MACHINE LEARNING PER CARATTERIZZARE GLI ATTACCHI TERRORISTICI

SILVIA FIGINI (*)

Nota presentata dal m.e. Silvio Beretta
(Adunanza del 24 maggio 2018)

SUNTO. – Per i dipartimenti di sicurezza la comprensione delle dinamiche degli eventi terroristici attraverso lo studio di "pattern" ricorrenti può contribuire allo sviluppo della strategia antiterrorismo. Le tecniche di apprendimento automatico, opportunamente integrate con l'opinone dell'esperto, sono utili per descrivere i comportamenti terroristici con elevata precisione. Questa nota intende proporre l'applicazione di tecniche computazionali per l'analisi del Global Terrorism Database. Le proposte metodologiche e computazionali descritte nel seguito potrebbero supportare i dipartimenti di sicurezza e di governo, fornendo indicazioni e informazioni derivate dall'analisi dei dati.

***

ABSTRACT. – For security departments understanding the dynamics of terrorist events finding significant and recurrent patterns can have an important impact in the counter-terrorism strategy development. Machine learning techniques coupled with domain knowledge are useful to understand terrorist behaviours with high accuracy, thus helping policy makers for time-sensitive understanding of terrorist activity, which can enable precautions to avoid against future attacks. In this paper different computational techniques, able to derive relationships among terrorist attacks and detect terrorist behaviours, are used on the Global Terrorism Database. The analysis proposed in this paper could help security and government departments to prevent terrorist attacks and to reduce financial, human and political losses. Furthermore, this information can be useful for law enforcement agencies to propose reactive strategies.

(*) Dipartimento di Scienze Politiche e Sociali, Università degli Studi di Pavia, Italy. E-mail: silvia.figini@unipv.it

1. Introduzione

L'analisi del rischio derivante da atti terroristici viene affrontata, nel rispetto della normativa vigente, nell'ambito delle funzioni convenzionalmente riferite alla "Difesa Civile", ossia inerente la sicurezza dello Stato, comprendendo tutte le situazioni emergenziali che derivano da atti definibili "di aggressione alla nazione" e pertanto anche quelle connesse agli atti terroristici. Essa ha il compito di assicurare la continuità dell'azione di governo, proteggendo da un lato la capacità economica, produttiva e logistica del Paese e dall'altro riducendo l'impatto degli eventi di crisi sulla popolazione.

La letteratura specialistica ed in particolare le pubblicazioni dell'agenzia federale americana FEMA (Federal Emergency Management Agency), tra cui sicuramente vale la pena evidenziare il documento intitolato "Managing the emergency consequences of terrorist incidents: a planning guide for state and local governments", classifica le tipologie di minaccia generate dall'uso delle cosiddette "armi di distruzione di massa", definite a loro volta come qualsiasi arma che è progettata o destinata a causare la morte o gravi lesioni corporali attraverso il rilascio, la diffusione, o l'impatto di sostanze chimiche tossiche o velenose, organismi patogeni, radiazioni o radioattività, esplosive o incendiarie.

Un programma di "Previsione e Prevenzione", rispetto all'analisi ed alla definizione del rischio terroristico, è orientato alla individuazione delle principali tipologie di evento rispetto alle quali potranno essere definite le procedure di intervento, nel rispetto delle competenze specifiche definite per il rischio terroristico.

2. Rassegna della letteratura

Nell'osservare un dato fenomeno, è spesso importante monitorare se una quantità che ci interessa raggiungerà o non raggiungerà un livello critico. Questo tipo di analisi diventa fondamentale quando il fenomeno studiato può avere un forte impatto sulla vita umana, come nel caso degli eventi terroristici.

Lo studio di modelli che forniscano risposte accurate in merito ai rischi di terrorismo e ai processi sociali e politici globali che generano questi eventi (see e.g. Sornette and Ouillon, 2012, McMorrow, 2009) è di estremo interesse a livello mondiale. Il lavoro proposto da

McMorrow (2009) considera la variabile "numero di morti" riferita a singoli eventi terroristici come variabile obiettivo da spiegare in funzione di altre caratteristiche legate all'attacco, come ad esempio aspetti longitudinali del fenomeno (vedi ad esempio Enders e Sandler, 2002), motivazioni di carattere politico o sociale (vedi ad esempio Brown, Dalton e Hoyle, 2004, Enders and Sandler, 2006, Valenzuela *et al.*, 2010), caratteristiche delle organizzazioni terroristiche (vedi ad esempio Asal e Rethemeyer, 2008 o Enders, Sandler e Gaibulloev, 2011). Buona parte dei lavori si basa sull'analisi delle serie storiche e di strumenti qualitativi per produrre scenari possibili (vedi per esempio. Wulf, Haimes e Longstaff, 2003).

Pape (2003) e Li (2005) propongono, per l'analisi dei fenomeni terroristici, l'applicazione di modelli quantitativi basati sull'analisi fattoriale e più recentemente Desmarais e Cranmer, 2011 e Tutun *et al.*, 2017 studiano il terrorismo attraverso le reti sociali.

Come riportato nel lavoro di Tutun *et al.*, 2017, "prevedere un evento terroristico è un sogno, ma identificare una zona rischiosa utilizzando eventi passati è una realtà". Attraverso l'analisi dei dati è possibile derivare un insieme di informazioni per ridurre i rischi degli attacchi con l'obiettivo di contenere il rischio generale e quello di comprendere il fenomeno.

Al fine di rilevare potenziali aree critiche, in questa nota vengono utilizzati diversi approcci di *machine learning*, analizzando i comportamenti legati all'attività terroristica passata e infine valutando il rischio futuro di un evento terroristico in una particolare area geografica. Quando si studiano particolari fenomeni come la criminalità, è prassi comune mappare gli eventi criminali per individuare punti nevralgici attraverso tecniche di segmentazione non supervisionata (Eck *et al.*, 2005) eventualmente integrate da modelli locali (Usha e Rameshkumar, 2014) che consentono di valutare le associazioni tra eventi. Questo lavoro presenta tecniche di identificazione e di caratterizzazione degli attacchi terroristici basate su metodi di clustering fondati sui concetti di "densità" e di "hot spot". Sono stati studiati anche modelli di previsione per valutare con elevata precisione la rischiosità di un'area geografica specifica. Le tecniche di calcolo impiegate forniscono una stima quantitativa della probabilità, sotto condizione di incertezza, di un evento terroristico in una specifica area geografica. Le evidenze empiriche sono ottenute utilizzando dati quantitativi derivati dal Global Terrorism Data Base. Riteniamo che i risultati ottenuti utilizzando que-

ste tecniche, abbinati alle conoscenze degli esperti del settore, potrebbero aiutare le agenzie governative a prevenire le conseguenze di eventi terroristici e a controllare i comportamenti terroristici stessi, riducendo così il rischio di eventi futuri. I risultati potrebbero potenzialmente consentire un ampliamento delle tecniche standard impiegate nei dipartimenti di sicurezza.

3. Modelli di *machine learning* per comprendere eventi terroristici

I modelli non supervisionati di classificazione basati su "Density-Based Spatial Clustering of Applications with Noise" (*DBSCAN*) (see e.g. Ester M. *et al.* 1996) identificano raggruppamenti di punti che presentano similarità misurata attraverso il concetto di intorno (ε – *neighbourhood)* e distanza d:

$$N_{\varepsilon}(p) : \{q | d(p, q) \leq \varepsilon\} \quad (1)$$

dove d è una misura di distanza, ε R^{+} e p un punto.

Una regione di punti è "densa" se il numero di *neighbours* è maggiore di un valore soglia specificato. Il valore della soglia consente di classificare le nostre osservazioni (punti) in "core", "border" e "noise" come riportato in *Fig. 1.*

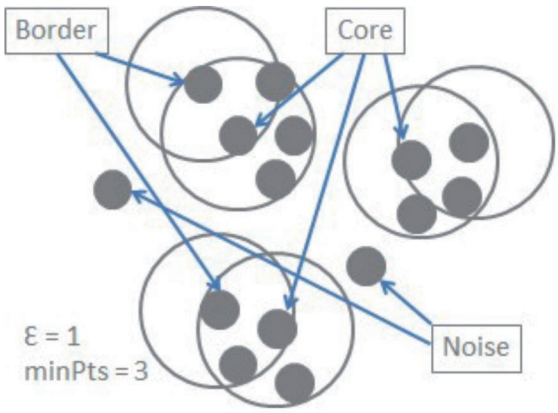

Fig. 1 – Rappresentazione dei punti (punti core, di bordo e di rumore).

Il risultato dell'algoritmo DBSCAN è duplice: regioni dense nello spazio dati (gruppi di osservazioni) e un insieme di punti che vengono classificati come valori anomali dell'insieme dati in analisi.

Nel nostro contesto, l'algoritmo DBSCAN è indicato per l'analisi degli eventi terroristici (Divya *et al.*, 2014) e a differenza degli algoritmi gerarchici di cluster analysis, il numero di gruppi (o cluster) viene identificato automaticamente dalla procedura. Applicando l'algoritmo DBSCAN è possibile identificare aree geografiche che presentano una maggiore concentrazione di attacchi terroristici o episodi di crimine nel tempo.

Un secondo obiettivo dell'analisi è quello di ricavare relazioni tra le caratteristiche degli attacchi terroristici attraverso tecniche di tipo locale basate sulle associazioni (Agrawal R. *et al.*, 1993), con l'obiettivo di estrarre correlazioni interessanti, schemi frequenti, associazioni o strutture casuali tra insiemi di elementi all'interno di un dataset organizzato in modo transazionale. Le misure più comuni in grado di valutare la validità della regola sono: support, confidence e lift.

L'ultimo obiettivo dell'analisi è legato alla caratterizzazione di un determinato evento terroristico attraverso l'uso di modelli supervisionati. Ding *et al.* (2017) hanno proposto modelli basati sulle reti neurali per la previsione di attacchi terroristici. Nella nostra ricerca, confontiamo modelli parametrici (es. Regressione Logistica, LR) con modelli non parametrici (es. gradient boosting machine GBM, random forest RF, ed Evolutionary Learning of Globally Optimal Classification Tree, EVTREE).

4. Dati a disposizione

I dati analizzati in questo studio provengono dal Global Terrorism Database (GTD) che raccoglie diverse informazioni sugli attacchi terroristici avvenuti in tutto il mondo. Nell'ultima versione del dataset vengono raccolti tutti gli attacchi terroristici tra il 1970 e il 2015.

Esso è gestito dal Consorzio Nazionale per lo studio del terrorismo e le risposte al terrorismo (START). Le informazioni raccolte sono il risultato di un processo deliberativo e consultivo avviato inizialmente dal comitato consultivo GTD tra gennaio e maggio 2006, le successive

revisioni sono state apportate dal personale GTD, con la guida dell'Advisory Board.

Nella GTD un attacco terroristico è definito come l'uso effettivo o minacciato di forza e violenza illegali da parte di un attore non statale per raggiungere un obiettivo politico, economico, religioso o sociale attraverso la paura, la coercizione o l'intimidazione.

I dati a disposizione contengono 156.772 attacchi terroristici in 206 paesi diversi, avvenuti tra il 01/01/1970 e il 31/12/2015. Per essere coerenti con le precedenti analisi di questo documento, vengono considerati solo gli attacchi terroristici avvenuti dopo l'11/09/2001, quindi 83.527 attacchi in 158 paesi diversi.

La *Tab. 1* mostra il numero di attacchi terroristici e il numero di morti durante gli attacchi in Europa nel periodo considerato confrontando l'Europa orientale e occidentale. È evidente che negli ultimi anni c'è stato un aumento del numero di attacchi terroristici, specialmente nell'Europa orientale, con un conseguente aumento anche dell'impatto degli attacchi.

Tab. 1 – Numero di attacchi per ognuno degli anni in esame.

Anno	**Numero di eventi**	
	Europa orientale	**Europa occidentale**
2001	38	330
2002	111	104
2003	100	121
2004	45	59
2005	75	100
2006	70	98
2007	62	72
2008	209	162
2009	165	180
2010	259	132
2011	196	92
2012	173	188
2013	165	253
2014	958	214
2015	684	321

Per comprendere la natura degli attacchi terroristici è anche importante osservare l'obiettivo coinvolto e il tipo di attacco. Nelle *Tabs. 2* e *3* sono mostrate le distribuzioni di tipo e target, confrontando l'Europa orientale e occidentale.

Tab. 2 – Incidenza di attacchi e morti per ognuno degli anni presi in esame.

Tipologia di attacco	**Percentuale di eventi**	
	Europa orientale	**Europa occidentale**
Deflagrante	55.6%	57.8%
Assalto armato	26.8%	9.5%
Assassinio	5.3%	1.4%
Attacco a strutture/infrastrutture	4.6%	27.4%
Rapimento ostaggi	3.8%	0.5%
Assalto disarmato	1.0%	1.0%
Barricamento con ostaggi	0.3%	0.5%
Dirottamento	0.1%	0.6%
Sconosciuto/Non specificato/Altro	2.35%	0.31%

Tab. 3 – Incidenza di attacchi per ogni anno preso in esame.

Tipologia obiettivo	**Percentuale eventi**	
	Europa orientale	**Europa occidentale**
Aeroporti ed Aerei	0.2%	0.5%
Affari e Business	7.2%	17.9%
Istruzione	0.1%	1.3%
Forniture di cibo e acqua	0.1%	0.0%
Governativo	12.4%	15.8%
Giornalisti e Media	1.6%	1.4%
Militare	29.3%	2.0%
ONG	0.4%	0.5%
Polizia	17.6%	12.2%
Cittadini private e proprietà private	16.1%	27.8%
Figure e istituzioni religiose	3.1%	4.6%
Telecomunicazioni	0.33%	4.6%
Terroristi e milizia non governativa	0.3%	0.2%
Turisti	0.1%	0.4%
Trasporti	5.7%	3.3%
Utilità	1.2%	0.3%
Partiti politici violenti	0.1%	0.4%
Altro	0.3%	3.6%
Sconosciuto	2.6%	5.9%

Osservando il tipo di attacchi è evidente che il più frequente è di tipo deflagrante; inoltre, notiamo che le situazioni in Europa orientale e occidentale si presentano molto diverse. In Europa occidentale gli attacchi alle strutture ed infrastrutture sono il secondo tipo più frequente, mentre nell'Europa orientale troviamo assalti armati.

Questa differenza è evidente anche rispetto agli obiettivi degli attacchi. Nell'Europa orientale gli obiettivi più frequenti sono a carat-

tere militare e poliziesco, mentre in Europa occidentale gli obiettivi più frequenti sono privati cittadini e imprese.

In primo luogo, utilizzando l'algoritmo DBSCAN, gli hot spot sono identificati come aree critiche con un livello elevato di frequenza di attacchi terroristici. Quindi l'associazione tra località, target coinvolti, proprietà e tipo di attacchi viene valutata mediante analisi delle regole di associazione, considerando singolarmente i diversi hot spots identificati. Infine, viene valutata la probabilità di un evento terroristico per ogni specifico Paese considerato.

I risultati spiegati si ottengono osservando gli attacchi in una finestra temporale che va dall'11/09/2001 (data degli attacchi alle torri gemelle) fino al 31/12/2015. Inoltre, sono stati considerati solo gli attacchi terroristici in Europa.

Inizialmente gli attacchi sono raggruppati usando l'algoritmo DBSCAN per identificare gli hot spots, ovvero le aree geografiche che soffrono principalmente di attacchi terroristici. Per sviluppare questa analisi sono state prese in considerazione informazioni sulla posizione degli attacchi, in particolare le variabili di latitudine e longitudine dal database GTB.

Per applicare DBSCAN, dobbiamo assegnare un valore al raggio di vicinato ε e alla soglia di densità minPts. Dopo un'attenta analisi di sensitività abbiamo selezionato minPts = 10 poiché questo valore fornisce una chiara descrizione di un gruppo significativo di eventi in termini di interpretabilità dei risultati. Per selezionare il valore ε un metodo comune consiste nel tracciare i punti kNN distanze (ovvero la distanza dal kth vicino più vicino) in ordine decrescente e cercare una discontinuità nel grafico. Osservando la trama nella *Fig. 2* impostiamo ε = 1. Per valutare la distanza tra due punti viene utilizzata la distanza euclidea.

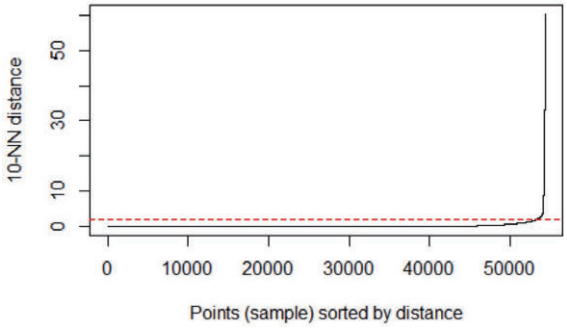

Fig. 2 – Distanze.

Di conseguenza, l'algoritmo DBSCAN ha identificato 35 diversi hot spot. La *Fig. 3* mostra la posizione nella mappa europea degli hot spots ottenuti. Ogni punto rappresenta un attacco terroristico e la dimensione del cerchio riflette il numero di morti nell'attacco. Colori diversi sono correlati a diversi cluster, vale a dire diversi hot spot identificati tramite l'algoritmo DBSCAN. Come previsto, alcune località geografiche, purtroppo note per aver subito attacchi terroristici, sono identificate come punti caldi, tra questi: il nord dell'Irlanda, il nord della Spagna e Madrid, la Corsica e il confine tra Russia e Ucraina. I risultati ottenuti da DBSCAN sono confermati anche da caratterizzazioni storiche, inclusi motivi sociali e politici.

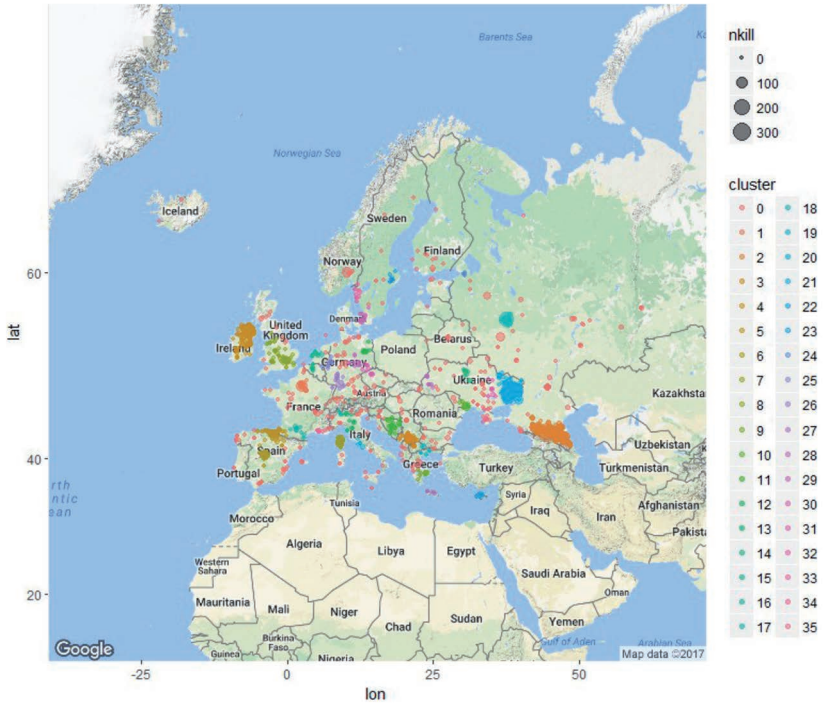

Fig. 3 – Mappa Europea con i punti individuati.

Dopo aver identificato le aree geografiche ad alto rischio di attacchi terroristici è anche interessante capire le peculiarità di questi attacchi e scoprire se esistono delle relazioni tra posizione, tipo di attacco e bersaglio.

Per analizzare questi aspetti dei fenomeni, è stato applicato l'algo-

ritmo delle regole di sequenza, prima sul set di dati totale e poi su ogni singolo hot spot identificato tramite l'algoritmo DBSCAN. In questa analisi si definisce come transazione una combinazione di diversi elementi quali posizione, tipo di attacco e bersaglio coinvolto, in modo da indagare se ci siano alcuni schemi ricorrenti tra queste informazioni.

Sulla base dei dati a disposizione, come criterio per considerare interessante una regola di associazione, vengono considerati solo i casi con un lift maggiore di 1. Questi indicatori evidenziano che LHS e gli elementi RHS appaiono più spesso insieme del previsto, ovvero il verificarsi di LHS ha un effetto positivo sul verificarsi di RHS. Viene quindi utilizzato l'algoritmo Apriori impostando la soglia su 1.

Sotto queste ipotesi si trovano in totale 158 regole interessanti. Tra questi, il valore minimo di occorrenza di una regola è 29 e il massimo 742, con un valore medio di occorrenza di 120. La *Tab. 4* mostra alcuni esempi di associazione tra posizione dell'attacco, bersaglio coinvolto e proprietà e tipo di attacco. È possibile osservare le relazioni tra la posizione geografica e il tipo di attacco, ad esempio a Donetsk, in Ucraina, gli assalti armati alle unità militari hanno un'alta frequenza, mentre in Corsica gli attacchi terroristici che utilizzano strumenti deflagranti sono più comuni; in Africa gli attacchi sono rivolti, con alta probabilità, infrastrutture e strutture. Vengono inoltre visualizzati i valori di affidabilità e occorrenza per ciascuna regola rilevata.

L'analisi delle regole di sequenza può essere applicata anche a ciascun hot spot separatamente, in questo modo è possibile identificare quali sono i tipi di attacchi più probabili e il target coinvolto per posizione.

Seguendo questa idea, è possibile trarre alcune conclusioni su particolari aree geografiche. Di seguito alcuni esempi di applicazioni su alcuni hot spot identificati tramite l'algoritmo DBSCAN:

- Hot spot 21, situato tra Ucraina e Russia: gli attacchi armati o deflagranti ai militari sono il tipo più probabile di attacchi terroristici
- Hot spot 4, situato nell'Irlanda del Nord e nel Regno Unito: gli attacchi deflagranti a cittadini privati, proprietà e infrastrutture può avvenire con una probabilità maggiore rispetto ad altri tipi di attacchi.
- Hot spot 9, situato in Grecia: gli attacchi più frequenti sono a strutture e a infrastrutture, così come attacchi deflagranti all'edificio del governo.

Infine, vengono confrontati diversi algoritmi predittivi per valutare quale sia la probabilità di attacchi terroristici in una specifica regione geografica nel mese successivo.

Tab. 4 – Esempi delle regole di associazione ottenute.

Lato sinistro	Lato destro	Confidenza	Occorrenza
Luogo: Donetsk, *Tipologia:* Assalto armato	*Obiettivo:* Militare	0.88	220
Luogo: Attica	*Tipologia:* Attacco a strutture ed infrastrutture	0.50	176
Obiettivo: Militare, *Tipologia:* Assalto armato	*Luogo:* Donetsk	0.59	220
Luogo: Luhansk	*Obiettivo:* Militare	0.57	250
Luogo: Corsica	*Tipologia:* Deflagrante	0.94	193
*Obiettivo:*Trasporti	*Tipologia:* Deflagrante	0.88	227

Per sviluppare questa analisi viene creato un nuovo set di dati, definito, per ogni mese considerato e paese, dal verificarsi o meno di un evento terroristico nel mese successivo. Questo risultato binario viene quindi utilizzato come variabile obiettivo per i modelli supervisionati impiegati. In questo nuovo set di dati 1890 osservazioni sono etichettate come 1 e 19842 come 0. Le covariate impiegate sono: la regione del paese, i timestamp (ad es. Numero di giorni dall'11/01/2001), il livello di violenza nella stessa regione e in tutti le altri Regioni europee (ad es. Numero di attacchi) nei sei mesi precedenti. Ulteriori informazioni sulla politica e la fragilità sociale di ogni specifico paese nel tempo sono anche prese in considerazione e sono tratte dalle matrici dell'indice di fragilità di ciascun paese. La spiegazione di ciascuna variabile può essere trovata in Messner *et al.*, 2015. Nella *Tab. 5* è presentato il riassunto di covariate impiegate.

Tab. 5 – Riepilogo covariate utilizzate.

Variabile	Min	Q1	Media	Q3	Max
Nr. di precedenti attacchi nello stesso paese	0	0	6.09	2	676
Nr. di precedenti attacchi in Europa	0	92	195	212	828
Punteggio ordinamento politico	-7	9	8.66	10	10
Punteggio di frammentazione dell'ordinamento politico	0	0	0.19	0	3
Durata del regime	0	13	40.14	63	167
Indice di fragilità dello Stato	0	0	2.11	3	11
Efficacia	0	0	0.98	2	6
Legittimità	0	0	1.14	2	5
Effetto sicurezza	0	0	0.14	0	2
Legittimità della sicurezza	0	0	0.29	1	3
Efficacia politica	0	0	0.33	1	2
Legittimità politica	0	0	0.62	1	3
Legittimità economica	0	0	0.18	0	2

Per il modello Gradient Boosting Machine il numero minimo di campioni in un nodo per iniziare la divisione viene preso pari a 10. Inoltre, sono stati esaminati un totale di 20 valori da 50 a 10000 per il numero di iterazioni, 5 possibili valori (1,3,6, 9,10) per la complessità dell'albero e 100 valori compresi tra 0,0005 e 0,05 con uno step di 0,05 per il tasso di apprendimento. Si è quindi osservato che l'AUC più alto si ottiene con un numero di alberi pari a 300, complessità dell'albero 9 e tasso di apprendimento 0,0195.

Vengono confrontate due diverse misure di prestazione: AUC e misura H (Hand D. J., 2009). La *Tab. 6* riporta i risultati ottenuti in termini di out-of-sample. Sulla base dei dati a portata di mano i modelli sono equivalenti in termini di capacità predittiva, come confermato dal test De Long (vedi De Long *et al.*, 1988).

Tab. 6 – AUC e indice H per i modelli predittivi.

Valutazione dei modelli	**LR**	**GBM**	**RF**	**EVTREE**
AUC	0.89	0.90	0.90	0.87
H	0.55	0.57	0.58	0.54

Per mostrare come il nostro approccio possa fornire risultati interessanti ai fini della valutazione del rischio di un attacco terroristico in un dato paese nel prossimo mese, ci focalizziamo sulla parte metodologica. Più precisamente, la fase di addestramento e test utilizzata in questa sezione coinvolge i dati fino al 30/11/2015. Ora proviamo ad applicare il modello al prossimo mese non preso in esame per la fase precedente: dicembre 2015. Viene quindi calcolata la media delle probabilità ottenute utilizzando tutti i modelli addestrati, e ciò che otteniamo è la probabilità prevista di un attacco terroristico per ciascun paese europeo nell'ultimo mese del 2015.

Usando 0,5 come soglia e confrontando questi risultati con eventi reali accaduti nel dicembre 2015, possiamo vedere che in Francia, Ucraina, Russia, Irlanda, Svezia, Grecia, Italia, Regno Unito e Germania è avvenuto un attacco terroristico e in effetti il modello indica per questi paesi una probabilità di attacco terroristico maggiore di 0,5. In ognuno di questi, osservando i dati, almeno un attacco terroristico ha avuto luogo nel dicembre 2015. Tutti gli altri paesi hanno una bassa probabilità ad eccezione della Repubblica Ceca con probabilità pari a 0,59, dove, fortunatamente, un attacco terroristico non ha avuto luogo in Dicembre 2015 (*Tab. 7*).

Tab. 7 – Probabilità prevista dell'evenienza di un attacco terrorstico per ogni nazione nel Dicembre 2015.

Nazione	**Probabilità**	**Nazione**	**Probabilità**
Albania	0.32	Italia	0.50
Austria	0.34	Kosovo	0.45
Bielorussia	0.26	Lettonia	0.26
Belgio	0.28	Macedonia	0.36
Bulgaria	0.39	Moldavia	0.30
Croazia	0.24	Montenegro	0.30
Cipro	0.34	Paesi Bassi	0.41
Repubblica Ceca	0.59	Norvegia	0.31
Danimarca	0.37	Portogallo	0.26
Estonia	0.29	Romania	0.18
Finlandia	0.38	Russia	0.87
Francia	0.75	Serbia	0.25
Germania	0.70	Spagna	0.50
Grecia	0.79	Swezia	0.65
Ungheria	0.31	Svizzera	0.42
Irlanda	0.72	Ucraina	0.76
		Regno Unito	0.79

4. Conclusioni e ulteriori analisi

Negli ultimi decenni i gruppi terroristici hanno ampliato la loro portata e i loro attacchi sono più frequenti e più letali.

Utilizzando i dati a disposizione, viene quindi sviluppato un modello per valutare il livello di rischio terroristico di diverse località.

I risultati ottenuti mostrano schemi ricorrenti di attacchi terroristici. Le nostre metodologie possono aiutare gli analisti del terrorismo a migliorare le misure antiterrorismo e potenzialmente a prevenire attacchi futuri.

Per ricerche future, prevediamo di raccogliere ulteriori dati sui terroristi e sui loro gruppi in modo da poter costruire un profilo su di essi. In questo modo, ci aspettiamo che si possano identificare preventivamente futuri episodi di terrorismo entro un raggio più breve e con una maggiore precisione in termini di posizione.

REFERENCES

[1] Agrawal R., Imielin ski T., and Swami A. Mining association rules between sets of items in large databases. *SIGMOD Rec.*, 22(2):207-216, (1993).

[2] Asal V. and Rethemeyer R. K. The nature of the beast: Organizational structures and the lethality of terrorist attacks. *Journal of Politics*, 70:437-449, (2008).

[3] DeLong E.R., DeLong D.M., and Clarke-Pearson D.L. Comparing the areas under two or more cor- related receiver operating characteristic curves: a non-parametric approach. *Biometrics*, 44:837-845, (1988).

[4] Desmarais B. A. and Cranmer S. J. Forecasting the locational dynamics of transnational terrorism: A network analytic approach. *European Intelligence and Security Informatics Conference*, pages 171- 177, (2011).

[5] Ding F., Ge Q., Jiang D., Fu J., and Hao M. Understanding the dynamics of terrorism events with multiple-discipline datasets and machine learning approach. *PLOS ONE*, 12, (2017).

[6] Divya G., Robinson R., and K. Selvan. Suitability of clustering algorithms for crime hotspot analysis. *International Journal of Science, Engineering and Computer Technology*, 4(7):231-234, (2014).

[7] Eck J., Chainey S., Cameron J., and Wilson R. Mapping crime: Understanding hotspots. *National Institute of Justice: Washington DC.*, (2005).

[8] Enders W. and Sandler T. Patterns of transnational terrorism, 1970-1999: Alternative time-series estimates. *International Studies Quarterly*, 46:145-165, (2002).

[9] Enders W. and Sandler T. The political economy of terrorism. cambridge. *Univ. Press, Cambridge*, (2006).

[10] Enders W., Sandler T., and Gaibulloev K. Domestic versus transnational terrorism: Data, decomposition, and dynamics. *Journal of Peace Research*, 48:319-337, (2011)

[11] Ester M.; Kriegel H.P.; Sander J. and X. Xiaowei. A density-based algorithm for discovering clusters a density-based algorithm for discovering clusters in large spatial databases with noise. In *Second International Conference on Knowledge Discovery and Data Mining*, pages 226-231, (1996).

[12] Hand D.J. Measuring classifier performance: a coherent alternative to the area under the roc curve. *Machine Learning*, 77:103-123, (2009).

[13] Li Q. Does democracy promote or reduce transnational terrorist incidents? *Journal of Conflict Resolution*, 49:278-297, (2005).

[14] McMorrow D. Rare events. *JASON Report, The MITRE Corporation, McLean, VA.*, (2009).

[15] Messner J., Haken N., Taft P., Blyth H., Lawrence K., Pavlou S., and Umana F. Fragile states index 2015. *Fund for Peace*, (2015).

[16] Pape R. A. The strategic logic of suicide terrorism. *American Political Science*, 97:343-361, (2003).

[17] Sornette D. and Ouillon G. Dragon-kings: Mechanisms, statistical methods and empirical evidence. *The European Physical Journal Special Topics*, 205(1):1-26, (2012).

[18] Tutun S., Khasawneh M.T., and Zhuang J. New framework that uses patterns and relations to under- stand terrorist behaviors. *Expert System with Applications*, (2017).

[19] Usha D. and Rameshkumar K. A complete survey on application of frequent pattern mining and association rulemining on crime pattern mining. *International journal of Advances in Computer Science and Technology*, 3:264-275, 04 2014.

[20] Valenzuela M. L., Feng C., Reddy P., Momen F., Rozenblit J. W., Eyck B. T., and Szidarovszky F. A non-numerical predictive model for asymmetric analysis. pages 311-315, (2010).

[21] Wulf W. A.; Haimes Y. Y. and Longstaff T. A. Strategic alternative responses to risks of terrorism. *Risk Analysis*, 23:429-444, (2003).