto), i terroristi hanno compensato rivolgendosi verso gli spazi pubblici. La previsione indica ai decisori politici che la vera priorità strategica dei prossimi anni sarà la messa in sicurezza dei *Soft Target* urbani, dove l'incertezza e il volume atteso sono massimi.

Foto dati

2.5.4 Dashboard 4: Analisi degli Esiti dell'Attacco (Successo vs Fallimento)

Obiettivo dell'Analisi

Mentre le dashboard precedenti hanno esaminato la frequenza, la letalità e la natura dei bersagli, questa visualizzazione sposta il focus sull'efficacia delle misure di sicurezza e dell'intelligence antiterrorismo. L'analisi si basa sulla variabile binaria dell'esito dell'attacco: **Successo** (l'attacco è stato portato a termine come pianificato) o **Fallimento** (l'ordigno è stato disinnescato, il terrorista intercettato o l'azione è fallita per cause tecniche).

L'obiettivo strategico è comprendere se le capacità difensive globali stiano migliorando nel tempo e se la natura del bersaglio influisca sulla probabilità di riuscita dell'attentato. La dashboard è composta da due visualizzazioni temporali sincronizzate e governate da un filtro globale per tipologia di bersaglio.

Foto

1. **Analisi Temporale dell'Efficacia (Composizione e Trend)**: La porzione principale della dashboard risponde alla domanda su come variano i risultati storicamente.

- **100% Stacked Bar Chart**: Il grafico a barre in pila normalizzato al 100% mostra visivamente la proporzione annua tra attacchi riusciti (porzione Arancione) e attacchi falliti (porzione Viola). A livello globale, emerge un dato strutturale: il terrorismo ha un tasso di successo fisiologicamente altissimo. Questo è tipico delle tattiche asimmetriche, in cui l'attaccante ha il vantaggio della sorpresa.
- **Trend Line dell'Efficacia (Tasso di Fallimento)**: Sotto l'istogramma, un grafico a linee isola e traccia unicamente la percentuale dei fallimenti nel corso dei decenni.
 - *Analisi Storica*: Si nota un picco anomalo di fallimenti nei primi anni '70 (intorno al 1972, prossimo al 20%).
 - *Il Trend Recent*: Il dato di business più rilevante si osserva nella parte finale della curva (dal 2010 al 2017). La linea del tasso di fallimento mostra una crescita rapida e costante, passando da valori sotto il 10% a picchi che superano il 15%-20%. Questo trend in salita è un indicatore positivo: certifica che l'implementazione di moderne tecnologie di prevenzione, la sorveglianza digitale e il miglioramento delle operazioni di *intelligence* stanno portando a sventare un numero sempre maggiore di attentati.

2. **Correlazione tra Bersaglio ed Esito (Analisi "Hard vs Soft Target"):** Per rispondere al quesito se sia più difficile colpire una base militare rispetto a una piazza pubblica, la dashboard è stata dotata di un **Filtro Dinamico per Target** (`targtype1.txt`). Questo strumento interattivo permette di condurre un'analisi differenziale immediata:

- **Hard Targets (es. Military / Police):** Selezionando bersagli istituzionali, dotati di protocolli di sicurezza attivi, perimetri fortificati e personale armato, la linea del "Tasso di Fallimento" tende a posizionarsi su valori percentuali mediamente più alti. Le difese passive e attive fungono da deterrente o riescono a neutralizzare la minaccia durante la fase di esecuzione.
- **Soft Targets (es. Private Citizens & Property):** Cambiando il filtro su obiettivi civili (luoghi pubblici, piazze, mercati), si osserva un restringimento della barra viola e un crollo della linea dei fallimenti. Privi di difese strutturali, questi bersagli garantiscono ai terroristi una probabilità di successo dell'azione quasi assoluta.

Conclusioni Strategiche

Questa dashboard chiude il cerchio dell'analisi, trasformando una variabile binaria in un misuratore di *performance* (KPI) per la sicurezza globale. La visualizzazione dimostra che, sebbene spostare l'attenzione sui *Soft Target* garantisca ai terroristi tassi di successo altissimi, gli sforzi di prevenzione sistematica degli ultimi anni stanno invertendo la rotta, registrando i tassi di fallimento dell'attacco più alti degli ultimi 40 anni.

Caso Studio Comparativo: *Military vs Airports & Aircraft*

Per rispondere al quesito specifico se sia più difficile colpire una base militare rispetto a un aeroporto, sono stati isolati i dati di queste due categorie tramite il filtro dinamico, analizzando le rispettive linee di tendenza dei fallimenti. Il confronto ha rivelato un dato statistico di grande rilevanza strategica.

- **Analisi del Target Military (Basi e Forze Armate):** Filtrando per obiettivi militari, il grafico a barre mostra che il tasso di successo degli attacchi rimane storicamente molto alto. Osservando la *Trend Line* del tasso di fallimento, notiamo che per decenni (dal 1970 al 2014) la percentuale di attacchi sventati ha oscillato in una fascia relativamente bassa, tra il 5% e il 10%. Solo nel biennio finale (2016–2017) si registra un'impennata che supera il 20%.

Interpretazione: Sebbene le basi militari siano *Hard Targets* (obiettivi fortificati), le truppe operano spesso in zone di conflitto attivo o in scenari asimmetrici, dove sono costantemente esposte ad agguati, ordigni improvvisati, rendendo la prevenzione assoluta molto complessa.

- **Analisi del Target Airports & Aircraft (Aviazione Civile e Infrastrutture):** Cambiando il filtro sul settore dell'aviazione, lo scenario cambia drasticamente. La prima evidenza tecnica è il cambio di scala dell'asse Y del grafico del Trend di Efficacia: mentre per i militari il tetto massimo era intorno al 20%, qui l'asse arriva all'80%. Storicamente, l'aviazione mostra tassi di fallimento molto più alti (spesso tra il 15% e il 30% già negli anni passati), con un picco anomalo e verticale nell'ultimo anno registrato (2017), dove la percentuale di attacchi falliti o sventati schizza quasi all'80%. Il grafico a barre soprastante conferma visivamente questo dato, mostrando ampie porzioni (fallimenti) che dominano in diverse annate.

Questa marcata discrepanza deriva dalla natura delle difese:

1. **Standardizzazione Globale:** Il settore aeroportuale è regolato da protocolli di sicurezza internazionali standardizzati (*metal detector, scanner a raggi X, controlli incrociati sui passeggeri, intelligence preventiva*) che bloccano la minaccia prima che entri nella fase esecutiva.
2. **Vulnerabilità Tattica:** Un aeroporto è un ambiente chiuso e controllato, dove l'attaccante deve superare filtri successivi. Un convoglio militare, al contrario, si trova spesso in campo aperto, dove l'attaccante può sfruttare il fattore sorpresa o la forza bruta.

Foto esempio

CAPITOLO 3

Power PI

Preambolo da scrivere

3.1 Seguire pdf esempio

Sitografia

- A.N.I.P.A, il portale della perforazione – www.anipapozzi.it