Le interviste

Proteggere una città nella città: sicurezza urbana o infrastruttura strategica?

Intervista a

Marco Pera,
Physical & Travel Security Manager di un primario polo fieristico

Fiera =
infrastruttura strategica ma critica per le ripercussioni che potrebbe presentare un evento infausto in un immenso contenitore di persone e asset

Partiamo dalle definizioni. Una fiera è un'infrastruttura critica?

Un quartiere fieristico si colloca a mezza via tra le infrastrutture critiche e le infrastrutture strategiche. Quelle *critiche* sono indispensabili per il funzionamento del sistema paese (utility, trasporti, sanità, catena alimentare etc), mentre quelle *strategiche* sono funzionali alla crescita economica del paese in un contesto sociale non critico. Se dunque la fiera si inquadra come infrastruttura strategica nella sua funzione di volàno per l'economia e il territorio, lato protezione va però assimilata ad un'infrastruttura critica per le ripercussioni a cascata che potrebbe presentare un evento infausto in un immenso contenitore di persone (lavoratori, espositori e visitatori) e di asset materiali e immateriali. Tenga presente che durante le manifestazioni i quartieri fieristici diventano dei microcosmi brulicanti di vita: vere città che nascono e muoiono con l'evento e che esigono una forma di tutela assimilabile alla sicurezza urbana, da gestirsi dunque in modo integrato tra le forze di sicurezza pubblica (che garantisce l'ordine pubblico e interviene in caso di emergenza) e la security privata, tecnologica e dei servizi, cui è affidata la gestione degli accessi e la tutela delle strutture e delle merci.

Durante le manifestazioni i quartieri fieristici diventano microcosmi brulicanti di vita: città nelle città che nascono e muoiono con l'evento e che esigono una forma di tutela assimilabile alla sicurezza urbana

Le fiere contengono le merci più diverse (incluse merci "vive" come piante o cibo, che potrebbero anche essere oggetto di contaminazione): in che modo si declina un progetto di sicurezza fisica in un contesto così multiforme?

Ogni manifestazione presenta peculiarità e specificità che richiedono un'analisi del rischio ad hoc. E' pur vero che un calendario consolidato di eventi consente di affrontare le criticità di fondo con un certo grado di preparazione, ma ogni piano di sicurezza va rivalutato sulla base del momento storico e delle specificità merceologiche (che possono attirare l'attenzione di dimostrazioni politiche o ideologiche, si pensi solo alla distribuzione di gas o più banalmente al pellame). E' comunque un lavoro in team: in caso di tensioni geopolitiche la funzione di security opera di concerto con l'intelligence manager; quando si espongono piante, alimenti o animali si lavora in accordo con ATS e NAS per controllare le merci e in generale si lavora in sinergia con le FFOO.

Il suo background di Carabiniere, e poi di Dirigente di Polizia Locale a Milano e infine di Comandante a Nembro (epicentro del Covid) nel disgraziato 2020, le è di ausilio nella funzione di security manager aziendale?

Se si lavora con la sicurezza e si ha a che fare con le Forze dell'Ordine bisogna saper parlare la lingua della Pubblica Amministrazione, rispettarne logiche e gerarchie, conoscerne le dinamiche interne per indirizzarsi alle competenze più corrette per risolvere tempestivamente un problema in caso di emergenza. L'appartenenza ad entrambi i mondi aiuta nella sottile opera di mediazione tra finalità e necessità, dal momento che la security privata ha come obiettivo primario la business continuity, mentre le FFOO sono deputate al controllo, alla verifica e all'intervento.

Restando sul tema della mediazione: l'affare Croudstrike ha confermato l'intreccio sempre più pervasivo tra mondo IT, sicurezza fisica e qualunque forma di operatività. Che relazioni ha il dipartimento di sicurezza fisica con la sicurezza cyber? Ci sono gelosie o feudi, anche in materia di budget?

Le nuove minacce emergenti dal mondo cyber, l'ibridazione degli attacchi, le norme in arrivo in materia di sicurezza informatica, ma anche i rischi legati ad un banale aggiornamento IT come nel caso Crowdstrike, stanno spostando – più che legittimamente – gli investimenti sul fronte della sicurezza cyber rispetto a quella fisica. In un contesto fieristico si potrebbe definire un rapporto di budget 70/30 a favore della cyber security: del resto parliamo di due linee criminose con finalità e modalità espressive molto diverse. Il crimine informatico si traduce in un danno economico che porta un guadagno all'attaccante, mentre il crimine tradizionale presenta in genere natura dimostrativa o politica. Tra l'altro i controlli agli accessi fisici in un quartiere fieristico sono molto rigidi, sia per le persone che per i veicoli, e le misure sono assimilabili alla security aeroportuale (metal detector, road blocker, tornelli, esibizione di credenziali, guardie giurate). Invece l'attacco cyber è più semplice e meno rischioso, oltre ad essere più complesso da rilevare. Ciliegina sulla torta: la sua magnitudo è potenzialmente infinita ed è assai raro intercettare e sanzionare l'attaccante.

Un crimine redditizio che richiede delle competenze: con quali competenze rispondere? Il security manager dev'essere più preparato in compliance, tecnologie, management o che altro? Il percorso formativo imposto ai professionisti della sicurezza certificati (ex DM269/2010) sarebbe a suo avviso da estendere anche al security management aziendale?

Il ruolo è complesso e richiede un'ampia gamma di competenze che spaziano dall'analisi del rischio alle tecnologie, dalla compliance al management (risk, travel security management), per non menzionare i soft skill. Mentre i cyber security manager vantano da sempre una formazione specializzata, per molto tempo i security manager - anche in realtà blasonate – provenivano dai dipartimenti più disparati: logistica, operation, HR. Ben vengano quindi specializzazione, formazione e certificazione obbligatorie, magari con un percorso universitario in modalità 3+2 o a ciclo unico. Il percorso ex DM 269/2010 potrebbe essere conservato come base triennale de minimis, mentre i due anni di laurea magistrale potrebbero offrire una formazione specializzata in travel, risk, compliance, etc.

Concludiamo con la vigilanza privata e i servizi fiduciari: nonostante gli aumenti salariali, non si trovano candidati. E c'è chi vuole imporre una certificazione delle competenze degli operatori di sicurezza... che ne pensa?

Per un ente fieristico la vigilanza privata è una risorsa cruciale, e non solo in quanto primaria figura di sicurezza, ma anche come biglietto da visita dell'immagine aziendale. Rappresenta infatti la professionalità di security più visibile al pubblico e la sua sussidiarietà rispetto alle FFOO è ormai un elemento imprescindibile. Negli ultimi tempi ho rilevato un miglioramento nel grado di preparazione delle guardie giurate,ma resta ancora un lavoro poco appetibile, nonostante i recenti aumenti salariali (ai quali alcune committenze sono sensibili, comprendendo il valore della professionalità). Quanto alla certificazione delle competenze degli operatori fiduciari, sarebbe certamente un passo opportuno. Spesso però si tratta di servizi a chiamata, non di rado di manodopera che è solo *in transito* in Italia: temo dunque che imporre la certificazione del personale si scontrerebbe con un grosso ostacolo nella messa a terra.