

**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

---

## Indice

---

<b>Introduzione</b>	<b>1</b>
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
<b>1    Qlik</b>	<b>6</b>
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
1.5    Analisi dell'impatto economico e danni causati . . . . .	18
1.6    Utente . . . . .	19
1.7    Obiettivo . . . . .	19
1.8    Filtri interattivi ed esempi di utilizzo . . . . .	20
<b>2    Tableau</b>	<b>24</b>
2.1    Seguire pdf esempio . . . . .	24
<b>3    Power PI</b>	<b>25</b>
3.1    Seguire pdf esempio . . . . .	25
<b>Sitografia</b>	<b>26</b>

---

## 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 &amp; 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
1.16	Analisi dell'impatto economico e danni causati . . . . .	19
1.17	Analisi dell'impatto economico e danni causati per filtro Macro-regione . . .	21
1.18	Analisi dell'impatto economico e danni causati per filtro Micro-regione (Italy)	21
1.19	Analisi dell'impatto economico e danni causati per filtro Tipo di Attacco (Armed Assault) . . . . .	23
1.20	Analisi dell'impatto economico e danni causati per filtro Gruppo Terroristico	23

---

## Elenco delle tabelle

---

1	Elenco completo delle 27 variabili selezionate dal GTD.	2
---	---	---

---

## 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", "latlng", "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"
]

df = pd.read_csv(file_path, usecols=columns_of_interest, encoding='ISO-8859-1')
```

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

```
numeric_cols_unknown = ["nkill", "nwound", "propvalue", "ransomamt", "nperps"]

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.

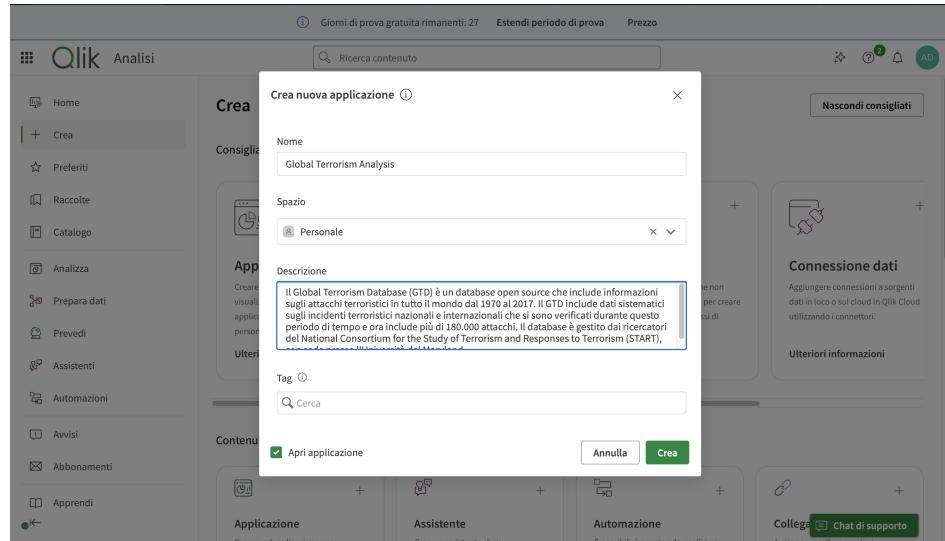


Figura 1.1: Creazione dell'applicazione

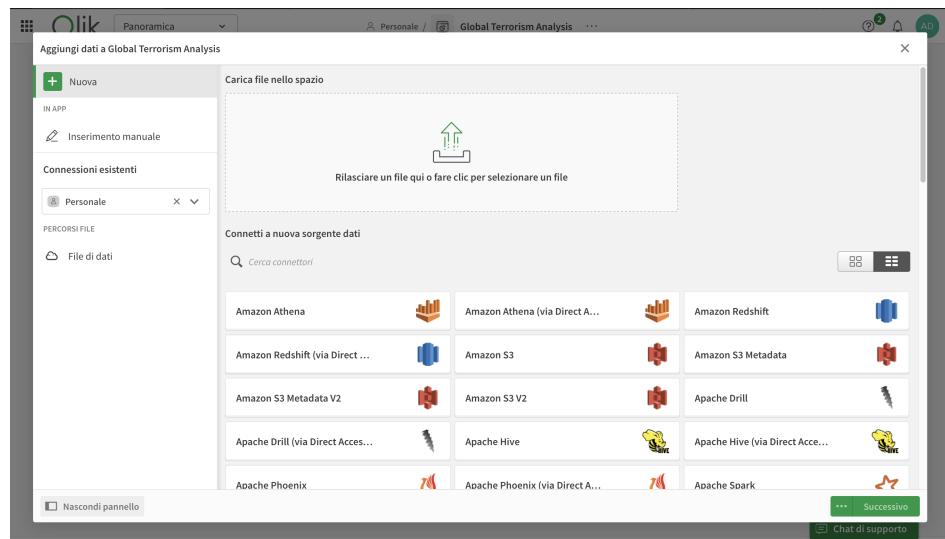


Figura 1.2: Upload del Dataset

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 "Hotspot<sup>1</sup>" 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:

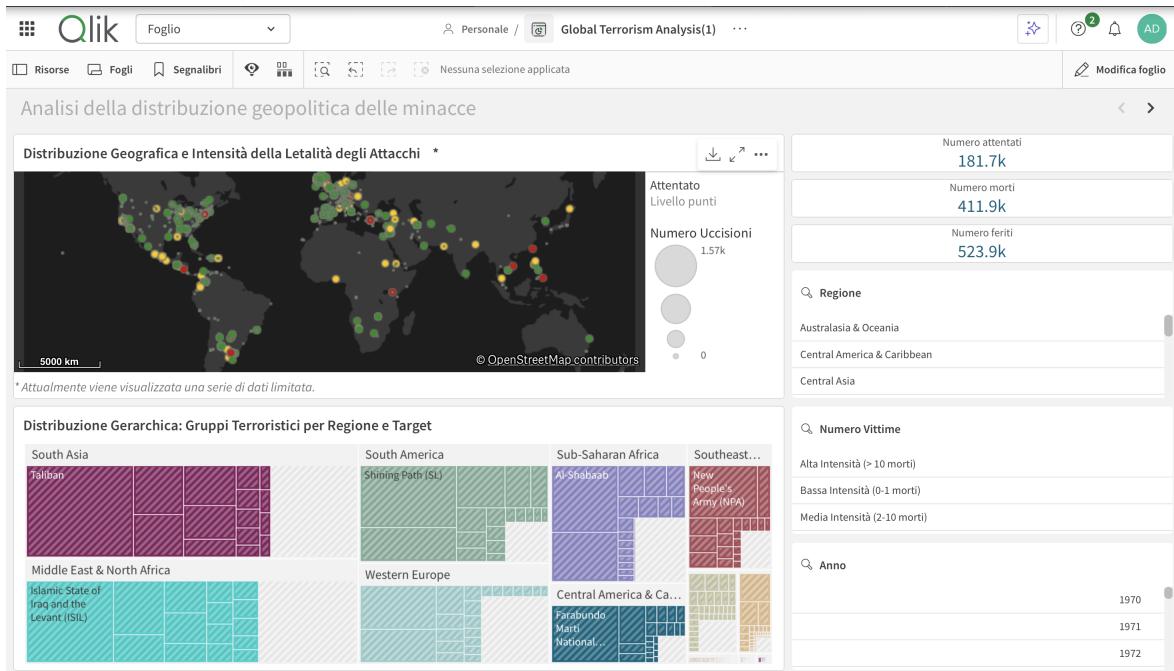
- il colore *Verde* identifica gli eventi a bassa letalità (0-1 vittime);
- il colore *Giallo* identifica gli eventi con impatto medio (2-10 vittime);
- il colore *Rosso* identifica le stragi o gli eventi critici (oltre 10 vittime);

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.

<sup>1</sup>Nel 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

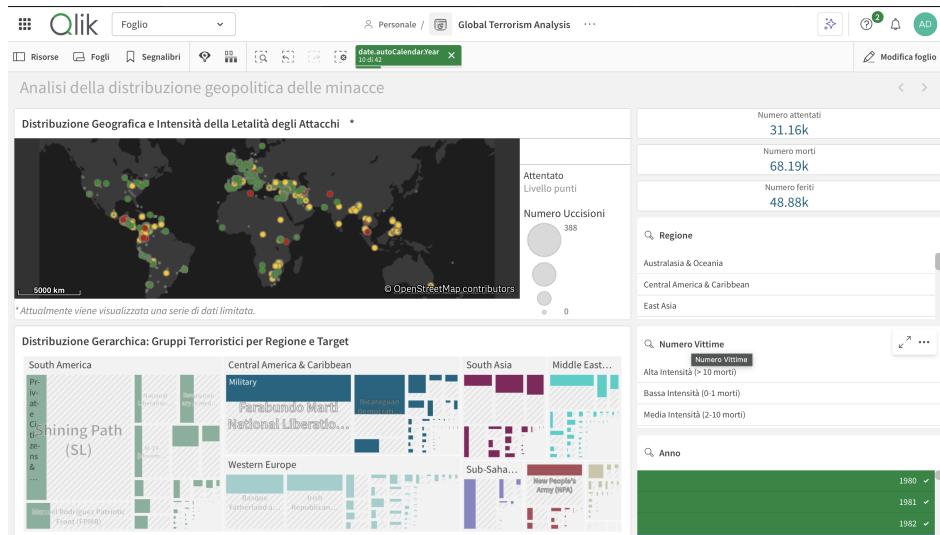
L’efficacia della dashboard risiede nella sua natura dinamica: l’integrazione dei filtri permette all’analista di esplorare i dati in modo interattivo per isolare specifici fenomeni o periodi storici. Di seguito vengono riportati due esempi pratici di utilizzo che dimostrano la capacità dello strumento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

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

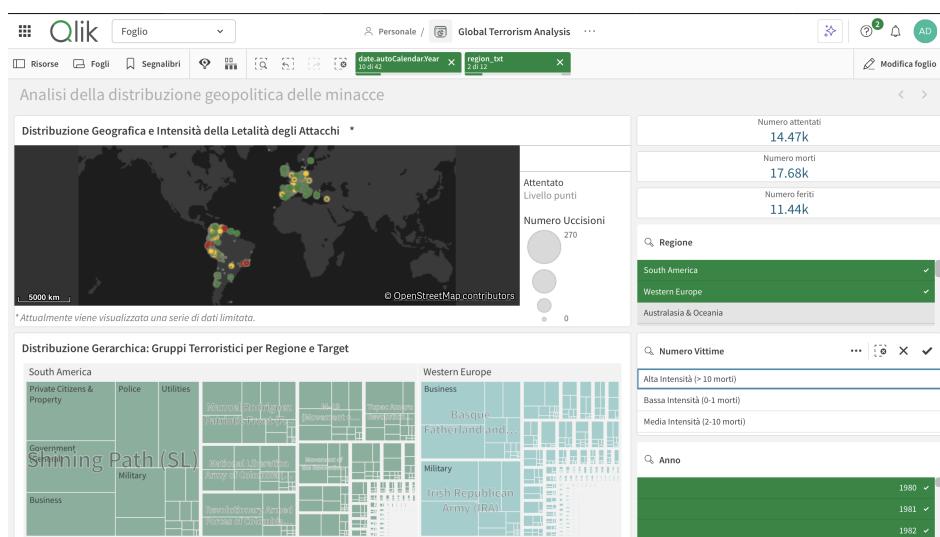
Questo scenario risponde alle domande: "Quali nazioni sono i principali Hotspot?" e "Chi sono i gruppi più attivi?".

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



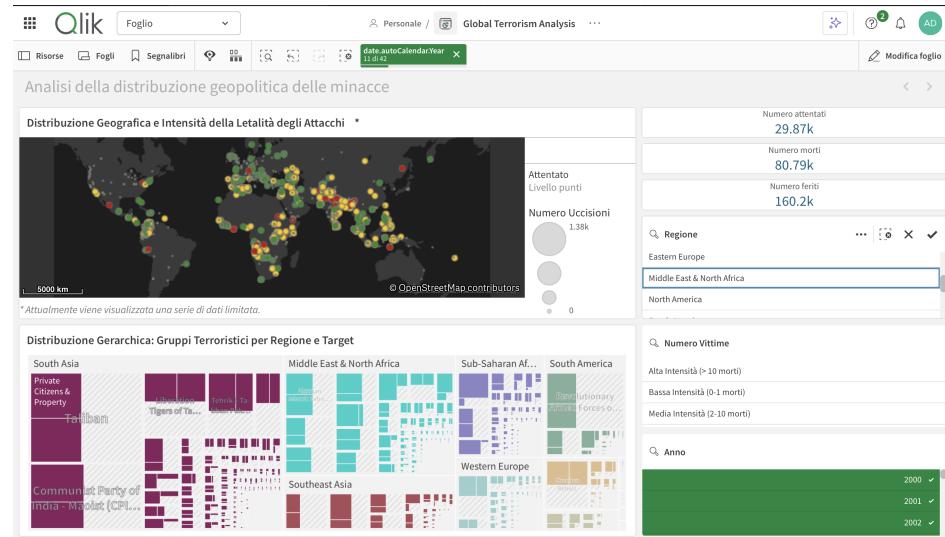
**Figura 1.4:** Analisi della distribuzione geopolitica delle minacce filtrando per Anno



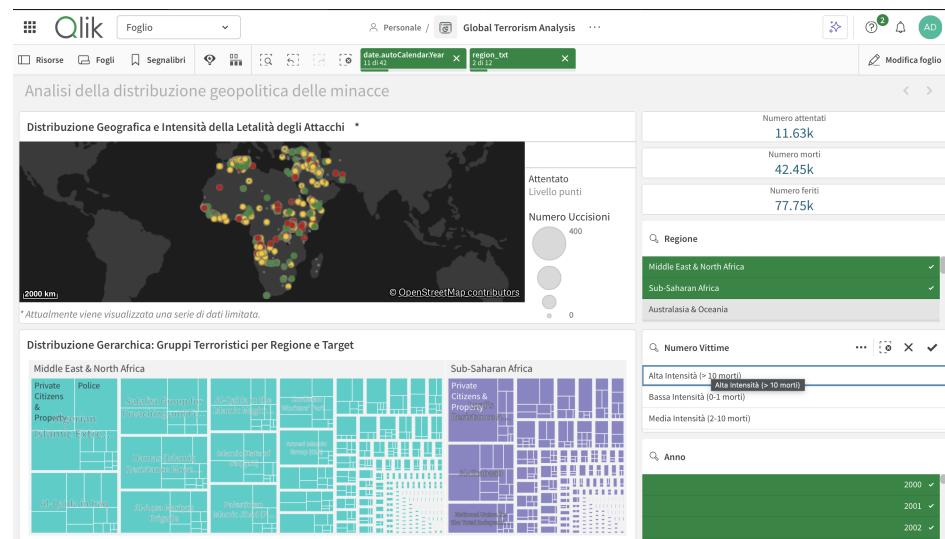
**Figura 1.5:** Analisi della distribuzione geopolitica delle minacce filtrando per Anno e Regione

- *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*.

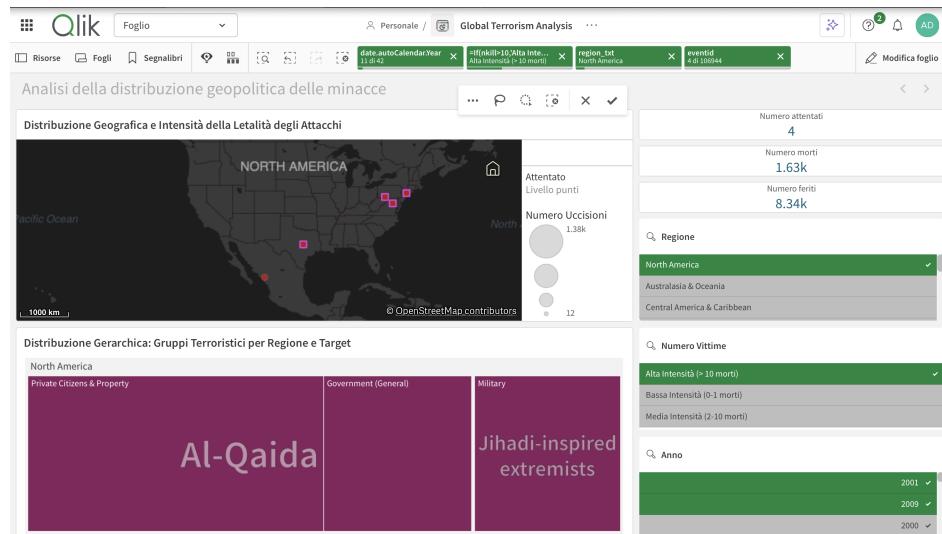
Questo strumento permette di segmentare il dataset in base al numero di vittime (*nkill*), applicando la stessa logica "a semaforo" visibile sulla mappa:

- *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

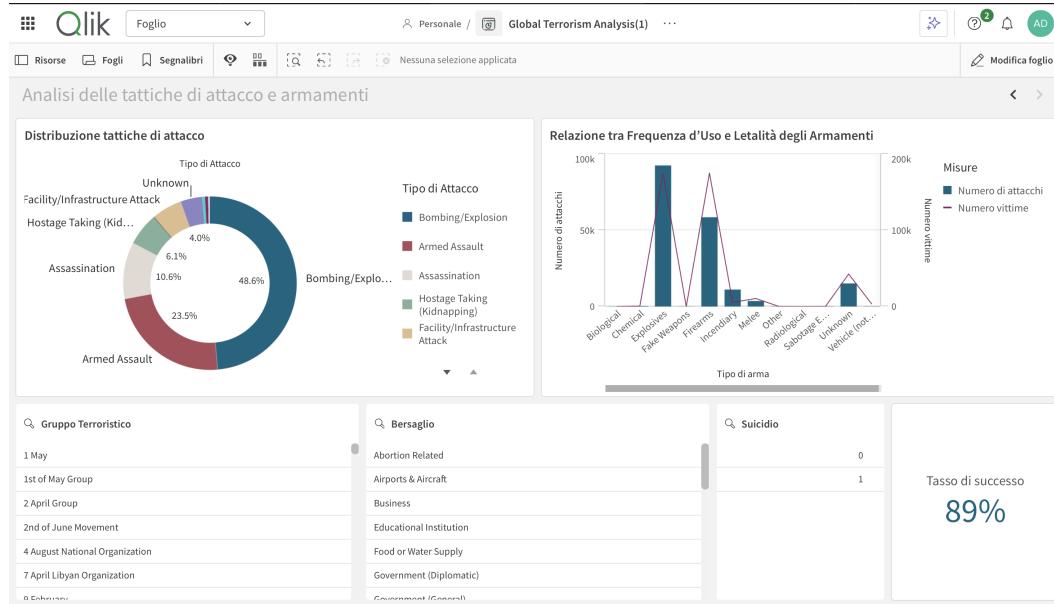
La Dashboard, mostrata in Figura 1.9, analizza le strategie operative e la sofisticazione militare dei gruppi terroristici, focalizzandosi sulla relazione tra il "Modus Operandi" adottato (tipologia di attacco), gli armamenti utilizzati e la letalità risultante. Nel dettaglio, il sistema monitora i principali 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.

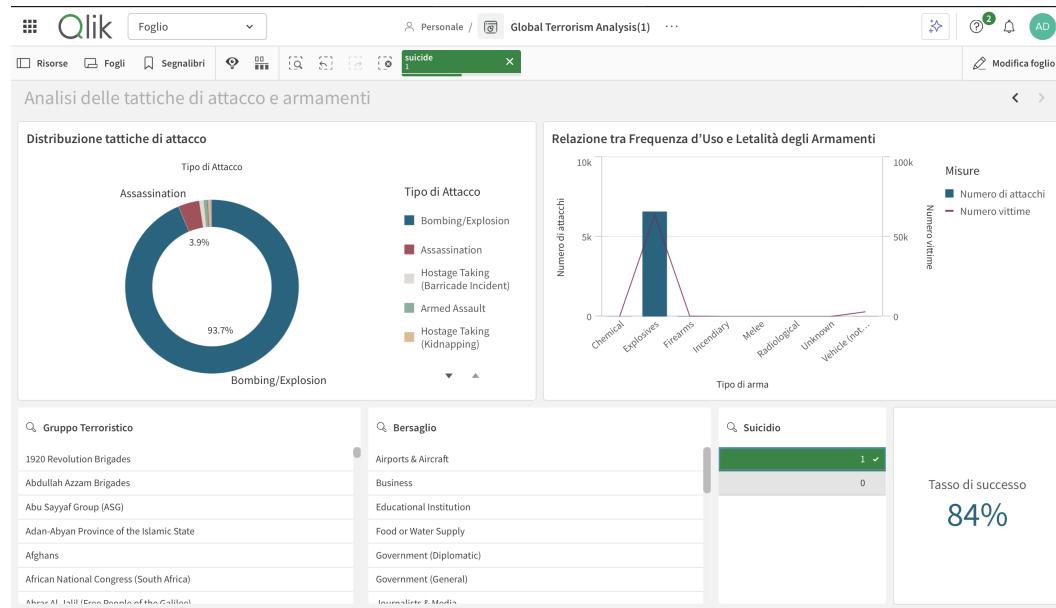
#### 1.4.3 Filtri ed esempi di utilizzo

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.

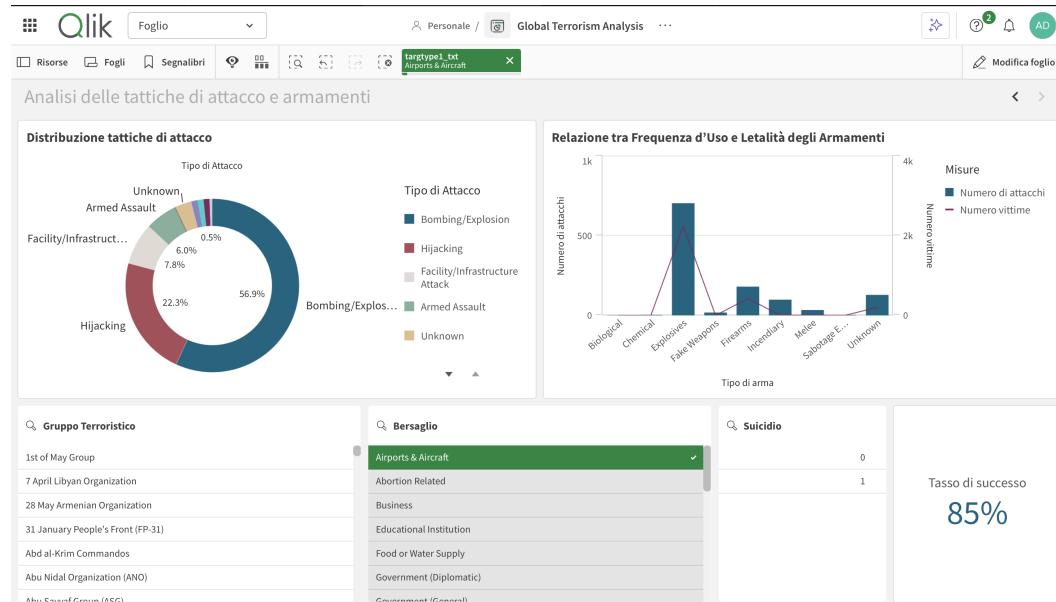
- **2. Qual è il tasso di letalità per ogni tipo di arma?** Applicando il filtro *Bersaglio = Airports & Aircraft*, il Grafico Combinato permette di isolare la minaccia specifica per il settore aviazione. L’analisi visiva evidenzia che gli *Explosives* (Esplosivi) costituiscono l’arma nettamente più 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.

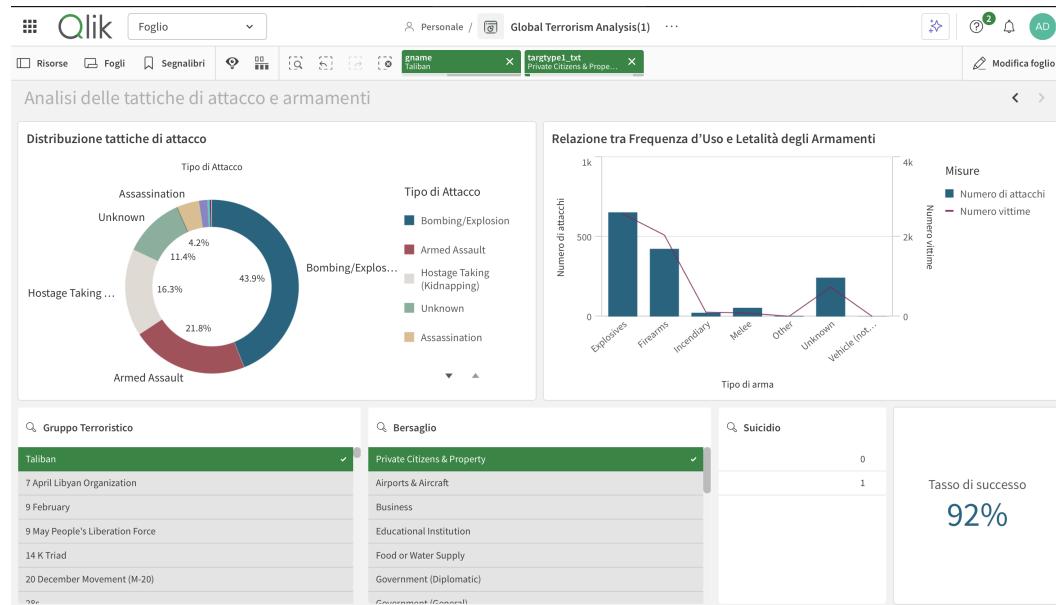


**Figura 1.11:** Analisi delle tattiche di attacco e armamenti: filtro Bersaglio

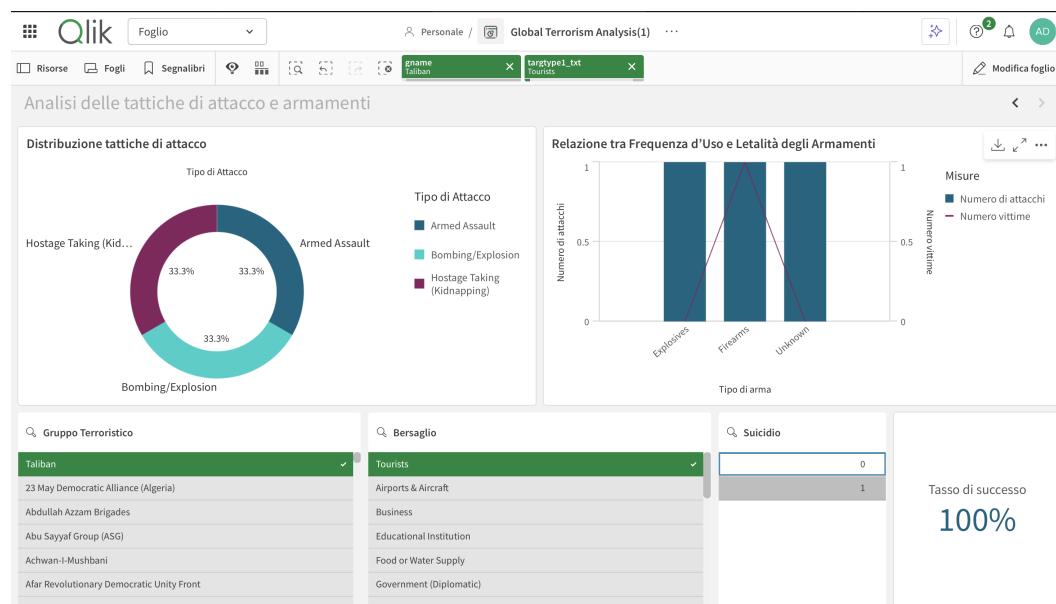
- **3. Adattamento Tattico al Bersaglio** Confrontando le modalità di attacco del gruppo Taliban su due categorie di vittime distinte, *Tourists* (Turisti) e *Private Citizens & Property* (Cittadini Privati), emerge una significativa variazione del *modus operandi*. Mentre contro i cittadini privati 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

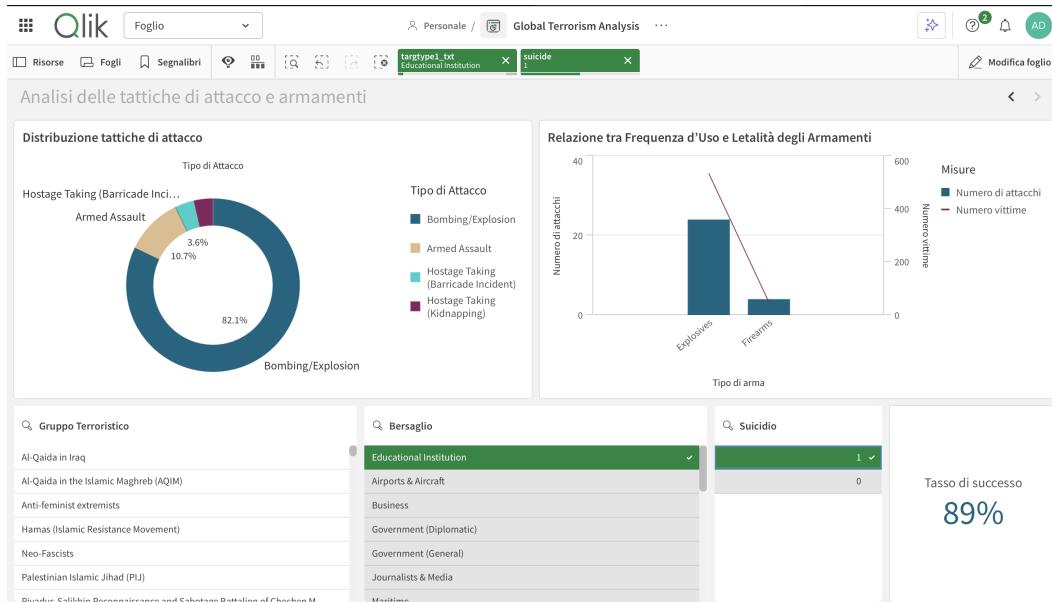


**Figura 1.13:** Analisi delle tattiche di attacco e armamenti: filtro Bersaglio Turisti

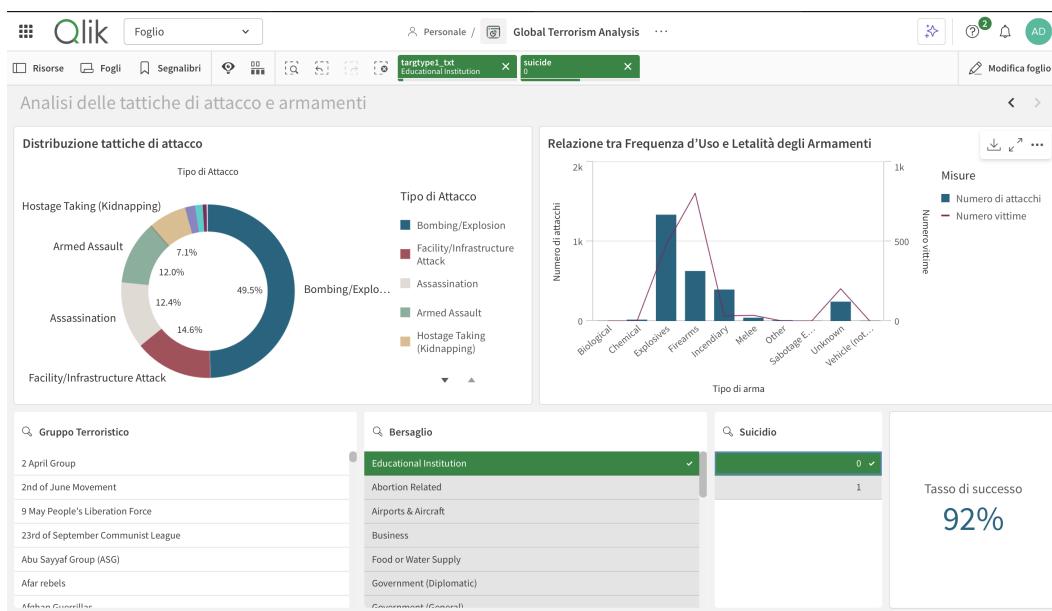
La dashboard, inoltre, permette verifiche puntuali su obiettivi specifici, come, ad esempio, gli *Educational Institutions* (Istituti Educativi). Confrontando le modalità di attacco tramite il KPI del *Success Rate*, emerge un risultato in controtendenza rispetto al dato globale: in questo contesto,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

## 1.5 Analisi dell'impatto economico e danni causati

La dashboard, mostrata in Figura 1.16, analizza le conseguenze economiche e i danni collaterali causati dagli attacchi terroristici. Essa permette di visualizzare il valore totale dei danni economici (in USD), suddivisi per regione geografica e tipo di attacco. Questo approccio consente di identificare le aree più colpite e i tipi di attacchi con maggiore impatto economico, fornendo informazioni utili per la pianificazione delle strategie di prevenzione e protezione.

I principali indicatori sintetici (KPI) includono:

- il *Totale dei danni stimati* (in dollari), come misura aggregata dell'impatto economico complessivo;
- il *Danno medio per attacco*, utile a distinguere tra fenomeni ad alta frequenza ma basso impatto e attacchi rari ma altamente distruttivi;
- il *Massimo danno registrato*, indicatore di eventi estremi ad elevata intensità economica.

Accanto agli indicatori sintetici, la dashboard si articola in tre principali visualizzazioni analitiche, ciascuna finalizzata ad approfondire una specifica dimensione dell'impatto economico del terrorismo.

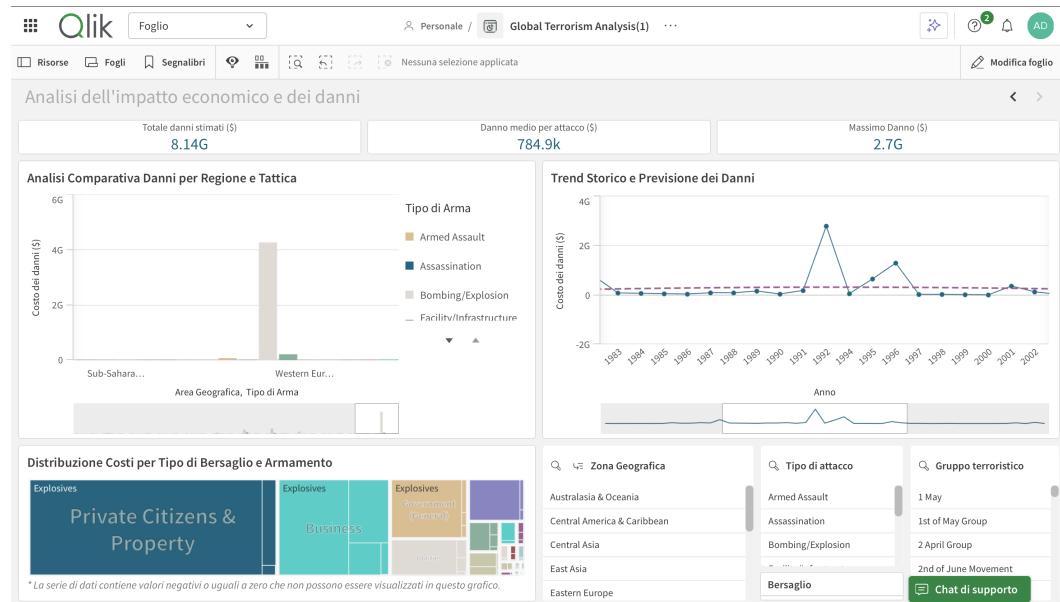
Il primo grafico, denominato *Analisi comparativa dei danni per regione e tattica*, rappresenta il totale dei danni economici in funzione delle macro-aree geografiche e della tipologia di attacco. Le regioni considerate (ad esempio Middle East & North Africa, South Asia, Sub-Saharan Africa, Western Europe, North America) costituiscono la dimensione territoriale dell'analisi, mentre le diverse tattiche operative (quali Bombing/Explosion, Armed Assault, Facility/Infrastructure Attack) introducono una seconda chiave di lettura. La combinazione tra area geografica e modalità d'attacco consente di individuare non solo dove si concentra il maggior impatto economico, ma anche quali strategie operative risultano più distruttive nei diversi contesti regionali. Tale confronto permette di evidenziare eventuali differenze strutturali tra aree del mondo, distinguendo tra regioni caratterizzate da elevata intensità finanziaria e regioni in cui i danni risultano più contenuti.

Il secondo grafico, *Trend storico e previsione dei danni*, analizza l'evoluzione temporale del valore economico distrutto. La rappresentazione mostra l'andamento annuale dei danni stimati, permettendo di osservare fasi di crescita, stabilizzazione o contrazione dell'impatto economico nel lungo periodo. L'inclusione di una linea di tendenza consente di evidenziare la direzione generale del fenomeno, distinguendo tra fluttuazioni episodiche legate a eventi straordinari e dinamiche strutturali più persistenti. Questa visualizzazione assume particolare rilevanza per valutazioni prospettiche e per l'analisi del rischio economico su orizzonti temporali medio-lunghi.

Il terzo grafico, una *Treemap della distribuzione dei costi per tipo di bersaglio e armamento*, approfondisce la dimensione operativa del danno economico. La rappresentazione gerarchica consente di analizzare il valore economico distrutto in funzione della categoria di bersaglio (ad esempio Business, Government, Utilities, Transportation) e del tipo di armamento utilizzato. La dimensione dei riquadri è proporzionale al totale dei danni associati a ciascuna combinazione, permettendo di individuare rapidamente le configurazioni a maggiore impatto patrimoniale. Questa visualizzazione evidenzia se determinate combinazioni – ad esempio specifici armamenti contro infrastrutture strategiche – risultino particolarmente onerose in termini economici.

La lettura congiunta delle tre visualizzazioni integra dunque una dimensione geografica, una dimensione temporale e una dimensione operativo-strutturale. La dashboard non si limita alla quantificazione aggregata delle perdite, ma consente di comprenderne la distribuzione

territoriale, l’evoluzione nel tempo e la relazione con le modalità di attacco e le categorie di bersaglio, offrendo un quadro analitico completo dell’impatto economico del fenomeno terroristico.



**Figura 1.16:** Analisi dell’impatto economico e danni causati

## 1.6 Utente

L’utente a cui è destinata questa dashboard è un Risk Manager operante nel settore assicurativo, finanziario o in ambito, con responsabilità nella valutazione e gestione del rischio geopolitico ed economico. Tale figura professionale utilizza lo strumento per analizzare l’impatto patrimoniale degli attacchi terroristici, valutando la distribuzione territoriale dei danni, la relazione tra tipologia di attacco e perdita economica e l’evoluzione temporale del fenomeno.

L’analisi fornita dalla dashboard supporta i responsabili della gestione del rischio nella quantificazione dell’esposizione finanziaria associata a specifiche aree geografiche, settori economici e modalità operative. In particolare, la combinazione tra confronto regionale, studio delle tattiche e andamento storico dei danni consente di distinguere tra contesti a elevata frequenza di eventi ma impatto contenuto e scenari caratterizzati da eventi meno frequenti ma economicamente devastanti.

Lo strumento risulta quindi funzionale alla definizione di politiche assicurative, alla determinazione dei premi in funzione del rischio territoriale e settoriale e alla pianificazione strategica di investimenti o aperture di nuove sedi in aree potenzialmente esposte. In questo modo, la dashboard contribuisce a trasformare il dato storico in informazione strategica, supportando decisioni orientate alla mitigazione del rischio economico e alla protezione del patrimonio aziendale.

## 1.7 Obiettivo

L’obiettivo principale dell’analisi è comprendere e quantificare l’impatto economico del terrorismo, valutandone la distribuzione territoriale, l’evoluzione temporale e la relazione con le modalità operative adottate. La dashboard consente di:

- identificare le aree geografiche e le tipologie di attacco che generano il maggiore danno patrimoniale, distinguendo tra contesti ad alta frequenza di eventi e scenari caratterizzati da perdite economiche particolarmente elevate;
- valutare la distribuzione dei costi in funzione del tipo di bersaglio e dell’armamento utilizzato, mettendo in relazione le configurazioni operative con il relativo impatto finanziario;
- analizzare l’andamento storico dei danni economici, individuando trend strutturali e possibili dinamiche evolutive utili alla previsione del rischio;
- supportare le decisioni strategiche in ambito assicurativo e aziendale attraverso evidenze empiriche sull’esposizione economica, favorendo la definizione di politiche di mitigazione del rischio e di allocazione efficiente delle risorse.

In sintesi, l’analisi mira a trasformare la complessità del fenomeno terroristico in informazioni chiare e utilizzabili, consentendo di comprendere non solo la dimensione quantitativa del danno, ma anche le sue caratteristiche qualitative e dinamiche, al fine di orientare efficacemente le strategie di gestione del rischio economico.

## 1.8 Filtri interattivi ed esempi di utilizzo

L’efficacia della dashboard risiede nella sua natura dinamica: l’integrazione dei filtri consente al Risk Manager di esplorare i dati in modo interattivo, isolando specifici scenari economici e verificando ipotesi strategiche in tempo reale. Attraverso la selezione mirata delle variabili, è possibile rispondere a quesiti operativi concreti.

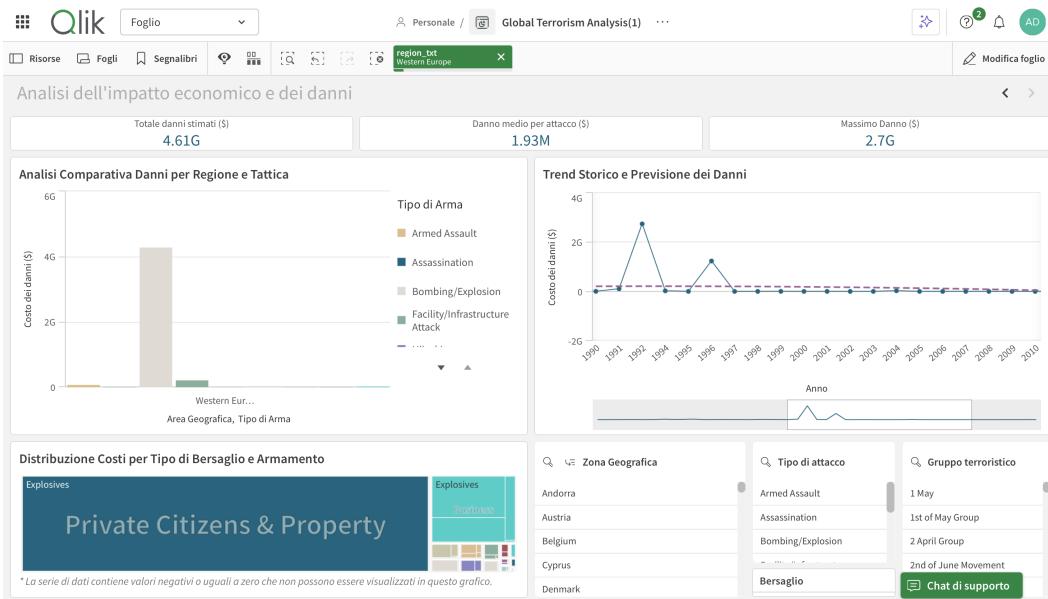
### • 1. Quali regioni e quali tattiche generano il maggiore impatto economico?

Osservando il grafico “Analisi comparativa dei danni per regione e tattica” nella sua configurazione globale, è possibile identificare immediatamente le macro-aree con la maggiore concentrazione di perdite patrimoniali. Successivamente, applicando il filtro *Regione*, l’analisi scende nel dettaglio per verificare se determinate modalità operative (ad esempio *Bombing/Explosion*) risultino sistematicamente associate ai danni più elevati in quell’area specifica.

Un esempio è mostrato nella Figura 1.17, dove, dopo aver individuato l’Europa Occidentale come area critica, è stato applicato il filtro *Western Europe*. La dashboard isola così un impatto economico complessivo di *4.61 Miliardi di dollari* e l’analisi incrociata dei grafici permette di ricostruire lo scenario:

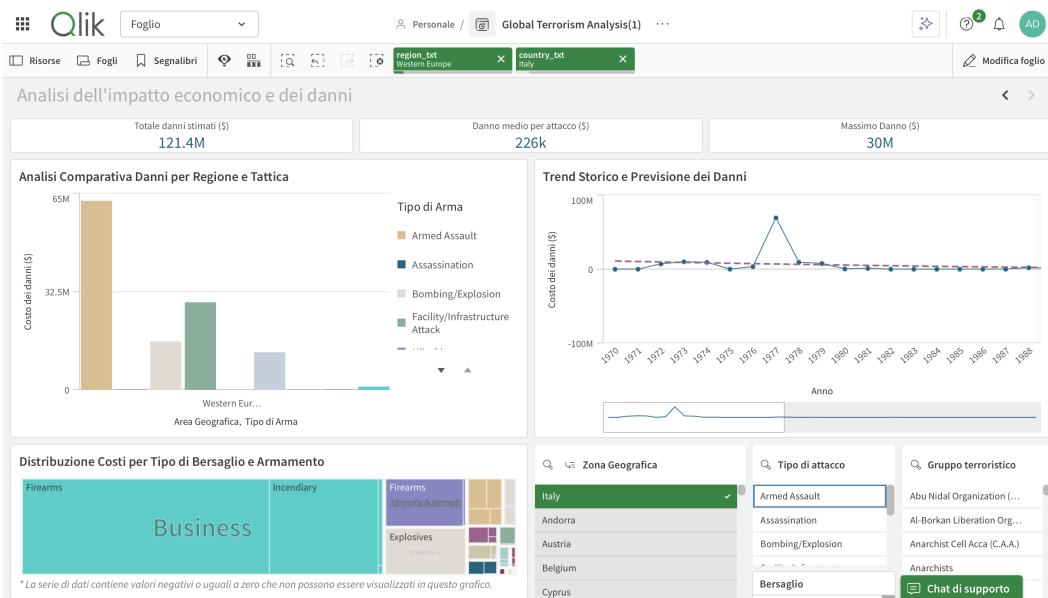
1. *Dominio delle tattiche esplosive*: Il grafico a barre evidenzia una prevalenza quasi assoluta della tattica *Bombing/Explosion* (barra beige), responsabile della quasi totalità dei danni. Il KPI del costo medio sale a **1.93 Milioni di dollari** per evento, un valore altissimo che riflette il costo delle infrastrutture europee colpite.
2. *Analisi del Trend Temporale*: Il grafico di dettaglio “Trend Storico” rivela che il danno economico non è costante, ma concentrato in specifici eventi catastrofici. Si osserva un picco estremo nel 1992 (con danni superiori a 2.5 Miliardi, visibile nel vertice massimo della linea blu) e un picco secondario nel 1996. Tuttavia, la linea di regressione (tratteggiata in viola) mostra una chiara pendenza negativa: dopo la fase critica degli anni ’90, la curva dei danni tende ad appiattirsi verso lo zero negli anni 2000, indicando una progressiva riduzione dell’impatto finanziario degli attacchi nella regione.

- 3. Settori critici:** La Treemap identifica infine i bersagli: il blocco *Private Citizens & Property* rappresenta la quota maggiore di capitale distrutto, seguito dal settore *Business*, confermando che i picchi di spesa sono stati causati da attentati contro proprietà civili e commerciali.



**Figura 1.17:** Analisi dell'impatto economico e danni causati per filtro Macro-regione

Tramite il filtro *Zona Geografica*, è possibile inoltre isolare ulteriormente l'analisi per singolo paese, passando da una macro-regione a un contesto nazionale specifico. Un esempio di studio di micro-regione è mostrato nella Figura 1.18.



**Figura 1.18:** Analisi dell'impatto economico e danni causati per filtro Micro-regione (Italy)

- 2. L'impatto economico è in crescita nel lungo periodo?**

Attraverso il grafico “Trend storico e previsione dei danni”, l'utente può analizzare l'andamento annuale del valore economico distrutto. L'integrazione di una linea di

**regressione** consente di distinguere tra picchi legati a singoli eventi straordinari e variazioni strutturali di lungo periodo, fornendo un supporto concreto alle valutazioni prospettiche sul rischio economico.

Ad esempio, osservando la dashboard in Figura 1.18, si nota che in Italia, pur essendoci stati eventi di grande impatto economico (come la strage di Bologna), l'andamento complessivo dei danni mostra una diminuzione nel tempo. La linea di regressione, con pendenza negativa, conferma questa tendenza.

Questo indica che, nel tempo sia la frequenza sia l'intensità degli eventi più distruttivi si sono ridotte, probabilmente grazie a misure di sicurezza più efficaci e a una maggiore capacità di risposta e protezione delle infrastrutture.

- **3. Qual è l'impatto economico di un certo tipo di attacco e come si distribuisce?**

Utilizzando il filtro *Attack Type* e selezionando, ad esempio, la voce **Armed Assault**, la dashboard isola i costi generati specificamente dalle incursioni armate. Questa vista permette di rispondere a tre interrogativi strategici sulla natura di questa minaccia:

1. **Geografia del danno (Macroaree):** Osservando il grafico a barre "Analisi Comparativa", emerge un dato significativo: la macroarea che ha subito i maggiori danni economici da assalti armati è l'**Western Europe**, seguita dal **South America**. Questo evidenzia come, storicamente, l'uso di armi leggere per colpire il patrimonio non sia stato esclusiva di zone di guerra, ma abbia avuto un impatto finanziario devastante anche nelle economie occidentali avanzate.
2. **Distribuzione su Obiettivi e Armamenti:** La Treemap rivela chiaramente quali settori pagano il prezzo più alto. Nel caso degli *Armed Assault*, il blocco dominante è il settore **Business** (aziende e attività commerciali), seguito da *Private Citizens & Property*. La scomposizione interna mostra che questi danni sono causati quasi esclusivamente tramite *Firearms* (armi da fuoco), confermando che l'assalto armato è una tattica mirata verso asset economici specifici piuttosto che distruzioni indiscriminate.
3. **Picco storico di criticità:** Infine, il grafico del trend temporale permette di datare l'apice della minaccia. La curva dei costi per gli assalti armati raggiunge il suo massimo storico assoluto nell'anno **1977**. Tale picco, visibile come un vertice isolato nel grafico, corrisponde storicamente a periodi di forte instabilità politica interna in Europa (ad esempio gli "Anni di Piombo"), dove l'assalto armato era una modalità operativa frequente per i gruppi eversivi.

La Figura 1.19 mostra la dashboard configurata con il filtro Armed Assault attivo.

- **4. Profilazione economica di un gruppo terroristico**

La dashboard consente un'analisi granulare focalizzata su singoli attori. Selezionando un determinato *Gruppo Terroristico* dal pannello filtri, l'intera interfaccia si riconfigura per mostrare il "profilo economico" dell'organizzazione.

- I **KPI** ricalcolano immediatamente il *Danno Medio* e *Massimo*, permettendo di capire se il gruppo opera con attacchi frequenti a basso costo o con rari eventi catastrofici.
- La **Treemap** svela la distribuzione dei danni del gruppo sui vari bersagli.
- Il **Trend Storico** traccia l'evoluzione della capacità distruttiva del gruppo nel tempo, evidenziando periodi di escalation o declino operativo.

Un esempio con il filtro *Gruppo terroristico* è mostrato in Figura 1.20

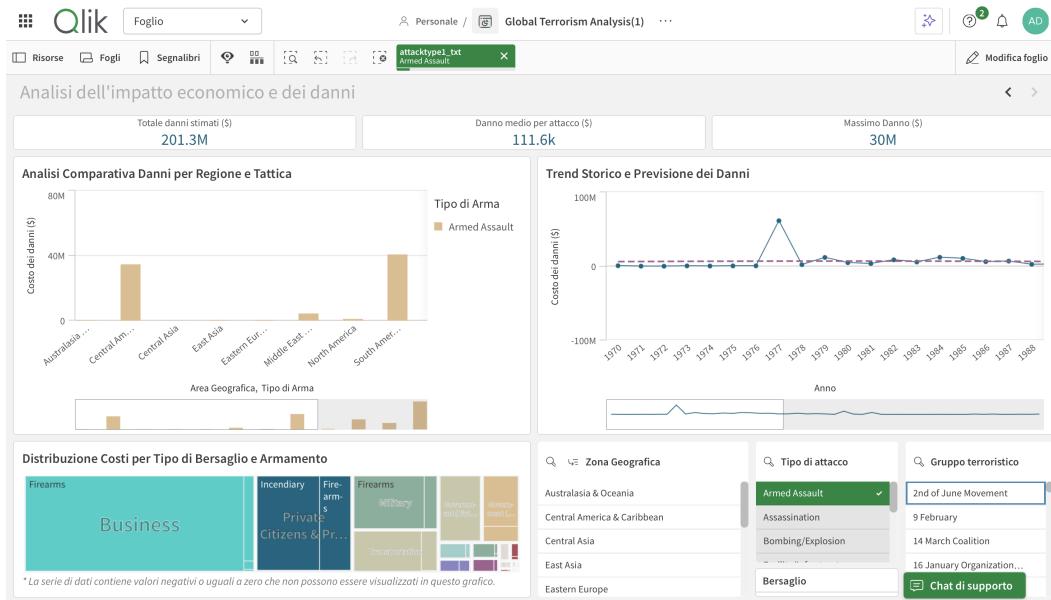


Figura 1.19: Analisi dell'impatto economico e danni causati per filtro Tipo di Attacco (Armed Assault)

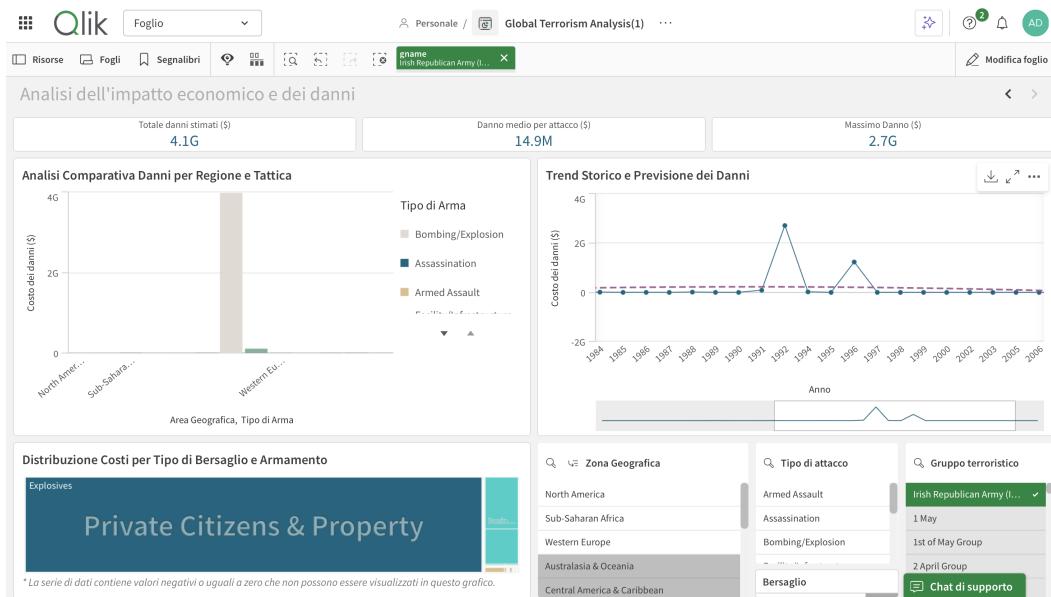


Figura 1.20: Analisi dell'impatto economico e danni causati per filtro Gruppo Terroristico

Nel complesso, la dashboard dimostra la propria capacità di rispondere a interrogativi strategici legati alla quantificazione e distribuzione del danno economico. L'interattività dei filtri trasforma la visualizzazione da strumento descrittivo a supporto decisionale, consentendo di adattare l'analisi a specifici contesti geografici, settoriali o temporali e di valutare in modo puntuale l'esposizione patrimoniale al rischio terroristico.

# CAPITOLO 2

---

Tableau

---

*Preambolo da scrivere*

## 2.1 Seguire pdf 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](http://www.anipapozzi.it)