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

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

Executive Summary

The evolution of the ISIS' language: a quantitative analysis of the language of the first year of Dabiq magazine – Matteo Vergani, Ana-Maria Bliuc

In questo articolo indaghiamo l'evoluzione dell'ISIS attraverso l'analisi del testo contenuto nella rivista ufficiale del gruppo in lingua inglese, Dabiq. Più specificamente utilizziamo il software di analisi del testo LIWC (nella sua più recente versione del 2015) per indagare l'evoluzione del linguaggio dell'ISIS nel corso dei primi 11 numeri della rivista Dabiq. La nostra analisi mostra interessanti risultati: in primo luogo, il senso di affiliazione sembra essere l'aspetto psicologico più importante per l'ISIS nel corso del tempo. Questo mostra come l'ISIS sia in difficoltà in particolare nel distinguersi da altri gruppi jihadisti con una ideologia molto simile e operanti nello stesso territorio, come al-Qaeda e il fronte al-Nusra. In secondo luogo, l'ISIS negli ultimi numeri ha utilizzato un linguaggio sempre più emotivo, e come sappiamo le emozioni svolgono un ruolo importante nello spiegare perché le persone si mobilitano per una causa. Questo suggerisce che l'ISIS sta cercando di attrarre nuove reclute utilizzando un linguaggio volto a mobilitare emotivamente i lettori, a differenza del periodo precedente in cui il gruppo ha cercato di utilizzare un linguaggio più istituzionalizzato probabilmente volto più a legittimarsi come fonte di autorità religiosa e politica. In terzo luogo, il linguaggio dell'ISIS mostra una crescente attenzione al genere femminile: questo non stupisce poiché l'ISIS è il gruppo jihadista che nella storia ha attratto il maggior numero di reclute di genere femminile. Questo dimostra come il progetto dell'ISIS sia non solo creare un esercito ma anche e soprattutto creare e consolidare uno stato in cui i cittadini possano vivere una vita "normale", avere una famiglia e creare una nuova società. Questo carattere utopistico è un'altra importante caratteristica che rende l'ISIS diverso da altri gruppi jihadisti. Infine, Infine le nostre analisi rivelano che l'ISIS è molto abile nell'adattarsi a nuove forme di linguaggio: ciò è dimostrato dal crescente uso di gergo proprio dell'ambiente online ("Net Speak"). Questa capacità mostra come l'ISIS sia particolarmente abile nell'aprire un dialogo

con individui di giovane età, come dimostrato dai complotti terroristici in cui erano coinvolti adolescenti occidentali di addirittura 14 anni. Riteniamo che le analisi del linguaggio di ISIS che presentiamo in questo articolo sia particolarmente interessante poiché svela aspetti psicologici del gruppo che sono spesso trascurati da analisi condotte con altri metodi.

Suicide Attacks: Strategy, from the Afghan War to Syraq and Mediterranean region. A triple way to read the asymmetric threats – Claudio Bertolotti, Andrea Beccaro

Suicide-attacks are one of the most important aspects of modern conflicts. They have played and continue to play a key role in wars like those in Afghanistan and in Iraq where suicide attack had a big impact during the Iraq war, and they represent a key tactics of Islamic State warfare. The aim of this article is the analysis of the problem of suicide-attacks viewed from two different angle. On the one hand the study of the phenomenon inside the debate of the transformation of war and hence highlighting how the new strategic environment (transformation of war debate; RMA; urbanization of conflicts) helps the evolution and effectiveness of the suicide-attacks. On the other hand the focus on the Afghan theatre of war and, thanks to a new database, the analysis of the data with a triple way reading (strategic level; operational level; tactical level) of the suicide-attacks will help to understand the suicide-attack phenomenon in the battlefield.

Gli attacchi suicidi sono uno degli aspetti più importanti dei conflitti moderni. Essi hanno svolto e continuano a svolgere un ruolo chiave in guerre come quelle in Afghanistan e in Iraq, dove gli attacchi suicidi hanno avuto un grande impatto durante il conflitto con gli Stati Uniti e rappresentano una tattica chiave della guerra dello Stato islamico. Lo scopo di questo articolo è analizzare il problema degli attacchi suicidi visto da due diverse angolazioni. Da un lato lo studio del fenomeno all'interno della discussione della trasformazione della guerra e, quindi, evidenziando come il nuovo contesto strategico (trasformazione della guerra; RMA; urbanizzazione di conflitti) aiuti l'evoluzione e l'efficacia degli stessi attacchi suicidi. D'altra parte l'attenzione al teatro di guerra afgano e, grazie a un nuovo database, l'analisi dei dati con una nuova e originale tripla lettura (livello strategico, piano operativo, livello tattico) degli attacchi suicidi che aiuterà a capire il fenomeno sul campo di battaglia.

Intelligence economica: una proposta per l'Italia – Laris Gaiser

In the wake of political upheavals at the end of the 20th century, national communities began living in an international setting that was considerably different from the traditional world order following the Second World War. The period marked by global bipolar competition was one of geopolitical stability and clear military alliances with countries having rather limited margins activity and economic freedom. Today, we are facing a situation of a new type of anarchy and the stability of the old political alliances has been undermined. The fluidity of international relations has forced countries to tackle global competition in such a way as to achieve the best possible outcome in terms of profits, development and wealth.

The role of the state, which had been for years under criticism, was to be minimized. Due to the pressure of liberal thinking, this objective had gained considerable importance. States, once again, had become active economic players, whose role it was to act as catalysts and push through reform strategies that would enable countries to maintain their competitiveness. Because of the geo-economic war, governments are required to become guarantors of social stability. This role needs to be based on a strategic vision which fosters economic growth and development through economic intelligence. This category in the field of economic geopolitics is new only in the nominal sense. Economic intelligence dictates that there be cooperation between the public and private sectors. The need for which may have been felt in the past, but implementation was only on a comparably minor scale.

Economic intelligence structures are a mere means of effective cooperation between the public and private sectors at a specific time in history, in which the two sectors would be seriously endangered if they failed to act together. Thus, the world of business maintains its vigour and vitality and the state is bestowed a mission that legitimises it. In order to survive inside a very challenging environment the State has to rethink itself. It becomes a "strategic state" with the final goal of fostering its competitiveness creating a stable economic intelligence system.

Economic intelligence could be defined as a discipline studying information needed by companies and states to make the right development decisions with the aim of fine-tuning their cognitive and decision-making capacities in the complex context of global competition

Economic intelligence consists of gathering and processing information relevant to the economic sector with the aim of making operational choices. It consists of activities aimed at obtaining information, surveillance of competitors, protection of strategic information and capitalising on this knowledge in order to influence, determine and control the global economic environment.

It is a power tool to be used by countries, in which the private and the public sphere are intertwined and communicating.

The Republic of Venice is taken as clear example of above mentioned capabilities. It serves as a mirror to better understand the ongoing transformations and to propose a solution for Italy where the Parliament in 2007 reformed the old Secret Service Act of 1977 paving the way for future development of economic intelligence. According to the current Constitution economic intelligence in Italy should enjoy full legitimation. The proposal consist of a reform that could take in account the already existing state system upgrading the constitutional and governmental bodies' with new functions in order to shape an efficient private-public intelligence cooperation.

Sulla scia degli sconvolgimenti geopolitici della fine del XX secolo, le comunità nazionali hanno incominciato a vivere in un contesto internazionale notevolmente diverso da quello scaturito in seguito alla Seconda Guerra Mondiale. Il periodo segnato dal bipolarismo era caratterizzato dalla stabilità geopolitica e da chiare alleanze militari all'interno delle quali i vari paesi avevano margini piuttosto limitati di autonomia e di libertà economica. Oggi siamo costretti a confrontarci con un nuovo tipo di anarchia globale in cui la stabilità delle vecchie alleanze politiche è minata e la fluidità delle relazioni internazionali costringe i paesi ad affrontare la concorrenza globale in modo da ottenere il miglior risultato possibile in termini di profitti, di sviluppo e di ricchezza.

Il ruolo dello stato ridotto quasi al minimo negli ultimi decenni sotto le pesanti critiche di gran parte del pensiero liberale si ripropone al centro della scena internazionale in seguito ai grandi cambiamenti geopolitici dei quali siamo testimoni. Esso ridiviene un soggetto economico attivo con il compito di catalizzare le esigenze del settore produttivo nazionale. Lo stato è costretto a riformare se stesso in modo da mantenere la propria competitività e a causa della guerra geoeconomica, i governi sono tenuti a diventare garanti della stabilità sociale. Questo ruolo deve essere basato su una visione strategica che favorisce la crescita e lo sviluppo attraverso l'*intelligence* economica. Essa è una branchia della geopolitica economica, nuova solamente dal punto di vista nominale, che impone la cooperazione tra il settore pubblico e quello privato. L'*intelligence* economica, seppur in forme diverse, già esisteva in passato ma trova oggi le condizioni necessarie per il suo sviluppo completo.

Le strutture d'*intelligence* economica sono un metodo efficacie di collaborazione tra settore pubblico e privato in un momento storico nel quale sarebbero entrambi seriamente minacciati qualora non agissero all'unisono. In tal modo il settore economico si garantisce lo sviluppo e lo stato ritrova una missione che lo legittima nuovamente. Lo stato ripensa se stesso all'interno di un mondo in continua evoluzione. Esso diventa uno "stato strategico" avente come obiettivo

finale quello di favorire la competitività del proprio sistema economico attraverso la creazione di una stabile *intelligence* economica che può definirsi come la disciplina che, studiando il ciclo dell'informazione necessario alle imprese e agli stati per effettuare scelte corrette di sviluppo, si prefigge di affinare le abilità cognitive e decisionali applicate alle complessità del contesto competitivo globale.

L'*intelligence* economica consiste nella raccolta e nell'elaborazione di tutte quelle informazioni che possono essere rilevanti per il settore economico e sulla base delle quali si possono effettuare delle scelte operative ponderate. Si compone di attività dirette a ottenere informazioni, sorvegliare i concorrenti, proteggere le informazioni strategiche e capitalizzare le conoscenze al fine di influenzare, determinare e controllare l'ambiente economico globale. Si tratta di uno strumento di potere a disposizione dei paesi in cui la sfera pubblica e quella privata comunicano e si coordinano. La Repubblica di Venezia, dove l'interesse di stato era strettamente legato all'interesse commerciale, è presa come chiaro esempio di tali capacità e serve come cartina di tornasole per meglio comprendere le trasformazioni in atto in Italia dove il Parlamento ha nel 2007 finalmente cambiato la vecchia legge sui servizi segreti aprendo la strada al possibile, futuro, sviluppo della disciplina dell'*intelligence* economica nazionale. Secondo l'interpretazione proposta essa è conforme alla Costituzione della Repubblica e pertanto pienamente legittima. Se l'Italia desidera rimanere competitiva sul mercato globale, dove continuare la trasformazione intrapresa prendendo in considerazione il sistema costituzionale e di governo già esistente e affidandogli nuove funzioni che possano plasmare un'efficiente cooperazione tra i vari attori del settore economico garantendo un costante flusso informativo.

Islamic extremism from the Balkans emerges in Italy – Giovanni Giacalone

Between 2014 and 2015 several counter-terror operations were conducted between Italy, Albania and Bosnia-Herzegovina; operations which led to the expulsion or arrest of jihadist recruiters, indoctrinators and potential volunteers.

Operations such as "Damascus", "Balkan Connection" and "Martese" exposed the presence of jihadist cells in Tuscany, Lombardy and the North-East of Italy, all areas of interest for Islamists from the Balkans, with several Islamic centers involved in organizing visits of radical preachers.

Over all, operation "Martese" attracted the attention of the Italian media as it became the first case of a whole Italian family which became radicalized and was ready to depart and seek a new life in the so-called "Islamic State". A radicalization that was facilitated by an Albanian network linked to Genci

Balla and Bujar Hysa, two Albanian preachers currently in jail in Tirana while on trial for jihadist propaganda and recruitment.

In this short article I will explore some of the Italian-Balkanic contacts and links that were activated by the jihadists in order to provide Isis with volunteers, focusing in particular on the Albanian networks.

Tra il 2014 e il 2015 diverse operazioni anti-terrorismo sono scattate tra Italia, Albania e Bosnia-Erzegovina; operazioni che hanno portato all'espulsione o all'arresto di reclutatori, propagandisti e potenziali volontari per la jihad.

Operazioni come "Damasco", "Balkan Connection" e "Martese" hanno messo in evidenza la presenza di cellule jihadiste in Toscana, Lombardia e nel nord-est d'Italia, tutte zone di interesse per gli islamisti dei Balcani e con diversi centri islamici coinvolti nell'organizzazione di visite da parte di imam radicali.

L'operazione "Martese" ha particolarmente attirato l'attenzione dei media italiani in quanto ha visto coinvolto il primo nucleo familiare radicalizzatosi e pronto a partire per cercare una nuova vita nel cosiddetto "Stato Islamico". Una radicalizzazione facilitata da una rete albanese legata a Genci Balla e Bujar Hysa, due predicatori estremisti attualmente in carcere a Tirana e sotto processo con l'accusa di propaganda e reclutamento per la jihad.

In questo breve articolo esplorerò alcuni contatti e collegamenti italo-balcanici attivati dai jihadisti per trovare volontari per l'Isis, focalizzandomi in particolare sulle reti albanesi.

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

L'utilizzo dei social media come strumento per monitorare gli aspetti più disparati è stato impiegato sin dalla loro comparsa sul panorama mondiale. Quando questa indagine migra dalla molteplicità di temi dei quali si può occupare per dirigersi verso un utilizzo puntuale in materia di sicurezza prende il nome di SOCMINT ossia SOCial Media INTelligence. Ambito di indagine sicuramente non nuovissimo ma di recente teorizzazione, la SOCMINT cerca ancora uno spazio all'interno del dibattito accademico per la sua collocazione nel più ampio spettro delle declinazioni dei processi di intelligence. Tuttavia, dal punto di vista operativo, l'utilizzo del monitoraggio a fini preventivi e investigativi del materiale o delle comunicazioni scambiate sui social network ha già portato a notevoli risultati nella lotta al terrorismo.

L'attenzione dell'opinione pubblica alla funzione di divulgazione della cultura del terrore tramite questi mezzi di comunicazione è scoppiata con la diffusione della propaganda del sedicente Stato Islamico. Un uso massivo del-

le piattaforme social contraddistingue sempre più la modalità pervasiva della pubblicazione virale di materiale propagandistico e didattico pubblicato da IS, attraverso il quale si cercano di reclutare nuovi mujaheddin che possano ingrossare le fila del combattenti per il Jihad. Come per l'utilizzo dei social in casi di emergenze naturali, i fruitori di questi mezzi diventano allo stesso tempo produttori di informazioni, in questo caso inneggiando alla "guerra santa" o contribuendo a far diventare virale la propaganda prodotta da IS.

"Un avido utilizzatore di Social Media", "Davvero attivo sui Social Media". Potrebbe sembrare la descrizione davvero di chiunque, non solo di un teenager ma anche di uomini e donne non nativi digitali che affollano costantemente i social. E invece è quanto è stato riportato da tutte le testate come tratto distintivo di Seifeddine Rezgui, nome de guerre Abu Yahya al-Qayrawani, 24 anni e un diploma di una scuola tecnica e futuro ingegnere, che durante il Black Friday (26 giugno 2015) ha ucciso a sangue freddo 38 persone sulla spiaggia di un resort a Susa, Tunisia. A qualche giorno dall'evento si è subito fatto riferimento ad un profilo Facebook riconducibile all'attentatore dove, mischiati tra post inneggianti il Real Madrid o i rapper più in voga, ce ne sarebbero stati diversi che inneggiano le bandiere nere del sedicente Stato Islamico: "Mio Dio sollevami da questo mondo ingiusto, fai che queste genti soffrano e muoiano, perché solo quando moriranno si ricorderanno di te", "Se l'amore per il jihad è un crimine, tutti possono testimoniare che io sono un criminale", e ancora "gli eroi sono nelle loro tombe, le persone reali in prigione e i traditori nel palazzo".

Sebbene, come per le stragi di Charlie Hebdo e del supermercato kosher, il responsabile della strage fosse in qualche modo noto alle forze dell'ordine, nessuna azione preventiva è stata messa in campo per evitare che un ragazzo, segnalato alle autorità anche se forse non per fatti strettamente legati al terrorismo, venisse fermato prima di colpire.

In questo articolo verrà invece analizzato, alla luce della letteratura disponibile sull'utilizzo della SOCMINT, il caso dell'arresto dei due individui, il tunisino Lassaad Briki e il pakistano Muhammad Waqas, responsabili della diffusione delle immagini di minaccia a luoghi sensibili di Milano/Roma, noto all'opinione pubblica come il caso dei "pizzini" dell'ISIS, che intendevano compiere un attentato in territorio italiano dopo essersi addestrati nei campi siriani.

The use of Social Media as an instrument useful to monitor the variety of the aspects of people's lives is acknowledged since their first appearance. But when this activity moves from the multiplicity of the issues it can take into account to focus on a more punctual use in terms of security it is known with the term SOCMINT, that is Social Media Intelligence. As it is not a new domain but it has just been theorized, SOCMINT is still looking for a space within the academic debate on its position and role in the wide spectrum of intelligence

processes. However, from an operative point of view, the preventive and investigative monitoring of the material and all the communications exchanged on the social network has already brought to relevant successes to fight terrorism.

The interest of the public opinion for the role of social media as a medium of terror has began with the spread of the so-called Islamic State propaganda. The pervasive publication of propagandistic and didactic materials is always more marked by the massive use of social platforms, through which terrorists are looking for new mujahidin to hire so that they can enlarge the number of people fighting for the Jihad. As for the use of social media in case of natural disasters, users are at the same time information producers by exalting the "holy war" or contributing to share IS propaganda. "An avid social media user", "really active on social media". This could really be the description of anyone, not only of a teenager but also of men and women not digital-born that use social media. Rather, it is the what have been reported by all journals as a distinctive trait of Seifeddine Rezgui, nome de guerre Abu Yahya al-Qayarawani, 24 years old, a degree from a technical school and a future engineer, that during the Black Friday (26th of June, 2015) killed 38 people on the beach of a resort in Susa, Tunisia. In the aftermath the press immediately referred of a Facebook profile, ascribable to the killer, on which, among comments supporting Real Madrid team or the most popular rappers, there were others supporting IS black flag: "May God take me out of this unjust world and perish its people and make them suffer. They just remember you when you die", "If the love of jihad is a crime, everyone can testify that I am a criminal", and more "The heroes are in their graves, real men in prisons, and traitors in the palace."

Although the killer was somehow known to the police, as happened for the Charlie Hebdo and the kosher supermarket massacres, no preventive actions were taken.

This article focuses on the arrest of two suspects, the Tunisian Lassaad Briki and the Pakistani Muhammad Waqas, responsible for the diffusion of picture of threating messages to sensitive places in Milan and Rome, known to the public opinion of the "pizzini" case, who intended to plan for an attack in Italy after being trained in Syria.

How cyberspace is used by terrorist organization: possible threats to critical infrastructures? The most recent activities of cyber counterterrorism – Mauro Pastorello

Il dominio del cyberspace è sempre stato considerato come il futuro per le azioni di attacco e spionaggio militari, ma per molti anni un suo potenziale

utilizzo in modo significativo, sia per scopi offensivi che difensivi, era visto come un miraggio tecnologico, la cui reale utilizzazione non si sarebbe mai avuta. Possiamo dire con certezza che mai come negli ultimi anni, questo miraggio si è trasformato in realtà, con tutti i suoi lati positivi e negativi.

L' analisi proposta nel mio articolo si focalizzerà sullo studio del cyberspace e del suo utilizzo come strumento e veicolo per lanciare degli attacchi con le nuove **cyber weapons**, ovvero tutte quelle "armi" che possono non causare vittime, in termini di perdita di vite umane, ma che possono distruggere e mettere in ginocchio l'economia di un intero Paese o di una società, prese mi mira da hacker o cracker che possono agire da soli, per conto di associazioni o gruppi, o addirittura per altri Paesi e lanciare quindi dei veri e propri attacchi cibernetici con il loro avallo, nel silenzio della società civile.

A livello metodologico, il cyberspace e i relativi domini, saranno analizzati secondo la teoria di Clark, mettendo in luce come la convergenza fisicologica delle infrastrutture ha ormai reso obsolete le classificazioni che si limitavano a indicare se un'infrastruttura fosse fisica *strictu sensu* o logica e come questa convergenza rende ancora più importante e necessario un approfondimento sul tema, dato che molti dei nostri dati personali o altre informazioni si trovano in rete, esposte alle vulnerabilità e minacce di questa nuova dimensione e quindi fortemente a rischio; successivamente verranno forniti alcuni esempi pratici di recenti attacchi cyber e delle loro possibili conseguenze. In ultimo, sarà analizzata la minaccia terroristica nel cyberspace, il cosiddetto **cyberterrorism**, che Barry Collin definisce come: "*the convergence of physical and virtual worlds where cyber weapons produce physical consequences*".

L'attacco Stuxnet, lanciato contro una centrale nucleare in Iran, e quello recentissimo lanciato contro la società italiana Hacking Team, produttrice di software per intercettazione dati, hanno fatto rivalutare il problema e portano ad elaborare nuove considerazioni, come ad esempio l'aumento massiccio dell'automazione e del controllo di apparati industriali completamente gestiti da remoto attraverso il cyberspace. A questa situazione si aggiunge anche il cambiamento di vita sociale che ha segnato gli ultimi anni, con l'esigenza sempre più forte di ciascuno di noi ad essere connesso nel cyberspace 24 ore su 24, per l'utilizzo di social network, la visualizzazione di mail da smartphone, l'attivazione da remoto del teleriscaldamento in casa e tantissimi altri servizi gestibili in "rete".

Tutto ciò ha fatto sì che diversi Paesi hanno focalizzato la loro attenzione sul cyber world, analizzando nel dettaglio il tipo di utilizzo che ne fanno le strutture Governative, aziendali ed economiche dei rispettivi sistemi Paese, migliorando la legislazione in ambito di cyber security e nella protezione delle infrastrutture critiche, possibili obiettivi delle "cyber weapons".

Per quanto riguarda il nostro Paese, l'Italia, la sicurezza delle infrastrutture critiche e, più in generale, la sicurezza cibernetica, sono gestite dalle Agenzie di intelligence (AISI, Agenzia Informazioni e Sicurezza Interna, e AISE, Agenzia Informazioni e Sicurezza Esterna) coordinate dal DIS (Dipartimento Informazioni e Sicurezza), insieme al CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche) formato dalla Polizia Postale e delle Comunicazioni e dal UACI (Unità Anti Crimine Informatico).

L'obbiettivo finale di questo articolo è di evidenziare che vi sono delle precise strategie di attacco e difesa nel mondo cyber, basti pensare alla recente formazione della Cyber Brigate nell'Esercito di sua Maestà in Gran Bretagna, che ha il compito di gestire attacchi e difesa cibernetica, o ad un'altra divisione da poco venutasi a creare, la Hacking Division dello Stato Islamico, e che per far fronte a questo nuovo "dominio" militare è assolutamente necessaria una rilettura e rivalutazione delle strategie si difesa dei vari Paesi e condividere quanto più informazioni possibili, cosi da migliorare la risposta ad un eventuale attacco che, per la natura stessa del "terreno" sfruttato (il cyberspace) potrebbe avere delle ripercussioni non solo nel Paese oggetto dell'attacco, ma anche il tutti gli altri Paesi o sistemi, a causa delle interdipendenze del mondo cyber.

A Case Study Analysis of the Implementation of GIS Technology for Safety and Security Planning during Major Sport Events – Giovanni Pisapia

Over the past decade there has been a substantial international body of research focused on various aspects of security planning during major sport events (inter alia Klauser 2008, Boyle and Haggerty 2009, Bennet and Haggerty 2011, Fussey et al. 2011, Pisapia and Fonio 2011, Fussey et al. 2012). More specifically, there has been research focused on utilizing Geographical Information System (GIS) technology for safety, security and emergency management purposes (inter alia Greene 2004, Kataoka 2007, Radke and Hanebuth 2008).

This article describes the overall benefits of implementing Geographic Information System (GIS) technology for drafting, managing, and monitoring successful safety and security operational plans for major sport events. GIS has been utilized for planning various major sport events with encouraging results (Field, 2012). How GIS technology has been applied thus far in this sector is illustrated through this article with detailed, first-hand knowledge of the best practices and key lessons learned from three major sport events:

2010 FIFA World Cup in Johannesburg, South Africa – XX Commonwealth Games 2014 in Glasgow, Scotland – 1st European Games 2015 in Baku, Azerbaijan. The 2012 Olympic Games in London, England, is discussed as well.

As these three case studies illustrate, GIS technology allows the integration of spatial information into a single, holistic picture, whereby a dynamic, common operating picture is created to enable everyone to see the same information and deploy resources accordingly (Kataoka, 2007).

The examples from Johannesburg, Glasgow, and Baku highlight how critical maps are for major sport events as they provide an invaluable context to decision-making. Major risks from not utilizing GIS technology for such large-scale projects include, but are not limited to:

- Silo approach: disjointed plans with inaccurate spatial data between internal role-players and external stakeholders, in particular outside the venue boundaries. This could affect both planning stage (e.g. failure to assess the interaction of event activities with the city day to day movements) and event time (e.g. difficulty in coordinating emergency operations)
- Not-envisaged mapping costs: additional non/envisaged mapping-related tasks rise as the planning progresses. The costs to effectively carry them out by outsourcing them could be costly for the OC
- Copyrights breach: possible civil penalties and reputational damage arising from inadvertent license breach by OC staff using online maps for business purposes without authorization
- Un-scoped mapping tasks: as the event approaches, external stakeholders request OC to provide updated and detailed event maps outside the venue boundaries (e.g. event client groups' movements), which are not available
- Internal and external unfulfilled expectations: general expectation, from both internal functional areas and partner agencies, that some of the maps will be produced by the OC through GIS technology closer to the event

While this article focuses on the use of the GIS technology for safety and security purposes, an all-encompassed use of the technology for the entire event's planning activities could lead to identifiable downstream cost and time savings, as well as reducing exposure to risks arising from errors in the planning process from data latency. In addition, expanding the usage of the software can strengthen the level of cooperation and collaboration between internal role-players and external partners.

An area, which requires further attention and consideration, is the post-games legacy use of GIS. There are tangible benefits, including newly developed or enhanced spatial databases, as well as intangible benefits, such as enhanced cooperation and networking between local and national government departments. It is therefore recommended that future use of GIS should parallel the holistic vision of the host city, and most opportunely, if

possible, for crime-prevention (i.e. crime mapping, crime analysis) and disaster management. GIS for major sport events can establishment significant lasting legacies for the resident population if coordinated with the host city effectively from its inception.

Negli ultimi dieci anni, è stato pubblicato un numero consistente di articoli sui vari aspetti della pianificazione della sicurezza in occasione di eventi sportivi di rilievo (tra l'altro Klauser 2008, Boyle e Haggerty 2009, Bennet e Haggerty 2011, Fussey et al. 2011, Pisapia e Fonio 2011, Fussey et al. 2012). Inoltre, la ricerca si è anche focalizzata sull'utilizzo del Geographical Information System (GIS) per la pianificazione di operazioni di sicurezza e di gestione delle emergenze (tra l'altro Greene 2004, Kataoka 2007, Radke e Hanebuth 2008).

Questo articolo descrive i benefici dell'utilizzo della tecnologia Geographic Information System (GIS) per la sviluppo, gestione e monitoraggio dei piani operativi di sicurezza per eventi sportivi di rilievo. GIS è già stato utilizzato per la pianificazione di vari grandi eventi con risultati incoraggianti, come ad esempio i Giochi Olimpici di Londra 2012 (Field, 2012). L'utilizzo del GIS in questo settore è illustrato, nell'articolo, attraverso una dettagliata descrizione dei principali insegnamenti e prassi tratti dall'utilizzo della tecnologia durante tre grandi eventi sportivi: Coppa del Mondo FIFA 2010 a Johannesburg, Sud Africa – XX Giochi del Commonwealth 2014 a Glasgow, Scozia – 1 ° Giochi Europei 2015 a Baku, Azerbaijan.

Come questi tre casi dimostrano, la tecnologia GIS consente di integrare informazioni geo-referenziali in un'unica piattaforma, dalla quale si ricava un quadro operativo comune per permettere la condivisione di informazioni e supportare il processo decisionale tra i diversi enti preposti all'organizzazione di grandi eventi (Kataoka, 2007).

Gli esempi provenienti da Johannesburg, Glasgow e Baku evidenziano come la produzione di mappe accurate siano un elemento critico per la pianificazione della sicurezza per eventi sportivi di rilievo, in quanto forniscono il quadro per un effettivo processo decisionale da parte degli enti coinvolti. L'articolo, inoltre, descrive i principali rischi derivanti dal non-utilizzo della tecnologia, tra cui:

- Piani operativi scollegati, con dati geo-referenziali imprecisi, tra i vari operatori, in particolare al di fuori dei confini dei siti
- Costi per la produzione di mappe non previsti durante la pianificazione iniziale, che potrebbe risultare in un aumento delle spese previste del Comitato Organizzatore a ridosso dell'evento

- Possibili violazione di copyright ed eventuali sanzioni civili e danni reputazionali derivanti dall'improprio utilizzo di mappe disponibili online, da parte del personale del Comitato Organizzatore, per scopi commerciali
- Aspettative disattese relative all'utilizzo di mappe per l'evento da parte di operatori locali, nazionali ed internazionali (ad esempio Comitati Olimpici Nazionali)

Questi rischi possono influenzare negativamente durante sia la fase di progettazione (ad esempio la mancata interazione ed influenza reciproca tra le varie attività operative) che di messa in atto dei piani di sicurezza (ad esempio, la difficoltà di coordinare le operazioni di emergenza tra le varie istituzioni) per l'evento.

Mentre questo articolo si concentra sull'uso del GIS per la pianificazione di sicurezza, un uso della tecnologia più ampio per l'intera pianificazione di grandi eventi conduce a rilevanti benefici grazie all'utilizzo di accurati ed esclusivi dati geo-referenziali da parte di diversi enti. L'utilizzo del software rafforza in questo modo la cooperazione e collaborazione tra la varie parti interessate.

Una area che richiederebbe ulteriore attenzione e considerazione è il lascito post-evento della tecnologia. L'esperienza insegna che esistono molteplici benefici relativi all'uso del GIS per la pianificazione della sicurezza di grandi eventi; ad esempio la creazione di banche dati geografiche o la maggiore cooperazione tra vari enti locali e nazionali predisposti all'organizzazione dell'evento. L'uso del GIS potrebbe essere utilizzato anche per altri progetti relativi alla sicurezza e prevenzione del crimine all'interno della città ospitante, quali la mappatura ed analisi della criminalità e la gestione delle emergenze, per conferire una visione d'insieme per una pianficazione effettiva ed efficace della sicurezza prima, durante e dopo l'evento.

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