Evidence-Based Design e strategie di Smart Force Protection Engineering: frontiere per antiterrorismo e Sicurezza Nazionale

di Giuseppe Lacanna[1]

Il primo dovere di un Governo è quello di proteggere la propria popolazione. La minaccia terroristica che attualmente affrontiamo è sfaccettata, diversificata e in continua evoluzione. La polizia, i servizi di sicurezza e di intelligence, e altri partner strategici fanno tutto il possibile per combattere questa minaccia, ma la realtà è che risulta molto difficile, se non impossibile, eliminare il rischio di ogni possibile attacco. Ciò che abbiamo visto in Francia, Regno Unito, Germania, Turchia, Belgio e Svezia, in particolare dal 2014, ha causato morti e vittime tra persone che svolgevano le loro attività quotidiane, spesso in luoghi aperti al pubblico o pubblici; questi eventi hanno cambiato la vita di molte altre persone, oltre a quelle coinvolte in maniera diretta. Tuttavia, la vita quotidiana pubblica può anche essere stravolta in maniera indiretta, attraverso atti di sabotaggio indirizzati a luoghi non pubblicamente accessibili, come il caso di opere infrastrutturali considerate strategiche per il loro impatto pubblico, infrastrutture che garantiscono il normale fluire della vita quotidiana della popolazione di una nazione e che ne possono condizionare pesantemente il comportamento.

Tra queste, le infrastrutture di rete e le strategie di cybersecurity continuano ad assumere un ruolo sempre più importante, ma non bisogna trascurare anche la crucialità delle infrastrutture fisiche, tangibili, di natura diversa da quelle di rete o militari.

Gli attacchi contro i Paesi, la loro identità e la loro popolazione, avvengono, non solo all'interno dei confini nazionali, ma spesso al di fuori di essi, lontano dagli occhi della maggioranza della popolazione domestica: il caso più esemplare è rappresentato da ambasciate, consolati e basi militari all'estero, dove gli obiettivi non sono solo le infrastrutture in quanto tali, ma anche il personale operante al proprio interno, meglio noto come "la Forza". Gli attacchi al cuore di un Paese possono colpire anche strutture e luoghi non necessariamente pubblici o di carattere istituzionale, luoghi che sebbene aperti al pubblico sono di natura privata, ma di fruizione pubblica, e sono al tempo stesso simbolicamente rappresentativi dell'identità di una Nazione, sia sul territorio nazionale che all'estero: IKEA, Carrefour, Eataly, solo per citarne alcuni, possono essere esempi validi di questa categoria.

Le strategie di sicurezza di antiterrorismo a livello di Force Protection Engineering, proveniente dall'ambito militare, devono essere implementate su una scala più ampia di quella attuale, in aree e strutture considerate sensibili a causa della loro rappresentatività strategica per la Nazione e probabilmente e sulla base del grado di apertura al pubblico, piuttosto che solo sul carattere istituzionale e la sola funzione operativa che espletano.

L'obiettivo di questo articolo è quello di stimolare una maggiore consapevolezza dell'importanza dell'adozione di strategie di counter-terrorism e pubblica sicurezza a livello delle infrastrutture e dell'ambiente costruito, analizzando alcune tra le best practices basate sull'evidenza scientifica (evidence based design) ed iniziative di policy governative di Paesi colpiti dalla minaccia del terrorismo.

1 https://www.sicurezzaegiustizia.com/giuseppe-lacanna/

L'importanza del controterrorismo e della Sicurezza Nazionale

Il controterrorismo e la Sicurezza Nazionale sono questioni critiche che hanno un impatto significativo sulla sicurezza e il benessere sia degli individui che delle Nazioni. La minaccia del terrorismo è diventata una preoccupazione principale per molti Paesi in tutto il mondo, poiché i gruppi terroristici continuano a compiere attacchi contro i civili e le infrastrutture strategiche. Gli sforzi che vengono compiuti in materia di antiterrorismo mirano a prevenire, interrompere e reagire alle attività terroristiche. Ciò include misure come la raccolta di informazioni, sorveglianza ed operazioni di polizia finalizzate ad interrompere lo sviluppo, e soprattutto l'esecuzione, di piani terroristici, assicurando alla giustizia coloro che ne sono responsabili. A queste si aggiungono anche misure per prevenire la radicalizzazione e il reclutamento di individui da parte delle organizzazioni terroristiche.
Il concetto di Sicurezza Nazionale, d'altra parte, si riferisce alla capacità di un Paese di proteggere i propri cittadini e il proprio territorio da minacce sia esterne che interne di qualsiasi genere. Esso si sviluppa su diverse aree, come la difesa militare, la sicurezza delle frontiere, la sicurezza cibernetica e la protezione delle infrastrutture strategiche. Assicurare la Sicurezza Nazionale è essenziale per mantenere la stabilità e proteggere la sovranità di una Nazione. Il controterrorismo e la Sicurezza Nazionale sono strettamente correlati, poiché gli attacchi terroristici spesso minacciano sia la sicurezza degli individui che la stabilità delle Nazioni. Pertanto, è necessario un approccio onnicomprensivo e multidimensionale a entrambe le questioni per affrontare efficacemente la minaccia del terrorismo e garantire la sicurezza di una Nazione. La debolezza, o l'incapacità, di prevenire, intercettare ed affrontare queste minacce può avere conseguenze significative, tra cui perdite di vite, feriti e danni ad infrastrutture critiche per la vita del Paese e dei suoi cittadini; nonché provocare disordine economico ed erosione delle libertà civili.
Pertanto, l'importanza del controterrorismo e della tutela della Sicurezza Nazionale non può essere sopravvalutata e richiede costante attenzione e risorse per rimanere al passo con una minaccia sempre più multidimensionale ed in continua evoluzione.

Il ruolo dell'ingegneria nel contesto del controterrorismo

L'ingegneria svolge un ruolo fondamentale nel controterrorismo e nella tutela della Sicurezza Nazionale, poiché aiuta a progettare e sviluppare i sistemi, le strutture e le tecnologie utilizzati per proteggere i cittadini, gli operatori della sicurezza, ed i beni di uno Stato da eventuali attacchi terroristici. Gli ingegneri utilizzano le loro abilità e conoscenze di materiali, meccanica, sostanze, e principi di progettazione strutturale ed architettonica per creare soluzioni in grado di resistere agli effetti di esplosioni di ordigni militari o di tipo rudimentale (IED), del fuoco di armi leggere e di altre forme di aggressione, non ultime quelle di tipo Chimico-Batteriologico-Radioattivo-Nucleare (CBRN) o condotte a mezzo di sistemi UVT (droni).
Il ricorso all'utilizzo di particolari classi di calcestruzzo rinforzato e acciaio, nonché alle proprietà

balistiche e antiesplosivo di ogni elemento architettonico, dagli infissi e finestre, alle porte e coperture, tutto per ridurre al minimo i danni causati dalle deflagrazioni, aumentando l'assorbimento dell'onda d'urto e riducendo le proiezioni di schegge di materiale, è uno dei principali ambiti della difesa infrastrutturale.
Ciò rientra nella progettazione ed implementazione dei cosiddetti sistemi di Difesa Passiva, ovvero barriere fisiche, come muri, recinzioni, fossati e barriere meccaniche, atte a proteggere dal fuoco di armi leggere e ordigni, intrusioni non autorizzate con o senza sfondamento e da altre forme di aggressione fisica.
L'obiettivo è creare barriere difficili da scalare, penetrare o violare., sia per tutelare l'incolumità della forza operante all'interno di tali infrastrutture, che per garantirne la loro continuità operativa.
Rientrano in quest'ambito, anche lo sviluppo di soluzioni come valvole di esplosione e sistemi di sovrappressione per proteggere dagli effetti delle esplosioni, tanto gli edifici sopra terra, che le strutture sotterranee come tunnel e bunker, in questo caso progettati per resistere ad attacchi di ben più ampia magnitudine, del tipo aereo e missilistico.
Oltre alle barriere fisiche, di difesa cosiddetta 'passiva', l'ingegneria svolge anche un ruolo importante nella progettazione e implementazione di sistemi di difesa e sicurezza attivi come quelli elettronici, tipo telecamere CCTV di sorveglianza e sensori di movimento, per rilevare e controllare l'accesso a zone sensibili non autorizzate. Le soluzioni in questo ambito includono anche lo sviluppo ed utilizzo di sistemi di sicurezza biometrici, come il riconoscimento delle impronte digitali o del volto, controllo targhe ANPR /LPR, e sistemi a radiofrequenza RF anti-drone/sciame di droni (Swarming).
In generale, si può asserire che l'ingegneria svolge un ruolo cruciale nell'attività di controterrorismo, e quindi di tutela della Sicurezza Nazionale, mettendo a disposizione la conoscenza e l'esperienza tecnica per lo sviluppo e l'implementazione di soluzioni di difesa passiva ed attiva ad hoc finalizzate alla protezione della popolazione (sia forza lavoro che comuni frequentatori) e delle infrastrutture strategiche di uno Stato.
Nel corso del tempo, la concentrazione di queste questioni di difesa delle infrastrutture, in ambito principalmente militare, si è consolidata nella disciplina della Force Protection Engineering (FP), la quale ancora oggi è usata come dottrina dai Paesi membri della NATO.
Il punto è che ad oggi, probabilmente anche infrastrutture non proprio di carattere militare dovrebbero ispirarsi ad alcune delle soluzioni di FP per fronteggiare gli effetti di una minaccia terroristica fluida, che puo' attaccare ovunque per colpire anche in maniera indiretta uno Stato e i suoi valori.

Il concetto di Evidence-Based Design e di Smart Force Protection Engineering

Il concetto di progettazione basata sull'evidenza (EBD) è un approccio che utilizza dati e ricerche di impronta scientifica per informare la progettazione e lo sviluppo di edifici, sistemi e tecnologie. Si basa sul principio che le decisioni relative alla progettazione, ovvero Design in inglese, debbano essere informate da evidenze scientifiche aggiornate e specifiche per quel determinato intervento, piuttosto che

dall'intuizione o dalla consolidata esperienza professionale pregressa, magari maturata su interventi simili, ma non proprio esattamente congruenti.
Per progettare e sviluppare edifici, infrastrutture e sistemi preposti alla loro difesa in grado di resistere agli effetti degli attacchi terroristici, la progettazione, partirebbe dall'analisi retrospettiva dei dati sugli attacchi passati, degli effetti causati dai diversi tipi di arma o esplosivi utilizzati, e da una valutazione oggettiva delle prestazioni delle misure protettive esistenti, anche simulata con software specifici. Una scansione della letteratura scientifica in materia e possibilmente una serie di user-surveys, incrociate con opportuni rapporti informativi sulla condizione generale socio-politico-economica, completano quella che comunemente è definita 'triangolazione' degli effetti.
La Smart Force Protection Engineering (SFPE) è un approccio innovativo all'ingegneria di protezione della forza classica (Force Protection Engineering, FPEng), che combina l'EBD con tecnologie e sistemi avanzati per creare soluzioni ancora più efficienti ed efficaci.
La SFPE, che in teoria deriva dalla meglio nota Force Protection (FP), utilizza le ultime tecnologie in aree come la sensoristica, l'analisi automatizzata dei dati e l'intelligenza artificiale (AI) per creare un sistema di protezione della forza integrato, che mette a sistema le soluzioni di protezione fisico-meccaniche con sistemi di monitoraggio e analisi in tempo reale, risultando quindi in un sistema di difesa più robusto in fase di attacco e flessibile in fase di risposta. La maggiore differenza con la FP tradizionale, sta esattamente in quanto appena enunciato: vale a dire, l'implementazione di sistemi smart o guidati da algoritmi di AI su sistemi di difesa passivi pressoché statici, dal punto di vista della loro funzione.
La combinazione di EBD e SFPE offre un approccio potente allo sviluppo ed implementazione di strategie di controterrorismo a livello della protezione infrastrutturale e dell'incolumità fisica sia della forza lavoro che opera al proprio interno che di altri comuni cittadini frequentatori della stessa o delle immediate vicinanze, contribuendo di conseguenza alla tutela generale della Sicurezza Nazionale; tutto ciò in quanto tale combinazione di approcci consente agli ingegneri di progettare e sviluppare soluzioni ad hoc altamente efficaci, basate su ricerche e dati solidi che ne validano le funzionalità prima della reale esecuzione, contribuendo pertanto anche all'ottimizzazione delle risorse finanziare impiegate.

L'importanza delle infrastrutture intelligenti, ovvero smart infrastructures

Le infrastrutture intelligenti, meglio note come smart infrastructures, sono infrastrutture come edifici, ad esempio, che utilizzano tecnologie avanzate e sistemi di rilevamento, analisi e proiezione di dati per migliorare le loro prestazioni, ed efficienza di risposta a sollecitazioni esterne; il tutto in maniera automatizzata.
L'infrastruttura si autoregola in fase di risposta, è viva e reattiva, sulla base del tipo di input che identifica come proveniente dall'esterno e sulla sua classificazione. La modulazione automatizzata della risposta

spesso avviene sulla base di uno storico di dati che permette agli algoritmi alla base del sistema di riconoscere gli indizi, anche preliminari, di una minaccia esterna e rispondere al momento opportuno e nella maniera più giusta. Di fatto un tale sistema offre un supporto non indifferente ad attività che tradizionalmente richiederebbero un ingente dispendio di energie e risorse, senza la garanzia di un giusto livello di reattività nella risposta.
Nel caso del contrasto al terrorismo, le infrastrutture intelligenti possono comprendere edifici, sistemi di trasporto e altre infrastrutture critiche, che sono in grado di adattarsi alle minacce di sicurezza ed innescare una serie di misure di auto-protezione, andando a prefigurare un sistema di difesa attivo complementare alla eventuale sicurezza armata e al sistema di difesa passivo.
Un esempio di infrastruttura intelligente potrebbe includere telecamere CCTV che utilizzano l'intelligenza artificiale per rilevare comportamenti categorizzati come sospetti e segnalarli automaticamente alle autorità competenti, o sensori in grado di rilevare la presenza di esplosivi o altre sostanze pericolose, oppure addirittura di un drone sospetto in avvicinamento, innescando automaticamente una serie di misure di difesa meccaniche che bloccano l'accesso ad alcune aree dell'edificio o del compendio. Per non parlare dell'accesso carraio con i rispettivi controlli di sicurezza, che potrebbero essere in toto o in parte automatizzati con l'interpolazione di sistemi LPR/ANPR e sistemi di lettura biometrici che si basano su banche dati interne che contengono ad esempio i dettagli degli autorizzati all'accesso.

Un aspetto importante delle infrastrutture intelligenti è l'integrazione e la condivisione dei dati tra diversi sistemi, agenzie e punti di controllo, nonché intere network di edifici, in un futuro neanche tanto prossimo: il riferimento in questo caso è alle network di edifici intelligenti, che da smart buildings creano le meglio note smart cities, ovvero una serie di edifici e infrastrutture smart collegate e comunicanti tra loro all'occorrenza. Ciò può presupporre l'uso di banche dati condivise, strumenti di analisi dei dati e sistemi di comunicazione che dal livello di controllo decentralizzato e indipendente possono passare a quello centralizzato, consentendo a diversi attori di diverse organizzazioni di condividere informazioni in tempo reale e coordinare i loro sforzi per attivare misure di protezione ad hoc, ad esempio nel caso di attacchi terroristici su larga scala.
In sostanza, l'architettura alla base delle infrastrutture intelligenti rispetto a quelle tradizionali può contribuire a migliorare la resilienza dei sistemi di difesa sia passiva che attiva di edifici ed infrastrutture critiche, ovvero la loro capacità di resistere e reagire ad interruzioni dei loro normali flussi operativi innescate da eventi avversi come attacchi terroristici.

Smart cities e smart infrastructures: rischi, opportunità e vulnerabilità nelle città del futuro

Nel mondo di oggi, le città stanno rapidamente evolvendo grazie all'innovazione tecnologica. Le smart cities, o città intelligenti, stanno emergendo come uno dei modelli di sviluppo urbano più promettenti per affrontare le sfide sociali, economiche ed ambientali. Le smart cities, poi, altro non sono che una network

di smart buildings e smart infrastructures interconnessi tra di loro, basate su uno scambio continuo di dati. Tuttavia, come con ogni trasformazione radicale, ci sono rischi, opportunità e vulnerabilità da considerare attentamente.

Le smart cities offrono numerosi vantaggi, ma presentano anche sfide significative. Due dei principali rischi sono la privacy e la sicurezza dei dati raccolti. Le smart cities raccolgono una grande quantità di informazioni sensibili attraverso sensori e dispositivi connessi, creando così il rischio di violazioni della privacy e accessi non autorizzati alle banche dati condivise. L'adozione di misure di sicurezza robuste e politiche di protezione dei dati solide diventa fondamentale per prevenire intrusioni cibernetiche e abusi delle informazioni personali dei cittadini.

Le sfide legate alla privacy non possono essere ignorate o sottovalutate. Gli accessi non autorizzati alle banche dati condivise possono portare a gravi violazioni della privacy. I dati personali dei cittadini, come informazioni finanziarie o abitudini di consumo, possono essere utilizzati in modo improprio per scopi di sorveglianza o discriminazione. Inoltre, la creazione di profili invasivi basati sui dati raccolti nelle smart cities può limitare la libertà individuale e favorire la profilazione discriminatoria. La protezione dei dati personali e la sicurezza delle informazioni diventano, quindi, prioritari per garantire che le smart cities, e prima ancora gli smart buildings, non mettano a rischio la privacy dei cittadini.

Nonostante i rischi, le smart cities offrono anche opportunità significative. La loro implementazione consente di promuovere l'efficienza energetica e la sostenibilità, grazie alla gestione intelligente dell'energia e all'ottimizzazione dei trasporti. Inoltre, le smart cities promuovono la mobilità intelligente attraverso l'adozione di soluzioni avanzate come il trasporto pubblico intelligente e le auto elettriche, riducendo la congestione del traffico e migliorando la qualità dell'aria. Inoltre, stimolano una partecipazione attiva dei cittadini alla vita pubblica grazie all'uso di piattaforme digitali e strumenti di interazione. Tra le opportunità significative, non dimentichiamo, però che l'interconnessione di alcune infrastrutture intelligenti, come fino adora descritti, nel caso dei sistemi di difesa di infrastrutture critiche può essere di notevolissima importanza, così come la tracciabilità delle abitudini e degli spostamenti nell'ambito investigativo, che in questo caso risulterebbe ampiamente facilitata.

Per concludere, le smart cities e le smart infrastructures o smart buildings, rappresentano una visione promettente per il futuro delle città, ma richiedono un approccio equilibrato che affronti sia i rischi che le opportunità. È necessario garantire politiche di protezione dei dati solide, misure di sicurezza robuste e una maggiore consapevolezza sulla privacy digitale, specificatamente adattate a questo tipo di sistemi. Solo attraverso un'impostazione olistica e attenta alla sicurezza e alla privacy, le smart cities e le smart infrastructures possono realizzare il loro potenziale per migliorare la vita dei cittadini senza compromettere i loro diritti e la loro privacy.

I vantaggi dell'utilizzo dell'Evidence-Based Design applicato alle misure di controterrorismo.

La vera potenza dell'utilizzo dell'approccio EBD nella progettazione di sistemi di difesa delle infrastruttre sta nel procedere nella valutazione delle scelte dei dettagli progettuali, qualsiasi sia il livello, attraverso scenari di attacco reali simulati, spesso attraverso l'utilizzo della realtà virtuale e quella aumentata VR/AR, ma non di rado anche di mockup 1:1, come nel caso di Paesi come gli Stati Uniti d'America.

Tra i vantaggi dell'utilizzo dell'Evidence-Based Design (EBD) nella progettazione e valutazione delle misure difensive a protezione di infrastrutture critiche, della forza operante al loro interno e di comuni frequentatori dell'area dagli effetti di azioni terroristiche, possiamo menzionare:

1. Efficacia migliorata: utilizzando dati provenienti da un processo di ricerca scientifico per informare le decisioni progettuali, l'EBD può supportare la creazione di sistemi difensivi più efficaci della media nella protezione da eventuali attacchi terroristici. Ciò può comprendere la progettazione di edifici e infrastrutture più resistenti agli effetti delle esplosioni o lo sviluppo di altri sistemi di sicurezza di tipo elettronico, meccanico o biometrico.

2. Efficienza aumentata: l'EBD può contribuire all'individuazione della soluzione difensiva più efficace quando ci si trova a dover scegliere tra diverse soluzioni disponibili. Attraverso l'analisi e comparazione delle prestazioni delle misure di protezione esistenti, per esempio, gli ingegneri possono individuare possibili aree di miglioramento e sviluppare soluzioni di più alta prestazione e accuratezza.

3. Maggiore comprensione della minaccia: analizzando i dati relativi alla conduzione degli attacchi terroristici passati, delle caratteristiche tipologiche delle infrastrutture, l'EBD può aiutare a identificare modelli e tendenze nelle metodologie di attacco utilizzate. Ciò può essere alla base della progettazione di strategie e tattiche di difesa passiva e attiva, e contribuire quindi al miglioramento della sicurezza generale di una Nazione, delle sue infrastrutture, e dei suoi cittadini.

5. Efficienza dei costi: l'utilizzo dell'EBD può anche contribuire ad ottimizzare i costi associati agli sforzi di contrasto al terrorismo, per quanto riguarda l'impatto economico delle strategie di difesa e protezione dei siti pubblici e strategici e del personale in forza al proprio interno. Ciò può comprendere la riduzione dei costi di costruzione, manutenzione e funzionamento delle misure protettive da adottare.

In generale, utilizzando l'EBD si possono creare soluzioni difensive più efficaci ed efficienti, migliorando la resilienza dei sistemi di difesa delle infrastrutture critiche e fornendo una risposta più completa alla minaccia del terrorismo; per arrivare ad un aumento della sicurezza generale di una nazione.

Esplorando le strategie di Smart Force Protection Engineering

Ci sono diverse strategie che possono essere utilizzate per comporre un sistema di SFPE. A seconda del livello di difesa che si ritiene opportuno installare, tali strategie possono essere implementate in maniera combinata o singola. L'implementazione, dunque, di diverse strategie porta ad una complessità del sistema di difesa che necessita di una pianificazione e coordinazione dettagliata, seguita da tutta una serie di test di verifica e validazione. Solo in questo modo è possibile giungere alla realizzazione di un sistema di SFPE completo, efficace e coordinato, tenendo sempre a mente che la multidimensionalità della minaccia terroristica odierna richiede una risposta difensiva altrettanto multidimensionale.

Tra le strategie più utilizzate nell'ambito dei sistemi di SFPE si possono annoverare:

1. Sistemi anti-esplosione: questa strategia mira a ridurre al minimo i danni causati dalle esplosioni, facendo leva sulle proprietà dei materiali di costruzione, principalmente calcestruzzo rinforzato e acciaio, ma anche vetro stratificato con proprietà balistiche. Porte, finestre ed infissi vari con proprietà balistiche rientrano in questa categoria. La loro combinazione ha come obiettivo la messa in sicurezza di edifici e infrastrutture, rendendoli in grado di resistere agli effetti di diverse armi da fuoco ed esplosivi.

2. Progettazione di barriere fisiche: questa strategia prevede l'utilizzo di barriere fisiche come muri, recinzioni ed ostacoli fisici di varia morfologia per proteggere infrastrutture ed operatori dal fuoco di armi di calibro modesto e attacchi condotti con veicoli terrestri; tipico è il caso di attacchi condotti con veicoli in cui sono occultate cariche esplosive. L'obiettivo delle strategie messe appunto in questo ambito é rendere l'avvicinamento e penetrazione di un sito difficile da violare e arginare, compartimentalizzandolo, l'eventuale punto di contatto.

3. Sistemi di sicurezza elettronici: questa strategia prevede l'utilizzo di sistemi di sicurezza elettronici, come telecamere di sorveglianza, sensori di movimento e sistemi di sicurezza biometrici anche basati su algoritmi di intelligenza artificiale (AI), per rilevare e comunicare gli indizi di una potenziale minaccia. A questa categoria appartengono anche i sistemi jammer anti-drone automatici che rilevano ed abbattono droni sospetti, proteggendo di fatto un sito anche dal punto di vista di piccoli strumenti aerei. L'utilizzo di tecnologie avanzate come l'intelligenza artificiale consente un monitoraggio e un'analisi in tempo reale delle minacce potenziali, rendendo possibile un rapido rilevamento ed un'eventuale risposta immediata.

4. Progettazione di strutture sotterranee: questa strategia prevede la progettazione e la costruzione di strutture sotterranee come tunnel e rifugi per proteggere da attacchi aerei e missilistici. Queste strutture, solitamente costruite con calcestruzzo rinforzato e acciaio, possono includere valvole anti-esplosione e

sistemi di sovrappressione per proteggere l'interno del sito dagli effetti delle esplosioni.

5. Cybersecurity: le strategie di cybersecurity mirano alla protezione delle infrastrutture critiche al livello dei sistemi di rete internet e tutto ciò che ad esso è connesso, come hardware, software e repository di dati sensibili. L'obiettivo, in questo caso, è la protezione da accessi non autorizzati ed attacchi cibernetici finalizzati all'alterazione, cancellazione e distruzione dei dati, nonché al malfunzionamento o paralisi del flusso operativo di un sito, infrastruttura o organizzazione. Tipici esempi di misure di difesa a questo livello includono l'utilizzo di firewall, sistemi di tracciamento e rilevamento delle intrusioni sospette ed il ricorso alla crittografia per proteggere contro l'accesso non autorizzato, l'uso improprio e la disruption dei sistemi informativi.

6. Strategie di Risk Assesment e Management: la valutazione e la gestione del rischio è una misura che sebbene faccia parte del processo di pianificazione del sistema difensivo / protettivo, spesso nei sistemi di SFPE la si trova anche implementata all'interno di alcune soluzioni in maniera più o meno automatizzata. Il caso più tipico é quello di software il cui riconoscimento della minaccia in quanto tale avviene sulla base di una stratificazione e clusterizzazione degli indizi rilevati, che quindi vengono identificati, analizzati e valutati al fine di gestire la risposta ad un'eventuale minaccia.

Best practices in materia di SFPE ed EBD

In giro per il mondo ci sono diversi esempi di protezione di infrastrutture strategiche che si basano su sistemi di SFPE ed EBD. Tra i più importanti per il tipo di soluzioni adottate si possono citare:

1. Il One World Trade Center: costruito per sostituire le torri gemelle distrutte negli attacchi terroristici dell'11 settembre, l'edificio è stato progettato per resistere agli effetti di un attacco terroristico multiplo; ha pareti resistenti alle esplosioni e materiali con proprietà balistiche, nonché un sistema di isolamento del basamento per proteggersi contro deflagrazioni di grande magnitudine, che includono un eventuale collasso della struttura su se stessa.

2. La London Underground: la London Underground, ovvero la metropolitana di Londra, è un esempio di infrastruttura basata su sistemi misti di SFPE. Il sistema ferroviario sotterraneo utilizza una serie di misure di sicurezza, tra cui videocamere di sorveglianza, sensori di movimento e sistemi di controllo degli accessi, per rilevare le minacce potenziali o identificare ed isolare il comparto dove un'azione avversa viene condotta. A tale sistema attivo, si sovrappone quello di difesa passivo che si basa su tutta una serie di compartimentalizzazione fisica dei percorsi.

3. Il Pentagono: il Pentagono a Washington D.C. è forse l'esempio più avanzato di sistema SFPE

misto terra-aria. L'edificio è stato progettato per resistere agli effetti di diversi attacchi terroristici, anche condotti simultaneamente, e include sia soluzioni di difese passive, che mirano ad ostacolare l'accesso pedonale e carraio, che attive, che mirano alla identificazione automatizzata delle minacce e in alcuni casi alla stessa risposta di neutralizzazione. L'intera infrastruttura può resistere non solo ad esplosioni, ma anche ad attacchi CBRN, e si basa su un complesso sistema di rilevamento e controllo che fa ampio utilizzo di algoritmi di AI, biometrica e sistemi jamming.

4. Il museo del Louvre: il Louvre a Parigi è un esempio di struttura strategica aperta al pubblico utilizza sistemi di difesa e sicurezza attivi avanzati come la tecnologia di riconoscimento facciale, l'analisi comportamentale e l'intelligenza artificiale per rilevare potenziali minacce e impedire l'accesso non autorizzato. A questo si sommano tutta una serie di misure di difesa e sicurezza passive, soprattutto all'esterno dell'edificio lungo il suo perimetro, che sono anche occultate nel contesto artistico del museo, tipo barriere antisfondamento e blocchi fisici non sempre percettibili nell'immediato rifiniti con finiture artistiche.

Altri esempi includono aeroporti importanti, soprattutto quelli internazionali, ed edifici privati ad alto valore simbolico come, ad esempio, il grattacielo più alto del mondo, il Burj Khalifa di Dubai, la cui struttura è altamente a prova di esplosivo. Aeroporti tipo quello di Chicago O'Hare, oltre ai sistemi di difesa passiva e alle barriere fisiche, tra i sistemi di difesa attiva basati sul riconoscimento facciale ha implementato anche un sistema di analisi comportamentale che in base alla clusterizzazione dei movimenti del corpo è in grado di identificare e segnalare movimenti sospetti difficili da captare ad occhio nudo, data la grandezza del sito.
Questi sistemi avanzati di difesa e sicurezza si sono dimostrati efficaci nel proteggere le infrastrutture critiche in questi diversi contesti e mostrano come l'integrazione di diverse strategie può innalzare il livello di protezione degli utenti che sono all'interno dell'edificio o nelle immediate adiacenze esterne.
Tuttavia, è importante notare che l'efficacia di queste soluzioni integrate di SFPE dipenderà anche da fattori come il livello di manutenzione, la qualità dell'implementazione dei vari sistemi e della loro interoperabilità' ed ovviamente il livello di minaccia da fronteggiare.
È giusto notare che nessuna strategia è infallibile e i gruppi terroristici sono in continua evoluzione; quindi, le strategie di valutazione e mitigazione delle minacce devono essere regolarmente revisionate, aggiornate e migliorate, possibilmente attraverso un approccio di testing scientifico del tipo EBD.

I limiti e le difficoltà di strategie a volte troppo complesse

I sistemi di difesa descritti fino ad ora, basati su soluzioni tecnicamente avanzate, possono incontrare diversi limiti alla loro implementazione che prescindono dalla loro qualità tecnica, che spesso è certificata. Se da una parte ci sono le capacità tecniche di ogni singola soluzione che forma poi insieme a tante

altre il sistema difensivo finale integrato, dall'altra il processo progettuale, di appalto e realizzazione dell'opera può essere soggetto a diverse variabili che hanno un impatto finale notevole sulla efficacia ed efficienza di ciò che verrà realizzato.
Tra questi limiti, si possono citare i seguenti:

1. Costi elevati: implementare soluzioni di SFPE può essere costoso, soprattutto quando si tratta di costruire nuovi sistemi di difesa per adattare strutture esistenti. L'uso di tecnologie avanzate e materiali con specifiche prestazioni può aumentare notevolmente i costi in base al livello di protezione da raggiungere.

2. Disponibilità limitata di dati: uno dei componenti chiave dell'approccio EBD è l'utilizzo di dati di validazione e usabilità insieme a ricerche retrospettive per informare il processo decisionale in fase di progettazione. Tuttavia, in alcuni casi, potrebbero essere disponibili solo pochi dati sulle prestazioni di alcuni tipi di armi o esplosivi, così come sull'efficacia delle misure protettive esistenti.

3. La privacy: l'uso di sistemi di sicurezza elettronici per il riconoscimento di un individuo o un veicolo, come telecamere di sorveglianza e tecnologia LPR/ANPR o di riconoscimento facciale basata su dati biometrici, può sollevare preoccupazioni per la privacy. Tali questioni riguardano la raccolta e l'utilizzo dei dati da parte di questi sistemi.

4. Complessità: le strategie di SFPE basate su EBD possono essere complesse e difficili da implementare. Soluzioni complete ed efficienti includono l'integrazione di diversi sistemi e tecnologie di difesa sia passive che attiva. Ciò fa sì che si renda necessaria una coordinazione generale centralizzata ed unica delle diverse fasi sia di progettazione, che di implementazione, in quanto la inter-comunicabilità tra le singole soluzioni componenti il sistema di difesa finale è un parametro chiave al fine di garantire un alto livello di efficienza finale del sistema.

5. Imprevedibilità della minaccia: anche con i migliori dati e trend basati su ricerche retrospettive, è impossibile prevedere ogni minaccia. I gruppi terroristici sono in costante evoluzione e possono emergere nuovi tipi di attacchi che non sono coperti dalle strategie di SFPE ed EBD esistenti.

6. Ambito di applicazione limitato: l'ambito di applicazione delle strategie di SFPE é spesso circoscritto e limitato ad una specifica infrastruttura o una parte di essa, il che significa che la protezione è limitata solo ad un'area specifica. L'obiettivo da perseguire dovrebbe essere quello di una protezione olistica e coordinata dell'intera infrastruttura.

7. Manutenzione ed aggiornamenti: le soluzioni di SFPE, così come la letteratura scientifica in materia EBD, devono essere esaminate e aggiornate regolarmente per garantire che rimangano efficaci

contro le minacce che sono in continua in evoluzione. Ciò può essere costoso e richiedere molto tempo.

8. Dipendenza dalla tecnologia: la SFPE si basa fortemente sulla tecnologia e se questi sistemi falliscono o non vengono adeguatamente mantenuti, l'impatto può influire negativamente sull'efficacia della soluzione strategica attuata.

In generale, un'attenta analisi dei limiti che si possono incontrare sia nella fase progettuale che in quella di implementazione, va condotta in fase di pianificazione, prima, e costantemente revisionata e aggiornata, anche dal punto di vista del rapporto costi-benefici, poi, cercando di instaurare un dialogo critico costruttivo tra le diverse professionalità coinvolte a diversi livelli nella elaborazione di un piano di difesa per l'infrastruttura in oggetto.

Il contesto italiano e la protezione delle infrastrutture critiche

Il Governo italiano ha adottato il D.lgs. n° 374 del 2001, convertito in legge n° 438 del 2001, per contrastare il terrorismo internazionale dopo gli attentati dell'11 settembre 2001 a New York. Questo decreto ha introdotto nuove leggi e ampliato i poteri di arresto e fermo di polizia per combattere il terrorismo. Sono state anche ratificate convenzioni internazionali per la repressione del finanziamento del terrorismo e degli attentati terroristici con esplosivi.
Successivamente, con altre leggi e decreti, sono state introdotte ulteriori misure di contrasto al terrorismo, seguendo la strategia antiterrorismo dell'Unione europea. Queste misure includono la prevenzione della radicalizzazione, la protezione dei cittadini e delle infrastrutture, la collaborazione tra gli Stati membri e la pianificazione delle risposte agli attacchi terroristici.
Negli ultimi anni, il legislatore italiano ha continuato ad intervenire con nuove leggi per prevenire e contrastare il terrorismo, introducendo nuovi reati e misure di sicurezza. Ad esempio, la legge n. 153/2016 ha introdotto nuove fattispecie di reato legate al finanziamento del terrorismo e agli atti di terrorismo nucleare.
Il pacchetto antiterrorismo, noto come legge n. 43/2015, ha introdotto nuove leggi penali e contravvenzionali per combattere l'associazione con finalità di terrorismo e i foreign fighters. Sono state apportate anche modifiche agli strumenti investigativi e alle misure di prevenzione, ampliando l'applicazione delle misure di sorveglianza speciale e del divieto di soggiorno.
Sono state previste anche nuove disposizioni per la circolarità informativa e l'inibizione dell'accesso a siti internet legati alle organizzazioni terroristiche, nonché una nuova tipologia di trattamento dei dati personali per fini di polizia.
Tutte queste misure mirano a bilanciare la necessità di sicurezza con la tutela dei diritti individuali, affrontando le sfide poste dal terrorismo internazionale.

Le pianificazioni di difesa antiterroristica si concentrano sulla sicurezza necessaria per proteggere il paese dagli attacchi terroristici. Esistono due tipi di pianificazione. Il Piano nazionale di difesa da attacchi terroristici di tipo N.B.C.R., redatto nel 2003 dalla Presidenza del Consiglio dei Ministri, mira a migliorare le capacità di difesa e protezione e fornisce linee guida sulle azioni da intraprendere e le procedure da seguire per affrontare le minacce. In base a questo piano, sono state create pianificazioni specifiche per singole amministrazioni (come il Dipartimento dei Vigili del Fuoco, Soccorso Pubblico e Difesa Civile, il Ministero degli Affari Esteri, il Ministero della Difesa e il Ministero delle Infrastrutture e dei Trasporti).
Il Piano nazionale per la gestione di eventi di natura terroristica, approvato dal decreto del Ministro dell'Interno nel maggio 2004, è stato creato per gestire eventi terroristici. All'interno di questo piano, il Dipartimento di Pubblica Sicurezza ha emesso linee guida generali il 23 agosto 2005, al fine di favorire l'integrazione e l'omogeneizzazione delle pianificazioni locali, per garantire interventi coordinati sul territorio. Il Dipartimento di Pubblica Sicurezza ha quindi creato una pianificazione discendente per le pianificazioni e le esercitazioni antiterrorismo e di difesa civile, verificandone l'efficacia attraverso specifiche esercitazioni che, va ricordato, possono solo ipotizzare scenari, rimanendo comunque imprevedibili. Da questo piano derivano tre pianificazioni particolari: la pianificazione antiterrorismo, la pianificazione dell'ordine pubblico e la pianificazione per le emergenze nei porti e negli aeroporti.

Le pianificazioni di intervento presentano caratteristiche principalmente omogenee, ad eccezione del tipo di attacco terroristico che può essere l'uso di armi non convenzionali (armi di distruzione di massa) o l'uso di armi convenzionali. Nel caso di un attacco con armi di distruzione di massa, l'intervento dei Vigili del Fuoco nell'area contaminata deve tener conto di diverse aree: l'area calda, che è stata colpita direttamente; l'area tiepida, che si presume essere comunque contaminata; e l'area fredda, che non è contaminata. Le forze di polizia devono garantire la delimitazione dell'area tiepida, indossando indumenti e protezioni adeguate per operare in sicurezza.
Gli obiettivi considerati sensibili per la loro strategicità richiedono la protezione di diverse entità in base ad una valutazione del rischio a cui li si ritiene esposti. L'Ufficio per l'Ordine Pubblico emana linee guida generali e informa gli organi locali sulle necessità di protezione dei luoghi e degli obiettivi sensibili, in base ai diversi livelli di rischio potenziale. La valutazione e l'attuazione concreta delle misure di protezione sono responsabilità delle Autorità Provinciali di Pubblica Sicurezza.

Il Prefetto, in qualità di organo politico strategico, valuta le esigenze di protezione, anche attraverso incontri di coordinamento e con l'assistenza del Centro di Protezione Operativa per la Sicurezza Pubblica (C.P.O.S.P.), attiva, modifica e revoca le misure, graduandole in base al presunto livello di rischio e segnalando all'Ufficio per l'Ordine Pubblico ogni misura adottata. Il Questore attiva tempestivamente le misure, fornisce direttive tramite un ordine di servizio e organizza i servizi.
La protezione degli obiettivi sensibili è affidata alle Forze di Polizia, ovvero la Polizia di Stato, i Carabinieri e la Guardia di Finanza. Nel caso di esigenze specifiche ed eccezionali relative alla sorveglianza di

obiettivi fissi sensibili, come edifici istituzionali e altri di interesse pubblico, l'articolo 13 della legge 121/1981 consente alle autorità militari di mettere a disposizione del Prefetto personale militare delle Forze Armate da impiegare per tale scopo.

L'articolo 18 della legge 128/2001 stabilisce che il Consiglio dei Ministri, su proposta del Presidente del Consiglio dei Ministri, in accordo con i Ministri dell'Interno e della Difesa, può adottare uno o più programmi specifici per l'utilizzo di tali contingenti da parte dei Prefetti delle province in cui si presentano tali esigenze. Tali programmi, con la partecipazione del Capo di Stato Maggiore della Forza Armata interessata, hanno una durata massima di sei mesi, rinnovabile, e definiscono il numero massimo di personale utilizzabile in ciascuna provincia e le direttive per il loro impiego, nel rispetto delle norme vigenti e delle risorse disponibili. Prima dell'attuazione, i programmi vengono trasmessi alla Camera dei Deputati e al Senato della Repubblica per ottenere il parere delle relative Commissioni parlamentari competenti.

La legge 128/2001, nell'articolo 19, specifica i poteri dei militari nel loro ruolo di prevenire e contrastare comportamenti che possano minacciare l'incolumità delle persone o la sicurezza delle strutture sorvegliate, sottolineando che possono procedere all'identificazione e al trattenimento sul posto di persone e mezzi di trasporto per il tempo strettamente necessario a consentire l'intervento degli agenti delle forze dell'ordine.

In questo contesto normativo, è bene sottolineare che per “protezione degli obiettivi sensibili” potrebbe non necessariamente intendersi “protezione delle infrastrutture critiche”. Spesso si tende a confondere i due concetti. Nel primo caso, il concetto implica la salvaguardia delle strutture che forniscono servizi di interesse pubblico diffusi e che hanno un valore economico. Nel secondo caso, l'obiettivo è garantire la continuità nell'erogazione di un servizio essenziale alla popolazione.

Per quanto riguarda la sola protezione delle Infrastrutture Critiche, l'iter storico legislativo, comunitario e nazionale è riassumibile nei principali atti di seguito riportati:

Protezione delle Infrastrutture Critiche Informatizzate - La realtà italiana 10 marzo 2004 a cura della Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le Tecnologie;

COM 2004/702 del 20.10.2004 - Comunicazione della Commissione al Consiglio e al Parlamento Europeo: la protezione delle infrastrutture critiche nella lotta contro il terrorismo;

COM 2005/576 del 17.11.2005 - Libro Verde relativo a un programma europeo per la protezione delle infrastrutture critiche;

COM 2006/786 del 12.12.2006 - Comunicazione della Commissione relativa a un programma europeo per la Protezione delle Infrastrutture Critiche;

COM 2006/787 del 12.12.2006 - Proposta di Direttiva del Consiglio relativa all'individuazione e alla designazione delle Infrastrutture Critiche Europee e alla valutazione della necessità di migliorarne la protezione;

D.P.C.M. 8/4/2008 - Criteri per l'individuazione delle notizie, delle informazioni, dei documenti, degli atti, delle attività, delle cose e dei luoghi suscettibili di essere oggetto di segreto di Stato;

Ministero dell'Interno Decreto 9 gennaio 2008 - individuazione delle infrastrutture critiche informatiche di interesse nazionale;

Direttiva 2008/114/CE dell'8 dicembre 2008 - relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione;

ROAD MAP - Relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione;

DECRETO LEGISLATIVO 11 aprile 2011, n. 61 - Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione (GU n. 102 del 4-5-2011)

Nel giugno 2004, il Consiglio europeo ha richiesto la preparazione di una strategia globale per garantire la sicurezza delle infrastrutture critiche. In seguito, il 20 ottobre 2004, la Commissione europea ha emesso una comunicazione sulla protezione delle infrastrutture critiche nel contesto della lotta al terrorismo, proponendo una serie di misure volte ad aumentare la prevenzione, la preparazione e la risposta a livello europeo in caso di attacchi terroristici che coinvolgono tali infrastrutture.
Le conclusioni del Consiglio riguardo alle misure preventive, preparatorie e di risposta agli attacchi terroristici, insieme al programma di solidarietà dell'Unione europea sulle conseguenze delle minacce e degli attacchi terroristici adottato nel dicembre 2004, hanno sostenuto l'intenzione della Commissione di presentare un programma europeo per la protezione delle infrastrutture critiche (EPCIP) e hanno concordato sulla creazione di una rete informativa di allarme sulle infrastrutture critiche (CIWIN) gestita dalla Commissione.

Nel novembre 2005, la Commissione ha pubblicato un documento di consultazione sul programma europeo per la protezione delle infrastrutture critiche (EPCIP), presentando diverse alternative per lo

sviluppo dell'EPCIP e della CIWIN.
Le conclusioni del Consiglio "Giustizia e affari interni" (GAI) nel dicembre 2005, riguardanti la protezione delle infrastrutture critiche, hanno invitato la Commissione a presentare una proposta di programma europeo per la protezione delle infrastrutture critiche.

La comunicazione st16932 illustra i principi, le procedure e gli strumenti proposti per l'attuazione dell'EPCIP. La proposta di direttiva st16933 (2006/0276 CNS) presenta le misure proposte dalla Commissione per individuare e designare le infrastrutture critiche europee (ICE) e valutare la necessità di migliorarne la protezione.
L'obiettivo generale dell'EPCIP era migliorare la protezione delle infrastrutture critiche nell'Unione europea. Per raggiungere tale obiettivo, venne stabilita la creazione un quadro comune nell'UE per la protezione delle infrastrutture critiche, come descritto nella comunicazione. L'approccio alla prevenzione delle minacce deve essere "multirischio", dunque "multidimensionale".

La Direttiva 2008/114/CE dell'8 dicembre 2008 - relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, recepita in Italia con il D.lgs. 61/2011 rappresenta una pietra miliare nel contesto italiano in termini di protezione delle infrastrutture critiche e la loro protezione.
Ad oggi, la Direttiva (UE) 2022/2557, detta anche CER (da Resilience of Critical Entities) relativa alla resilienza dei soggetti critici completa e supera la Direttiva 2008/114/CE, che a partire dal 18 Ottobre 2024 verrà definitivamente abrogata. Pertanto, tutti gli Stati membri, Italia inclusa, hanno tempo fino al 17 Ottobre 2024 per elaborare il proprio decreto attuativo.
Il passaggio importante è la definizione degli obblighi per i soggetti critici di rafforzare la resilienza e la capacità di fornire servizi essenziali, nonché' una migliore definizione di "infrastruttura e soggetto critico" e norme riguardanti la loro difesa comune, procedure di comunicazione, vigilanza ed esecuzione.

Oltre oceano, negli USA, già dal maggio 2007 la Homeland Security Department aveva presentato un programma per la protezione delle infrastrutture critiche del Paese, di respiro molto più ampio, includendo nelle categorie delle infrastrutture critiche anche le Commercial Facilities (attività commerciali), trattandole quasi come la categoria dei Monuments and Icons (momumenti ed icone nazionali).
Nel vecchio continente, invece, la Gran Bretagna muove i suoi passi per l'attuazione del Protect Duty Consultation Paper, che tra le innovazioni più importanti introduce l'obbligo di dotare di misura di sicurezza anche passive ogni edificio aperto alla fruizione pubblica, anche a carattere privato e commerciale, come misura di tutela della sicurezza pubblica nazionale.

Conclusioni

In sintesi, la progettazione basata sull'evidenza (EBD) e la Smart Force Protection Engineering (SFPE) sono approcci innovativi che utilizzano tecnologie avanzate e analisi dati coordinate per ottimizzare le prestazioni e l'efficienza dei sistemi difensivi a protezione delle infrastrutture critiche.
Così facendo, entrambi possono offrire un contributo nell'ambito delle misure di controterrorismo e di tutela della Sicurezza Nazionale, in quanto contribuiscono ad aumentare la resilienza dei sistemi di protezione delle infrastrutture critiche, proteggendo al tempo stesso l'incolumità dei cittadini italiani operanti al proprio interno e dei cittadini comuni che fruiscono degli spazi anche immediatamente adiacenti. Come abbiamo visto, per pianificare ed implementare un sistema di protezione completo ed integrato al fine di fronteggiare una minaccia terroristica sempre più multidimensionale, si possono incontrare limiti che prescindono dalla efficienza tecnica di ogni soluzione difensiva scelta per essere parte del sistema finale.

In Italia, la definizione di "infrastruttura critica" proposta dal Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche, istituito dalla Presidenza del Consiglio dei Ministri nel 2003, fa riferimento a: "il complesso di reti e sistemi che includono industrie, istituzioni e strutture di distribuzione che, operando in modo sinergico, producono un flusso continuo di merci e servizi essenziali per la funzionalità e la stabilità economica di un Paese".
Il concetto di infrastrutture critiche può essere ampliato includendo il riferimento anche ad elementi fisici, tangibili e non tangibili, persone e organizzazioni che sono fondamentali per l'erogazione di servizi essenziali alla popolazione.
Inoltre, è necessario che "l'individuazione di un'infrastruttura critica derivi dalla sua funzione e, quindi, dall'aver identificato quali sono i servizi essenziali alla popolazione" (R. Setola, 2023).

Guardando all'iniziativa portata avanti in Gran Bretagna con il Protection Duty che intende estendere il concetto di protezione passiva alle infrastrutture aperte al pubblico come le attività commerciali localizzate in determinate zone, affidando ad un'agenzia specializzata come la National Protective Security Authority NPSA (ex Centre for the Protection of National Infrastructure, CPNI) la coordinazione del dialogo tra le diverse parti coinvolte nella progettazione delle misure di sicurezza protettiva fisica delle infrastrutture e del proprio personale, si auspica che anche il nostro Paese, magari in occasione del recepimento della nuova Direttiva (UE) 2022/2557, possa tener conto dell'estensione del concetto di difesa passiva a quelle infrastrutture che seppur non critiche per la loro funzione, sono localizzate in aree potenzialmente critiche, tipo centri storici o luoghi ad alta frequentazione pubblica.

Ispirarsi ai concetti di Force Protection, se pur non ai livelli richiesti dalle infrastrutture militari o altamente critiche, potrebbe aumentare il senso di sicurezza generale dei cittadini che operano all'interno delle loro attività.

Inoltre, le attività di ricerca e sviluppo, in questo settore devono essere costantemente supportate, perché se da una parte, le analisi dei dati sulla conduzione di attacchi terroristici pregressi, la stratificazione geografico-culturale e lo studio delle misure o azioni difensivo-protettive esistenti, possono aiutare ad identificare i cosiddetti "patterns" operativi e metodi di ingaggio; dall'altra parte, l'accuratezza e l' efficacia delle singole soluzioni tecniche sviluppate, sia in fase di rilevamento della minaccia, che di resistenza ad un potenziale attacco, necessitano di un aggiornamento continuo.

È, dunque, importante che i cosiddetti policy makers, i ricercatori e i tecnici dell'ingegneria ed architettura lavorino insieme, in maniera partecipata, al fine di elaborare strategie protettive e soluzioni tecnologiche sempre migliori, in grado di proteggere al meglio le infrastrutture critiche e strategiche, il loro personale ed i loro fruitori contro gli attacchi terroristici, nel segno della protezione e tutela della Sicurezza Nazionale.

Referenze

Corpo Nazionale VV.F.. Retrieved on 2023, 12 February. Legislazione e documentazione. https://www.vigilfuoco.it/aspx/page.aspx?IdPage=3857

Dell'Aria, D., Rossi, M., 2023. Direttive NIS 2 e CER: così l'Europa metterà in sicurezza le sue infrastrutture critiche.
https://www.cybersecurity360.it/cybersecurity-nazionale/direttive-nis-2-e-cer-cosi-leuropa-mettera-in-sicurezza-le-sue-infrastrutture-critiche/

De Vincentis, F., 2023. Sicurezza nazionale e protezione delle infrastrutture critiche. La lezione di Setola. https://formiche.net/2023/05/setola-infrastrutture-critiche/

European Commission, 2023. Retrieved on 2023, 24 May. Smart cities: cities using technological solutions to improve the management and efficiency of the urban environment. https://commission.europa.eu/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en#:~:text=A%20smart%20city%20is%20a,of%20its%20inhabitants%20and%20business.

Franchina, L., 2022. Resilienza delle infrastrutture critiche: così l'Europa concilia sicurezza fisica e cyber.

https://www.cybersecurity360.it/cybersecurity-nazionale/resilienza-delle-infrastrutture-critiche-cosi-leuropa-concilia-sicurezza-fisica-e-cyber/

Ministry of Defence UK. Retrieved on 2023, 20 January. Allied Joint Doctrine for Force Protection. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/454616/20150804-AJP_3_14_Force_Protection_Secured.pdf

Post, A., 2021. The Cybersecurity Risks of Smart City Technologies: What Do The Experts Think? https://cltc.berkeley.edu/publication/smart-cities/

Regione Lombardia, 2017. Direttiva UE sulle infrastrutture critiche. https://www.regione.lombardia.it/wps/portal/istituzionale/HP/DettaglioRedazionale/servizi-e-informazioni/Enti-e-Operatori/protezione-civile/infrastrutture-critiche/direttiva-ue-sulle-infrastrutture-critiche/direttiva-ue-sulle-infrastrutture-critiche

Servizio Studi Camera dei Deputati, 2011. Attuazione della direttiva 2008/114/CE - Designazione delle infrastrutture critiche europee Schema di D.Lgs. n. 319 (art. 1, co. 3, L. 4 giugno 2010, n. 96) Elementi per l'istruttoria normativa. http://documenti.camera.it/leg16/dossier/testi/AC0594_0.htm

UK Government, Home Office. Retrieved on 2023, 10 May. Consultation outcome to Protect Duty. https://www.gov.uk/government/consultations/protect-duty/outcome/government-response-document https://www.gov.uk/government/consultations/protect-duty/outco