ISSN 2421-4442

SICUREZZA TERRORISMO SOCIETÀ

Security Terrorism Society

INTERNATIONAL JOURNAL - Italian Team for Security, Terroristic Issues & Managing Emergencies

2
2015

EDUCatt

SICUREZZA, TERRORISMO E SOCIETÀ

INTERNATIONAL JOURNAL
Italian Team for Security,
Terroristic Issues & Managing Emergencies

2

ISSUE 2/2015

Milano 2015

EDUCATT - UNIVERSITÀ CATTOLICA DEL SACRO CUORE

SICUREZZA, TERRORISMO E SOCIETÀ
INTERNATIONAL JOURNAL – Italian Team for Security, Terroristic Issues & Managing Emergencies

ISSUE I – 2/2015

Direttore Responsabile:

Matteo Vergani (Università Cattolica del Sacro Cuore – Milano e Global Terrorism Research Centre – Melbourne)

Co-Direttore e Direttore Scientifico:

Marco Lombardi (Università Cattolica del Sacro Cuore – Milano)

Comitato Scientifico:

Maria Alvanou (Lecturer at National Security School – Atene)
Cristian Barna ("Mihai Viteazul" National Intelligence Academy– Bucharest, Romania)
Claudio Bertolotti (senior strategic Analyst at CeMiSS, Military Centre for Strategic Studies – Roma)
Valerio de Divitiis (Expert on Security, Dedicated to Human Security – DEDIHS)
Chiara Fonio (Università Cattolica del Sacro Cuore – Milano)
Sajjan Gohel (London School of Economics – London)
Rovshan Ibrahimov (Azerbaijan Diplomatic Academy University – Baku, Azerbaijan)
Daniel Köhler (German Institute on Radicalization and De-radicalization Studies – Berlin)
Miroslav Mareš (Masaryk University – Brno, Czech Republic)
Vittorio Emanuele Parsi (Università Cattolica del Sacro Cuore – Milano)
Anita Perešin (University of Zagreb – Croatia)
Giovanni Pisapia (Senior Security Manager, BEGOC – Baku – Azerbaijan)
Iztok Prezelj (University of Ljubljana)
Eman Ragab (Al-Ahram Center for Political and Strategic Studies (ACPSS) – Cairo)
Riccardo Redaelli (Università Cattolica del Sacro Cuore – Milano)
Mark Sedgwick (University of Aarhus – Denmark)
Arturo Varvelli (Istituto per gli Studi di Politica Internazionale – ISPI – Milano)
Kamil Yilmaz (Independent Researcher – Turkish National Police)
Munir Zamir (Fida Management&C7 – London)
Sabina Zgaga (University of Maribor – Slovenia)
Ivo Veenkamp (Hedayah – Abu Dhabi)

Comitato Editoriale:

Gabriele Barni (Università Cattolica del Sacro Cuore – Milano)
Alessandro Burato (Università Cattolica del Sacro Cuore – Milano)
Alessia Ceresa (Università Cattolica del Sacro Cuore – Milano)
Barbara Lucini (Università Cattolica del Sacro Cuore – Milano)
Davide Scotti (Università Cattolica del Sacro Cuore – Milano)

© 2015

EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.7234.22.35 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione); librario.dsu@educatt.it (distribuzione)
web: www.educatt.it/libri
Associato all'AIE – Associazione Italiana Editori
ISBN: 978-88-6780-958-5

copertina: progetto grafico Studio Editoriale EDUCatt

Table of contents

Focus: Grandi Eventi

SOCial Media INTelligence: un nuovo spazio per la raccolta di informazioni rilevanti

Alessandro Burato[1]

ITSTIME Italian Team for Security, Terroristic Issues & Managing Emergencies

Keywords

SOCMINT, Social Media Intelligence, Information, Social Network, Intelligence, Terrorism, Analysis, Regulation.

Parole chiave

SOCMINT, Social Media Intelligence, Informazioni, Social Network, Intelligence, Terrorismo, Analisi, Regolamenti.

1. COSA è?

La SOCial Media INTelligence è una delle tecniche di reperimento di informazioni utili al ciclo di intelligence tramite il monitoraggio e l'analisi dei contenuti scambiati attraverso i Social Media [1]. Al momento il dibattito teorico ruota intorno alla possibilità di considerare come autonoma tale tecnica, oppure come strettamente dipendente e quindi quasi assimilabile alla Open Source INTelligence. Parte dei diversi ambiti e approcci alla ricerca di informazioni significative (Techint, geoint, sigint, Humint, Masint, Cibint, etc) la OSINT (Open Source INTelligence) si configura come la sistematica raccolta, analisi e disseminazione di informazioni che possano essere giustificate da una specifica necessità di intelligence. L'errore che frequentemente viene fatto è di pensare che tale pratica sia confinata solo al materiale accessibile online. L'OSINT si riferisce invece, non solo ad Internet,

[1] Università Cattolica del Sacro Cuore – Milano
Largo Gemelli 1, 20123, Milano, (IT)
ITSTIME – Department of Sociology
E-mail address: alessandro.burato@itstime.it

ma anche a radio e televisione, giornali e riviste, pubblicazioni istituzionali ed accademiche, ecc. Questo aspetto, spesso ignorato, definisce invece una linea di demarcazione chiara tra OSINT e SOCMINT: quest'ultima infatti vede come oggetto delle sue indagini unicamente le informazioni scambiate tramite i Social Media.

A tal proposito è necessaria un'ulteriore precisazione. Il panorama dei social media infatti non deve essere ridotto alla semplice considerazione dei social network: parte integrante e forse più nota dei media sociali, i social network sono solo una delle componenti del notevolmente più ampio spettro dei social media, da ognuno dei quali la SOCMINT è in grado di estrarre informazioni con diversi gradi di rilevanza e significatività [2].

2. COSA può ottenere?

È evidente che l'aspetto fondamentale attorno a cui ruota tutto il dibattito sulla SOCMINT è l'identificazione degli obiettivi che è in grado di raggiungere. Le finalità dell'indagine dei Social Media attraverso la SOCMINT sono diverse ma possono essere raggruppate, con il solo scopo di esemplificare alcune, in tre macro categorie [1].

Dapprima, i social media possono fornire informazioni crowd-sourced, ciò dati direttamente generati dal pubblico che, aggregati secondo determinati parametri, sono in grado di delineare il quadro generale di una situazione in tempo reale. Questa pratica è stata impiegata recentemente in svariati contesti, dalla pianificazione dell'intervento umanitario in emergenze di tipo naturali e sanitarie [3,4], all'utilizzo per ragioni di sicurezza in occasione di fenomeni criminali.

In secondo luogo, la SOCMINT, essendo considerata una fonte di informazioni utili ai processi di intelligence, viene prevalentemente impiegata nel tentativo di ridurre l' "ignoranza" e migliorare la qualità del decision-making process fornendo al decisore un quadro informativo più dettagliato [5]. Questo aspetto è primario per la possibilità di migliorare la sicurezza pubblica. Se infatti lo spazio online viene sempre più frequentemente utilizzato per organizzare e coordinare attività criminali, i social media possono fornire uno strumento di inestimabile valore nella loro individuazione.

Nel caso specifico, i "pizzini", hanno fornito un segnale spia per l'apertura di una indagine. Le immagini che sono circolate su account Twitter riprendevano questi fogli con la scritta "siamo nelle vostre strade" fotografati tenendo sullo sfondo oltre a luoghi sensibili tra i quali il Duomo e la stazione centrale di Milano come anche la bandiere con il logo Expo. Sotto l'hashtag #IslamicStateInRome queste foto sono diventate virali proprio quando le stesse erano oggetto di una approfondita indagine svolta nel tentativo di capire

chi fosse l'autore dei messaggi. L'identificazione è avvenuta grazie alla fotografia scattata all'interno della stazione centrale, incrociando i dati visibili sul tabellone delle partenze/arrivi per capire quando era stata scattata e le videocamere di sorveglianza che ritraggono il sospettato scattarla.

Attraverso quindi l'utilizzo di diverse tecniche di indagine, dalle intercettazioni ai pedinamenti, gli inquirenti hanno formulato per i due le accuse di associazione con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico. Infatti, l'analisi delle informazioni a disposizione ha rilevato l'intenzione di Briki e Waqas di partire per la Siria, dove avrebbero ricevuto l'addestramento militare necessario per poi tornare in Italia e colpire, oltre alla base militare di Ghedi, la stazione ferroviaria di Brescia e la ditta di ortofrutta presso la quale lavorava il tunisino come addetto alle pulizie.

Tuttavia, l'utilizzo operativo degli strumenti della SOCMINT non può prescindere dal loro approfondimento e studio in ambito accademico, ma non solo, attraverso programmi di ricerca volti alla comprensione delle dinamiche sociali che su questi mezzi si generano, con lo scopo di affinare la possibilità di identificare eventuali indicatori o condizioni favorevoli all'insorgere di attività criminali, a comprendere meglio quali siano i processi di radicalizzazione prendendo in analisi i diversi utilizzi e impatti che le comunicazioni scambiate possono avere sul pubblico e ad approfondire le possibili interazioni tra comportamenti individuali e collettivi online e offline. La declinazione della *cultural intelligence*, pratica o strategia applicata da sempre anche se teorizzata solo recentemente, secondo gli orizzonti social è infatti uno degli aspetti più significati di ricerca al momento, proprio per approfondire il legame tra significante e significato nelle diverse sub-culture che proliferano nel web.

3. DOVE e PERCHÉ si applica?

La SOCMINT, come già riferito, si applica esclusivamente online. Questa peculiarità dello "spazio" all'interno del quale la raccolta e il monitoraggio delle informazioni si esplica pone la necessità di ripensarlo in merito alla sua distinzione tra "privato" e "pubblico". È noto che online, e specialmente sui social media, la distinzione tra queste due "tipologie" di spazio sia andata sfumandosi tanto che, per esempio, materiali (dati) simili pubblicati sullo stesso social network vengono considerati talvolta pubblici, altre volte privati e nella maggioranza dei casi quasi-privati [6]. Questa mancanza di percezione, e di standardizzazione, di ciò che è considerato privato e ciò che invece viene ritenuto di dominio pubblico porta all'impossibilità di applicare la connotazione spaziale al diritto di privacy lasciando quindi questi media senza un riferimento normativo definito. L'acquisizione dunque di tali materiali

da parte di soggetti terzi potrebbe portare alla diminuzione della percezione della sicurezza di questo "spazio speciale", minandone il suo stesso valore.

Infine, non sono da sottovalutare, nelle considerazioni circa l'impiego di queste tecniche in ambiti relativi alla sicurezza, le pressioni pubbliche al loro sistematico impiego a seguito di indagini che, grazie all'utilizzo della SOCMINT, hanno ottenuto ottimi risultati.

4. COME può essere eticamente e legalmente supportata?

Il tema relativo alla privacy (o alla sua aspettativa) in ambito Social Media è già stata riferita. In generale ogni indagine di intelligence deve mantenere un buon equilibrio tra il benessere economico e sociale, la sicurezza nazionale, che si declina in ordine pubblico e sicurezza pubblica, e i diritti di libertà e di privacy [7].

Nella SOCMINT vengono teorizzati a questo scopo tre livelli di investigazione: il primo prende in esame tutti i contenuti open (quelli per esempio per i quali non è prevista nessuna restrizione imposta dall'utente in termini di privacy), senza concentrare l'analisi su un singolo individuo al solo scopo di analizzare gli andamenti generale del fenomeno di interesse.

Il secondo invece vede oggetto dell'analisi la stessa tipologia di dati ma focalizzati su un singolo individuo al fine di ottenere un numero maggiore di informazioni che lo riguardano. Questa pratica è definita meno intrusiva in relazione invece all'ultima tipologia di investigazione che prevedere l'intercettazione di comunicazioni private.

Ora, quando queste tipologia di indagine non rischiano di minare alla base i principi generali sopra enunciati? È possibile contraddire il proverbio africano secondo cui quando gli elefanti lottano, è sempre l'erba la prima ad andarci di mezzo? La giustificazione della scelta di uno dei tre stadi di intrusività dovrebbe essere giustificata dai diversi parametri tra i quali la causa sufficiente per la violazione della privacy, la proporzionalità dei metodi impiegati per il raccoglimento delle informazioni necessarie, l'idoneità dell'autorità che intraprendete l'azione e le sue autorizzazioni, congiuntamente alla ragionevolezza del successo dell'operazione stessa.

5. COME si inserisce all'interno del circolo di intelligence?

Altra questione fondamentale da dirimere per poter giungere all'applicazione delle tecniche della SOCMINT riguarda le modalità con cui essa contribuisce in ognuna delle fasi che costituiscono il percorso attraverso il quale un'informazione diventa, come dicono i professionisti, "intelligence".

Primo step: ricerca delle informazioni. La raccolta del materiale condiviso attraverso i social media deve avere solide basi metodologiche: data l'enorme quantità di informazioni a disposizione la selezione del campione di quelle da analizzare riveste infatti un ruolo fondamentale. Purtroppo, questo processo, spesso demandato unicamente a persone con elevate competenze in sistemi informatici di filtraggio di dati, risulta più focalizzato sulla raccolta di campioni quanto più ampi tralasciando la rappresentatività degli stessi. Nelle scienze sociali, che dovrebbero trovare uno spazio maggiore nello sviluppo delle tecniche SOCMINT, il valore del campione prescelto è ritenuto di gran lunga più significativo del mero numero di dati raccolti che potrebbero non contenere informazioni rilevanti ai fini dell'analisi [8,9]. Un esempio della generale tendenza a sottostimare la significatività della rappresentatività del campione preso in esame, in particolare nell'analisi dei contenuti condivisi su Twitter, può essere riscontrata nella frequente identificazione degli hashtag quali barriere, già predisposte dallo strumento stesso, alle informazioni relative ad una specifica tematica. Recenti ricerche hanno dimostrato che solo una minor parte delle comunicazioni che si riferiscono ad uno stesso argomento viene "etichettata" attraverso l'utilizzo di queste parole, mentre la maggior parte del flusso resta fuori da tale logica [1].

Nel caso specifico oggetto di questo articolo, l'utilizzo dell'hashtag *#IslamicStateInRome* ha assunto un ruolo fondamentale per identificare l'oggetto specifico delle comunicazioni che venivano divulgate. Tuttavia, anche in questo caso, non è stato l'unico che ha coperto tutte le conversazioni sull'argomento: erano infatti utilizzati anche l'hashtag *#Islamic* seguito dalle parole *State In Rome*, e *#Islamic_State_In_Rome*.

Step 2 e 3: corroborazione e assegnazione di priorità alle informazioni raccolte. Con particolare riferimento alle sole risorse testuali (che costituiscono una parte del materiale analizzabile che comprende anche immagini e video) una delle tecniche impiegate per l'analisi è l'estrazione automatica del loro significato. Tale operazione consente infatti di isolare il materiale rilevante dividendolo in categorie utili alla corroborazione e all'impiego da parte dei decisori delle informazioni stesse [3]. Tuttavia il raggiungimento di tale obiettivo è reso particolarmente complesso da numerosi fattori tra i quali la valutazione del contesto e il concetto gruppo nello spazio online. Per quanto concerne il primo aspetto, contestualizzare l'informazione significa in primo luogo riferirsi al linguaggio come sua diretta espressione e dunque apprezzare nell'analisi l'intenzione, la motivazione, la significazione sociale ed eventuali aspetti denotativi e connotativi delle espressioni utilizzate. In altre parole, la rilevazione del contesto nel quale lo scambio di informazioni avviene passa attraverso la capacità di delineare la situazione e la cultura che lo hanno prodotto. Dall'altra parte, per completare quanto richiesto dagli

step 2 e 3 può essere necessario scavare a fondo in merito al concetto che sottende all'adesione a gruppi virtuali [10]. L'idea di "membership" che li caratterizza non deve essere pedissequamente omologata a quella che definisce le adesioni a gruppi reali: spesso infatti non viene richiesto il pagamento di alcuna "quota sociale", i legami tra i componenti sono più lassi e a volte dettati da pure ragioni opportunistiche. È significativo invece notare come alcuni gruppi online condividano una sorta di identità linguistica (abbreviazioni, modi di dire, espressioni comuni) che li rendono facilmente identificabili. A tal proposito la sociologia digitale fornisce ormai solide basi teoriche per la comprensione delle sub-culture che si sviluppano sui social media e i diversi utilizzi del linguaggio che li caratterizzano.

Ulteriore passaggio, legato a quello appena esposto, è quello espresso nello step 4: la validazione delle informazioni. Tale processo deve tenere conto di aspetti quali il "gaming" e l'"observation effect". Il primo riguarda il rilascio intenzionale di informazioni errate o volutamente ambigue mentre il secondo si configura come la tendenza a cambiare il proprio comportamento qualora si sia consapevoli di essere osservati. Briki e Waqas, una volta che le immagini postate sono diventate virali, hanno infatti chiuso i propri account e hanno limitato al minimo le interazioni social. Una volta valutata la presenza di tali fenomeni l'informazione filtrata e isolata si arricchisce di livelli di confidenza che possono essere supportati da ulteriori verifiche tramite la triangolazione con altre fonti.

L'ultimo step, quello della disseminazione, deve essere pensato sicuramente in termini di condivisione dell'informazione estrapolata tra i canali di intelligence strutturati, ma eventualmente anche con il pubblico social.

6. Conclusione

Con diversi gradi di impiego e di penetrazione, la SOCial Media INTelligence (SOCMINT) viene utilizzata dai servizi di intelligence internazionali per raccogliere dati rilevanti al fine di fornire informazioni aggiuntive circa determinate minacce. Nel dibattito internazionale intorno a questo metodo di raccolta e interpretazione di dati provenienti dal web 2.0 sono chiare alcune posizioni fondamentali per riuscire progressivamente ad attestare questa che al momento è quasi unicamente una pratica applicata come una disciplina vera e propria cioè corredata non solo da obiettivi e mezzi ma anche e soprattutto da una riflessione metodologica.

Innanzitutto, è chiaro che la SOCMINT, e di conseguenza coloro che se ne occupano, non hanno alcuna pretesa che questa possa essere la nuova, migliore e sostitutiva modalità di acquisizione dati di tutte le diverse sfaccettature del ciclo di intelligence. Tuttavia, è innegabile che l'evoluzione

delle modalità di comunicazione del terrorismo impongono ai servizi di intelligence di dotarsi di strumenti e competenze capaci di confrontarsi con questo fenomeno. Da questo punto di vista, le difficoltà maggiori riscontrare si riassumono in una "resistenza" generalizzata ad integrare questa tecnica alle altre, resistenza che è resa evidente dalla richiesta, da parte dei membri dell'intelligence stessa, di prove circa la sua efficacia. Come tutte le altre tecniche che compongono il ciclo di intelligence la SOCMINT è solo un ulteriore modalità di raccogliere dati che possano produrre informazioni che nello specifico, essendo prevalentemente presenti e diffuse online, sarebbero altrimenti difficilmente raggiungibili.

In secondo luogo, argomento spesso dibattuto sono le modalità con cui essa viene applicata. La SOCMINT, mutuata nell'ambito della sicurezza da quello del business, è da subito stata concepita come uno strumento di monitoraggio. Nata per verificare il posizionamento dei brand commerciali e fornire dati per la sentiment analysis, la SOCMINT si è concentrata sui processi di *data mining* rivolti a due principali aspetti degli ambienti "social": i contenuti e le relazioni. I primi hanno dato origine a diversi studi sui cosiddetti motori semantici utili nell'analizzare e filtrare grandi stringhe di dati come sono quelle delle comunicazioni che "scorrono" sui social, i secondi si concentrano maggiormente sulle relazioni virtuali che intercorrono tra i diversi user avvalendosi delle moderne tecniche di visualizzazione dei dati per darne una visione più ampia ed immediata. Evidentemente, tali visualizzazioni non esauriscono la ricchezza di informazioni e significato dei dati che rappresentano e dal punto di vista delle scienze sociali si rendono necessari dei sistemi di verifica di affidabilità ed efficienza di tali strumenti.

Tuttavia, l'ambito di utilizzo della SOCMINT non si limita ad un livello "passivo" di monitoraggio ma viene utilizzata anche in maniera proattiva per interagire con i diversi soggetti della rete. Esperienze internazionali, più o meno efficaci, dall'America all'Europa riferiscono di interventi svolti da personale qualificato nelle reti oggetto di monitoraggio.

È evidente che entrambe le modalità di applicazione della SOCMINT pongono problemi etici che vanno affrontati e ricondotti ad un approccio di gestione bi-direzionale: uno top-down, ossia garantito da norme e leggi, e uno parimenti fondamentale bottom-up che riguarda la formazione del personale addetto a tale ruolo.

Il dibattito è aperto, la pratica lanciata a livello internazionale, ora manca che si conduca la SOCMINT da un piano puramente "empirico", intendendo con il termine il fatto che la pratica è unicamente dettata dall'uso, ad un piano che maggiormente afferisca ad un disciplina sempre più formalizzata.

Le possibili linee di attività dunque si declinano nel reclutamento da parte dei servizi di intelligence di giovani nativi digitali che possano apportare

nuove prospettive di interpretazione ed analisi, nella definizione di un panorama legislativo preciso in materia, che contribuisca anche a far capire ed accettare all'opinione pubblica le attività che vengono intraprese, definendo ad esempio quali sono i limiti di intervento e la possibilità di utilizzare tecniche di investigazione speciali nei confronti si individui che ancora non sono considerabili sospetti; ed infine in un investimento nella formazione, che anche in questo ambito riveste un ruolo fondamentale, diretta sia all'interno degli stessi servizi di intelligence per colmare l'eventuale "gap generazionale" nell'approcciare la SOCMINT, sia ai governanti e legislatori perché si rendano conto in quale ambiente i servizi di intelligence si trovano ad operare.

References

[1] D. Omand, J. Bartlett & C. Miller (2012), *#Intelligence*, Demos

[2] *Omand, Sir David, Bartlett, Jamie, Miller, Carl, (2012).* 'Introducing Social Media Intelligence (SOCMINT), Intelligence and International Security

[2] Burato, A. (2015). *Social Media & Engaged Public: Possibilities and Responsibilities.* In: I. Apostol, J. Mamasakhlisi, D. Subotta, D.W.G. Reimer (eds) *Engaging the Public to Fight the Consequences of Terrorism and Disasters. NATO Science for Peace and Security Series*, IOS Press, pp 11-21

[4] Burato, A (2015). *Ebola: is it real? The role of communication, information, regulation and training in managing emergencies.* Sicurezza, Terrorismo e Società, 1, pp 83-98.

[5] A. Selamat, N.T. Nguyen, H. Haron (2013). *Intelligent Information and Database Systems*, 5th Asian Conference, ACIIDS 2013, Kuala Lumpur, Malaysia, March 18-20, 2013, Proceedings, Part I

[6] Bartlett, Jamie, Miller, Carl, Crump, Jeremy, Middleton, Lynne (2013). *Policing in an Information Age*, Demos, March 2013, [Online] Available at: <http://www.demos.co.uk/files/DEMOS_Policing_in_an_Information_Age_v1.pdf?1364295365> pp. 1-42, [accessed 2 September 2015]

[7] Cloke, P., Cook, I., Crang, P., Goodwin, M., Painter, J. and Philo, C. (2004) *Practising Human Geography*. London: Sage.

[8] Creswell, J.W. (2009) *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. 3rd eds. London: Sage.

[9] Bryden, J. and Funk, S. (2013) *'Word usage mirrors community structure in the online social network Twitter'*, Vol. 2, No. 3, 2013, [Online] Available at: <http://www.epjdatascience.com/content/2/1/3> [accessed 2 September 2015].

La Rivista semestrale *Sicurezza, Terrorismo e Società* intende la *Sicurezza* come una condizione che risulta dallo stabilizzarsi e dal mantenersi di misure proattive capaci di promuovere il benessere e la qualità della vita dei cittadini e la vitalità democratica delle istituzioni; affronta il fenomeno del *Terrorismo* come un processo complesso, di lungo periodo, che affonda le sue radici nelle dimensioni culturale, religiosa, politica ed economica che caratterizzano i sistemi sociali; propone alla *Società* – quella degli studiosi e degli operatori e quella ampia di cittadini e istituzioni – strumenti di comprensione, analisi e scenari di tali fenomeni e indirizzi di gestione delle crisi.

Sicurezza, Terrorismo e Società si avvale dei contributi di studiosi, policy maker, analisti, operatori della sicurezza e dei media interessati all'ambito della sicurezza, del terrorismo e del crisis management. Essa si rivolge a tutti coloro che operano in tali settori, volendo rappresentare un momento di confronto partecipativo e aperto al dibattito.

La rivista ospita contributi in più lingue, preferendo l'italiano e l'inglese, per ciascuno dei quali è pubblicato un Executive Summary in entrambe le lingue. La redazione sollecita particolarmente contributi interdisciplinari, commenti, analisi e ricerche attenti alle principali tendenze provenienti dal mondo delle pratiche.

Sicurezza, Terrorismo e Società è un semestrale che pubblica 2 numeri all'anno. Oltre ai due numeri programmati possono essere previsti e pubblicati numeri speciali.

EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.72342235 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione) - librario.dsu@educatt.it (distribuzione)
redazione: redazione@itstime.it
web: www.sicurezzaterrorismosocieta.it
ISBN: 978-88-6780-958-5

Euro 20,00