Minacce globali e tutela dei confini nazionali: nuovi strumenti integrati al servizio della Homeland Security

Author : Giovanni Villarosa

Date : 20 Giugno 2019

Nell'immaginario collettivo tradizionale, il confine viene sempre identificato come una *linea geopolitica* di separazione fra Stati, corrispondente alla volontà politica di garantire la **sicurezza nazionale**, difendendo i cittadini dai rischi, reali o presunti, che incombono sulla comunità nazionale.

Il processo di crescita e di capacità dei **sistemi** orientati alla protezione delle **frontiere** (aeroporti, porti, stazioni ferroviarie, varchi stradali) rappresenta una tematica significativa nel quadro generale della sicurezza nazionale; infatti, la protezione del *perimetro frontaliero* implica una costante evoluzione del livello tecnologico, sistemico, nonché organizzativo, che ne supporti efficacemente l'intero ciclo.

Ma il controllo di tali ambiti geografici, che rappresentano pur sempre degli spazi **internazionali**, implica una continua e specifica cooperazione tra **sistemi e organizzazioni** appartenenti a governi diversi.

I **rischi** interconnessi da valutare, e misurare nella logica del controllo, sono di varia tipologia, e riguardano: l'immigrazione clandestina, gli attentati e le azioni terroristiche, le azioni di sottrazione delle merci, nonché quelli derivanti dal contrabbando di sostanze pericolose o a rischio d'inquinamento ambientale, così come dal traffico illegale di prodotti ad alta tecnologia (prodotti, materiali, sostanze *dual use*).

Per garantire la sicurezza di una nazione è necessario disporre di *informazioni* immediate ed affidabili, gestite da un'unica **piattaforma integrata** (risorse umane e tecnologiche) che connetta, coordini e gestisca in tempo reale le funzionalità dei sistemi (rapidi ed efficaci nel processarle) e i sistemi di telecomunicazioni complementari per condividerle (veloci e sicuri).

Nel campo della sicurezza una piattaforma particolarmente efficace è conosciuta con l'acronimo PSIM (Physical Security Information Management); si tratta di un'interfaccia **uomo-macchina** unica che prescinde dalle molteplici tecnologie utilizzate in

campo, centralizzandole secondo un’architettura interoperabile, flessibile e aperta, con un ritorno interessante ed efficace: quello di far cooperare tra loro i diversi attori responsabili nei processi di security, safety, facility, ect.

Ad esempio, negli USA, le forze di polizia impegnate nelle attività operative di lotta al terrorismo, contrasto del traffico di droga e dell’immigrazione clandestina, vigilano le frontiere utilizzando tecnologie elettroniche particolarmente sofisticate, utilizzando poi, in una sorta di *data fusion,* le informazioni raccolte tramite le attività Comint (*communications intelligence*), Sigint (*signals intelligence*), Elint (*electronic intelligence*), e Radar (attività tipiche dell’intelligence governativa) come contromisura preventiva nel contrasto delle attività criminali **frontaliere**.

Questo perché, all’indomani dei tragici attacchi del 9/11, apparve subito chiaro come il confine fra la *sicurezza e difesa* stesse diventando **evanescente**, soprattutto in termini geografici; difatti, da quel momento in poi, circoscrivere la dimensione nazionale da quella internazionale, o le classiche operazioni di polizia da quelle tipicamente militari, sarà impossibile quanto utopico, vivendo ormai nella diffusa consapevolezza di avere a che fare con un terrorismo sempre più **globalizzato***,* in grado di colpire chiunque, ovunque e comunque, in ogni angolo del mondo; un motivo questo che ha spinto tutti governi nel dare una risposta concreta in materia di sicurezza nazionale, orientata al **superamento**, giustamente, del sovrano perimetro **geografico**, assumendo una nuova **dimensione strategica e operativa,** specifica e dalle caratteristiche globali.

Il primo Stato al mondo a occuparsi fattivamente del problema, come risposta all’attacco terroristico "*nine eleven"* sono stati, loro malgrado, proprio gli USA, creando una struttura *ad hoc* come il Department of Homeland Security (DHS, che sovraintende anche il Secret Service presidenziale), con il primario compito di proteggere, in tema di *security*, i confini degli Stati Uniti d'America da attacchi terroristici e, nello stesso tempo, il territorio da eventi tipicamente *safety*, come nel caso di eventi naturali disastrosi.

Nasce così la *Homeland Security* (HS), che si occuperà degli aspetti relativi alla protezione della popolazione da eventi indotti dall’uomo - quali terrorismo, sabotaggio, etc. - o naturali - come inondazioni, terremoti, etc. - utilizzando i sistemi tradizionali di *homeland protection*, principalmente costituiti dalle componenti di **osservazione e detezione** (sensoristica), di **decisione** (comando e controllo), e di **reazione** (attuatori), messi in rete tramite un sistema integrato di comunicazione.

Si delinea quindi una nuova terminologia all’interno del gergo letterario della **sicurezza** statunitense: perché la *homeland* nasce come risposta all’attacco terroristico sulle Twin Towers del Word Trade center di New York e racchiude in sé l’immane impegno politico e organizzativo attuato dal governo federale per fronteggiare e contrastare la crescente **minaccia asimmetrica** attuata dal terrorismo di matrice islamica fondamentalista.

Peraltro la strategia HS coniuga, attraverso un unico canale strategico di gestione e realizzazione, tre singole scienze: la Difesa, la Sicurezza e l’Intelligence; è poi articolata in **tre settori specifici**:

- *Security*, intesa come uno stato da conseguire e mantenere per promuovere il benessere dei cittadini e la vitalità democratica delle istituzioni;
- *Safety*, intesa come gestione delle emergenze, una pratica che deve essere sviluppata e condivisa da istituzioni e cittadini per reagire alla manifestazione dell'evento possibile;
- Protezione da attacchi del terrorismo, affrontato come una minaccia destinata a perdurare nel tempo a cui è necessario fornire risposte preventive articolate.

In Italia, il concetto di *homeland security* viene declinato (per astrazione) in **sicurezza nazionale,** indirizzandosi alla protezione delle infrastrutture critiche nazionali, della popolazione e dei confini di Stato; infatti, funzioni simili alla HS le ritroviamo come specifiche competenze nel Ministero dell'Interno (con la Polizia di Stato quale *ufficio di security*, la Difesa Civile e i Vigili del Fuoco quali *uffici di safety*), e presso la Presidenza del Consiglio dei Ministri (DIS, AISI e AISE quali agenzie *intelligence* e di *sicurezza nazionale*, la Protezione Civile come dipartimento di protezione dai disastri naturali e non).

Quando parliamo di una **infrastruttura critica**, intendiamo quell'insieme di sistemi fisici, informatici, e di tutta una serie di *risorse vitali* per il corretto funzionamento di uno Stato, giacché il loro collasso funzionale, la cd. **indisponibilità funzionale**, o la stessa distruzione genererebbe un impatto negativo sui servizi essenziali della nazione, sulla **sicurezza sociale** (safety, security, emergency), su quella economico-finanziaria, e sulla salute pubblica.

Da ciò si evince come la sicurezza, al di la delle ragioni etimologiche/epistemologiche, rappresenti di per sé **un'astrazione multidimensionale**, che assume un significato diverso su soggetti diversi, peraltro, in ambiti altrettanto diversi, e se guardiamo al significato sicurezza dato dalla HS, allora dobbiamo spaziare su ambiti multidisciplinari, come: *Safety, Security, Emergency, Risk Management, Prevention and Control of the Territory, Protection, Urbanization*, etc.

Dunque la sicurezza *homeland* non va erroneamente riferita al solo, quanto complesso, insieme dei confini geografici (marittimo-terrestre-aereo) che ogni nazione sovrana deve salvaguardare e proteggere, ma dovrà essere, seppur con sostanziali differenze, supportata anche da coerenti azioni politiche di **sicurezza urbana**, quale complemento specifico alla HS, perché come si è visto in questi anni l'una coadiuva l'altra, seppur con le dovute e sostanziali differenze strutturali, tecniche, ambientali, metodologiche.

La mutazione della minaccia terroristica, divenuta globale (arrivando fin dentro i confini nazionali) e la posizione geostrategica dell'Italia nel cuore del Mediterraneo, rappresentano fattori che hanno accresciuto in questi anni l'esigenza di rivedere i nostri parametri di sicurezza nazionale, in funzione della globalizzazione della minaccia, sia essa di origine antropica o naturale, ponendo in campo differenti approcci e nuove metodologie di contrasto, da parte delle istituzioni, delle FF.AA/FF.OO e dell'industria.

Come sempre, un **ruolo importante** continuerà a giocarlo l'**industria nazionale** giacché, fornendo strumenti e tecnologie innovativi, darà un contributo essenziale alle azioni di contenimento e contrapposizione al rischio di attacchi terroristici.

Ciò detto, osserviamo come le minacce saranno **sempre meno prevedibili** e la valutazione di cosa proteggere, da chi, quando e con quali modalità, diventerà sempre più complessa, con scenari sempre più critici, con un livello di sicurezza direttamente proporzionale alla possibilità di avere corrette informazioni, elaborarle, condividendole rapidamente, integrandole in un unico e comune sistema, capace di selezionarne gli interventi più adeguati, consentendo nel contempo di assumere le decisioni più efficaci.

Per dare risposte a questi nuovi scenari di rischio la *homeland protection* utilizzerà i **nuovi sistemi integrati** che l'industria oggi mette a disposizione, costituiti da un insieme complesso di sistemi e apparati, tecnologicamente molto avanzati, che svolgono sì funzioni autonome, ma sinergicamente interconnesse tra loro nello scambio dei dati operativi, aumentando esponenzialmente il potenziale della prevenzione nel contesto della sicurezza; parliamo del sistema VTS (vessel traffic service, sorveglianza e sicurezza porti, sicurezza della navigazione, monitoraggio di traffici illeciti in mare, etc) per il controllo del traffico marittimo, del sistema ATC (*air traffic contro*l, ad esempio il monitoraggio radar dei piccoli aeromobili utilizzati per atti terroristici che cercano di superare i dispositivi di sorveglianza aerea civile e militare) per il controllo del traffico aereo, e dei sistemi C4ISR (*command, control, communications, computers, intelligence, surveillance and reconnaissance*, *capabilities* vitali nella cyber security) di comando e controllo per la sicurezza terrestre, tanto per citare i più importanti.

Un esempio indicativo di questa **integrazione sinergica,** nel controllo delle frontiere marittima, aerea e terrestre, lo troviamo nella città di Genova: tre infrastrutture (portuale-aeroportuale-ferroviario) contigue e interoperanti tra loro, realizzate fisicamente all'interno dello stesso perimetro territoriale, e che sono nello stesso momento *critiche e di frontiera,* rappresentando un problema non trascurabile nell'analisi e nella valutazione delle vulnerabilità, come pure nella scelta delle adeguate misure di sicurezza da applicare.

L'autorità portuale, ad esempio, deve monitorare costantemente il transito dei container, il controllo delle merci, degli accessi e gli sbarchi dalle navi passeggeri, individuando eventuali clandestini, persone e merci riconducibili ad attività terroristiche (attacchi CBRNe), anche a beneficio delle altre infrastrutture adiacenti (aeroportuale e ferroviaria).

Insomma, proteggere i nostri confini dalle infiltrazioni terroristiche e dall'immigrazione clandestina, dal traffico di armi e armamenti, dal traffico di droga e dal contrabbando, promuovendo, nel contempo, il corretto scambio commerciale con l'estero e l'immigrazione legale, è di **vitale importanza** per la sicurezza interna e lo sviluppo economico del nostro sistema paese ma, soprattutto, rappresenta la garanzia della propria sovranità nazionale.

E mai come in questo periodo di forte contrapposizione sociopolitica - non soltanto nazionale - gli apparati della sicurezza pubblica e privata, che gestiscono e regolano i settori nevralgici (telecomunicazioni, trasporti, immigrazione, produzione e fornitura di energia, sanità, industria, etc.) dovranno applicare processi di contrasto, con un grado di approntamento di livello sempre crescente, alle diverse e inaspettate minacce generate quotidianamente dal terrorismo.

Sitografia

https://www.usa.gov/federal-agencies/.

https://www.dhs.gov/.

https://www.puntosicuro.it/.

https://www.anfos.it/.

http://www.masterhomelandsecurity.eu/.

Articolo a cura di **Giovanni Villarosa**