Corso di
SICUREZZA NEL TRASPORTO E NELLE INFRASTRUTTURE STRATEGICHE

Lezione 3 – Nozione Infrastrutture Strategiche

Ivan Rizzolo, Ph.D.
ivan.rizzolo@unipd.it


LA MINACCIA INVISIBILE

Il termine Infrastruttura strategica è stato un significato nel tempo un po' abusato…

Lo troviamo nella documentazione del Ministero dei Trasporti laddove per strategico si intendono infrastrutture «importanti» per il sistema Paese;

Altri domini nel tempo gli hanno dato significati diversi per situazioni diverse….

Anche un'autostrada è strategica per collegare il mare dalla montagna?

Infrastruttura critica

Con il termine infrastruttura critica si intende un sistema, una risorsa, un processo, un insieme, la cui distruzione, interruzione o anche parziale o momentanea indisponibilità ha l'effetto di indebolire in maniera significativa l'efficienza e il funzionamento normale di un Paese, ma anche la sicurezza e il sistema economico-finanziario e sociale, compresi gli apparati della pubblica amministrazione centrale e locale.

Infrastrutture critiche

Solitamente sono associati al concetto di infrastrutture critiche le risorse relative a:

Produzione, trasmissione, distribuzione, dispacciamento dell'energia elettrica e di tutte le forme di energia, quali ad esempio il gas naturale

Telecomunicazioni e telematica;

Risorse idriche e gestione delle acque reflue;

Agricoltura, produzione delle derrate alimentari e loro distribuzione;

Infrastrutture critiche

Sanità, ospedali e reti di servizi e interconnessione;

Trasporti aereo, navale, ferroviario, stradale e la distribuzione dei carburanti e dei prodotti di prima necessità;

Banche e servizi finanziari;

Sicurezza, protezione e difesa civile (forze dell'ordine, forze armate, ordine pubblico);

Le reti a supporto del Governo, centrale e territoriale e per la gestione e delle Emergenze

I Governi normalmente mettono a punto studi e progettano misure precauzionali per ridurre il rischio che le infrastrutture critiche vengano a mancare in caso di guerra, disastri naturali, scioperi, vandalismi o sabotaggi. Tale attività viene definita *protezione delle infrastrutture critiche - CIP - Critical Infrastructure Protection*. Attualmente i processi che sono alla base dei servizi e dei beni prodotti dalle infrastrutture critiche sono gestiti attraverso risorse informatiche, pertanto in questi casi si parla di infrastrutture critiche informatizzate. In tal caso si parlerà di *protezione delle infrastrutture critiche informatizzate - CIIP - Critical Information Infrastructure Protection*.

Anche in Italia si stanno sviluppando una cultura e un'attenzione (tecnica, scientifica e accademica) qualificate per questi temi, per le loro vulnerabilità esistenti e, soprattutto, per prevenire le conseguenze della crescente interconnessione sulla normale vita del Sistema Paese.

L'8 dicembre 2008 il Consiglio dell'Unione Europea ha emanato la *direttiva 2008/114/CE relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione*. Seppur relativa alle infrastrutture critiche europee, nonché parziale, in quanto focalizzata soltanto su quelle dei settori dell'energia e trasporti, il punto *a) dell'art. 2* da una definizione di infrastruttura critica, per la quale intende *"un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute,della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni"*.

In definitiva, per la difesa e protezione delle infrastrutture critiche sono necessarie e attese delle azioni da parte governativa, da parte delle aziende che le gestiscono, ma soprattutto da parte dei singoli che agiscono all'interno di una cultura orientata alla sicurezza con una visione ampia sui sistemi oltre che sui componenti. Progettisti, Consulenti, Responsabili IT e Responsabili della sicurezza aziendale, ma anche esponenti del mondo accademico, sono gli esperti da cui dipende il funzionamento e la protezione di molte infrastrutture strategiche. Da loro deve venire lo sviluppo di nuovi approcci e metodologie per ridurre le vulnerabilità e fronteggiare le nuove minacce a cui questi complessi sistemi, sempre più indispensabili per il nostro vivere quotidiano e la sicurezza e prosperità di un Paese, sono soggetti.

Con il D.Lgs n. 61 dell'11 aprile 2011 l'Italia ha recepito 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. Il decreto legislativo è entrato in vigore il 5 maggio 2011 a seguito della pubblicazione sulla Gazzetta Ufficiale (GU n. 102 del 4 maggio 2011).

Elenco dei settori di ECI (European Critical Infrastructures) sulla base della Direttiva 2008/114/CE

Settore I. *ENERGIA*

1. Elettricità - Infrastrutture e impianti per la produzione e la trasmissione di energia elettrica per la fornitura di elettricità
2. Petrolio - Produzione, raffinazione, trattamento, stoccaggio e trasporto di petrolio attraverso oleodotti
3. Gas - Produzione, raffinazione, trattamento, stoccaggio e trasporto di gas attraverso oleodotti - Terminali GNL

Settore II. *TRASPORTI*

- 4. Trasporto stradale
- 5. Trasporto ferroviario
- 6. Trasporto aereo
- 7. Vie di navigazione interna
- 8. Trasporto oceanico, trasporto marittimo a corto raggio e porti

Infrastrutture critiche: l'esempio delle centrali nucleari

Le infrastrutture critiche (IC) rappresentano un sistema strategico ritenuto essenziale per la funzionalità di una nazione, poiché forniscono i servizi primari per i cittadini e per il sistema economico e industriale: tutte le azioni che mirano a distruggere o interrompere un'infrastruttura critica, come gli eventi naturali/accidentali, le attività terroristiche o di carattere doloso, avranno sempre un impatto negativo per la sicurezza ed il benessere della società.

Nella lingua italiana esiste un solo termine per definire gli incidenti che rientrano nei perimetri della protezione da eventi di natura incidentale (colposa), da quelli specificatamente di origine criminale (dolosa), ed è il sostantivo sicurezza, ovvero: la condizione che rende e fa sentire di essere esenti da pericoli, o che dà la possibilità di prevenire, eliminare o rendere meno gravi danni, rischi, difficoltà, evenienze spiacevoli, e simili.

Le centrali nucleari, ma gli impianti atomici più in generale, vengono identificati come gli stabilimenti più sensibili dal punto di vista della sicurezza, classificati dalle normative nazionali come IC, mentre a livello sovrannazionale come infrastrutture critiche internazionali (ICI).

Nel campo della sicurezza nucleare la definizione che dà la IAEA (International Atomic Energy Agency) della nuclear security, è questa: la prevenzione, il rilevamento e la risposta a furto, sabotaggio, accesso non autorizzato, trasferimento illegale o altri atti dolosi che coinvolgono sostanze nucleari o radioattive o i relativi impianti.

Le centrali nucleari, ma gli impianti atomici più in generale, vengono identificati come gli stabilimenti più sensibili dal punto di vista della sicurezza, classificati dalle normative nazionali come IC, mentre a livello sovrannazionale come infrastrutture critiche internazionali (ICI). Nel campo della sicurezza nucleare la definizione che dà la IAEA (International Atomic Energy Agency) della nuclear security, è questa: la prevenzione, il rilevamento e la risposta a furto, sabotaggio, accesso non autorizzato, trasferimento illegale o altri atti dolosi che coinvolgono sostanze nucleari o radioattive o i relativi impianti. Nel perimetro delle attività nucleari, le attività safety, tanto quanto quelle di security, si pongono come comune obiettivo la sicurezza di limitare il rischio proveniente da materiali nucleari radioattivi e dai complessi impianti di produzione energetica. Sebbene ambedue si focalizzano sull'errore umano incidentale, la security pone un'attenzione aggiuntiva e particolare sui gesti di origine dolosa.

E se è vero che come IC si pone nello scenario della sicurezza collettiva con delle specifiche preoccupazioni, è soprattutto vero che il nucleare è una delle attività industriali che investe di più nella sicurezza, supportata, tra le altre cose, da un programma regolato da rigidi protocolli operativi.

Gli elementi strutturali su cui si fonda un'efficace architettura di sicurezza nucleare si riassumono in:

- un efficiente sistema normativo e legislativo;
- misure di sicurezza e protezione degli impianti;
- misure di sicurezza della logistica, collegata ai materiali sensibili;
- un sistema di controllo e tracciabilità per rilevare i traffici illeciti di materiale nucleare/radioattivo (contaminato);
- adeguate risorse umane qualificate, sostenute da efficaci mezzi tecnologici; divulgazione della cultura della security tra gli attori dei processi.

Premessi questi concetti, intuiamo subito come una profonda protezione degli impianti nucleari si concretizza quando si attiveranno, in maniera integrata, più linee di difesa quali ad esempio: un'attenta prevenzione, una corretta rilevazione, un'immediata risposta. Di contro, sappiamo bene come applicate singolarmente, nessuna di queste azioni risulterebbe risolutiva. Peraltro, una strategia integrata rispondente alle minacce terroristiche richiede ben altro ancora, per dire: un approccio a più livelli che, da una parte, blocchi l'approvvigionamento e l'uso per fini terroristici di materiale/rifiuto nucleare o radioattivo ma che, dall'altra, sia in grado di monitorare, e perseguire efficacemente poi, le organizzazioni terroristiche. Sappiamo come il possesso ingiustificato di informazioni, di materiale, o di altri fonti radioattive, costituisce l'elemento centrale intorno a cui si sviluppa, appunto, la nuclear security: senza tali elementi materiali cadono le premesse al nuclear terrorism (terrorismo nucleare).

Ciò detto, osserviamo, allora, come la prevenzione, intervenendo alla fonte, rappresenti il focus della prima linea di difesa.

Contestualmente alle attività preventive, le azioni di rilevamento di trasferimenti/traffici illeciti di materiale nucleare/radioattivo attraverso le frontiere o all'interno di uno stato, delineano la seconda linea di difesa.

La terza linea di difesa è disegnata dalla pianificazione e dal coordinamento di una possibile crisi (delineando i possibili scenari di impatto), derivante dal danneggiamento degli impianti, dalla movimentazione e dall'uso illegale di materiali/componenti nucleari/radioattivi.

Analizzando quanto detto sin qui, appare del tutto evidente come la sicurezza nucleare raffiguri una delicata responsabilità di ogni singolo Stato; ma è la cooperazione internazionale la grossa opportunità per realizzare un'azione sinergica comune, su scala globale, di contrasto al fenomeno terroristico.

E su questo argomento troviamo diversi provvedimenti internazionali, adottati immediatamente dopo l'Undici Settembre, disposizioni alle quali l'Italia aderì per potenziare la sicurezza atomica nazionale, e come contromisura al contrasto e alla lotta al terrorismo verso i siti e gli impianti nucleari (seppur in via di smantellamento).

Sul nostro territorio nazionale abbiamo ancora diversi siti, tra impianti di ricerca e centrali di produzione dismesse; quattro centrali: a Trino (VC), Caorso (PC), Borgo Sabotino (LT) e Garigliano (CE); più quattro impianti di ricerca dedicati al ciclo del combustibile nucleare: Eurex di Saluggia (VC), Itrec di Rotondella (MT), Ipu e Opec nel centro della Casaccia (RM) e dell'impianto FN di Bosco Marengo (AL).

Siti ormai dismessi e in via di chiusura, per effetto delle scelte politiche legate al referendum sul nucleare, che cancellò definitivamente il progetto nazionale basato sul fabbisogno di produzione di energia elettrica che prevedeva lo sfruttamento del combustibile prodotto da queste centrali.

Tra l'altro, furono proprio tali politiche referendarie ad avviare il programma nazionale sul nucleare alla decommissioning (la rimozione del combustibile esaurito per procedere al suo riprocessamento) degli impianti atomici, quale fase ultima del loro ciclo di vita; una riconversione di settore che, ad oggi, ha superato i 15 mld di € di costi, per il mantenimento in sicurezza di queste strutture, l'allontanamento del combustibile nucleare esaurito, la decontaminazione e smantellamento delle installazioni, per la gestione e messa in sicurezza dei rifiuti radioattivi.

Da ciò si comprende come la dismissione, e lo smantellamento degli impianti atomici poi, rappresentano un'attività ad alto valore economico, sociale e ambientale, che impegnano tecnologie avanzate, e un know how specializzato; ma valgono, però, anche una componente di rischio e di grado molto elevato, con tipici risvolti di natura safety and security decisamente marcati. Ma a questi processi va aggiunto, tutto il ciclo dei rifiuti radioattivi prodotti sistematicamente dalle attività di medicina nucleare, industriali e di ricerca scientifica; materiale generalmente classificato come il meno impegnativo, ma che invece problematico è, considerato il loro possibile utilizzo negli ordigni improvvisati, i c.d IED-CBRNe (Improvised Explosive Device-Chemical, Biological, Radiological or Nuclear explosive), più comunemente conosciuti come bombe sporche: difendere gli impianti, proteggendo nel contempo i materiali/rifiuti nucleari, da azioni dolose, è la giusta prevenzione al terrorismo nucleare; tutto questo sempre nell'ottica preventiva di eliminare il rischio potenziale di poter realizzare un ordigno sporco.

È semplice perciò intuire come, in realtà, gli aspetti della security e quelli della safety, apparentemente separati, si tengano insieme: quale che sia la natura, accidentale o dolosa di un avvenimento, è invece lo stesso il risultato che ne deriva in termini di rischi per la società; difatti tutti gli elementi prodotti dalla dismissione dei siti atomici, ovvero i combustibili irraggiati, i rifiuti radioattivi solidi condizionati e non, quelli liquidi, i materiali attivati e/o contaminati, i materiali fissili e fertili e le sorgenti radioattive, costituiscono singolarmente, o come insieme, un elemento di rischio notevole. Come si vede, per garantire elevati livelli di sicurezza in infrastrutture così rilevanti, come gli impianti nucleari e/o i depositi di stoccaggio dei materiali/rifiuti, è necessaria un'attenta analisi degli scenari incidentali (scenari ideali per attacchi terroristici), perché sussistono elevati livelli di pericolosità dovuti a fattori di rischio specifici e ambientali, legati tanto al trattamento del materiale energetico, quanto al trasferimento e al deposito dello stesso.

Il raggiungimento di un elevato livello di sicurezza è la naturale conseguenza dell'applicazione di una metodologia sistematica che si crea durante la fase preliminare di progettazione, all'interno della quale va sviluppato un processo di analisi del rischio terrorismo sviluppato in 3 fasi primarie, e distinte:

- valutazione della minaccia (Treath Assessment);

- valutazione della vulnerabilità (Vulnerability Assessment);

- valutazione del rischio (Risk Assessment).

Per grandi linee possiamo riassumere come la fase del Treath Assessment identificherà e analizzerà le possibili condizioni di pericolo, in termini di potenziale aggressione, e la modalità d'attacco; mentre nella fase di Vulnerability Assessment si valuterà la vulnerabilità della infrastruttura, riferita allo scenario di attacco, così come le caratteristiche specifiche e/o le carenze dei sistemi di sicurezza fisico-logico; infine, la fase di Risk Assessment sintetizzerà, analiticamente e numericamente, i risultati ottenuti dall'analisi di ogni tipologia di attacco in termini di vulnerabilità delle strutture, e le possibili conseguenze.

Le ripercussioni trasversali collegate ad un attacco terroristico sono sempre misurate rapportandole a elementi considerati indicativi:

- la perdita di vite umane;

- il danno materiale;

- il danno economico

- il danno reputazionale;

- l'impatto negativo sull'opinione pubblica

Da queste preoccupazioni è facile intuire come la sicurezza nucleare cominci proprio dal mettere in atto tutte le primarie e funzionali misure legate alla sicurezza fisica (physical security), come dire, la capacità di una robusta protezione fisica perimetrale (antintrusione attiva e passiva, contro degli accessi, videosorveglianza, tracciabilità dei movimenti di cose e persone all'interno delle aree protette, etc), specifiche procedure e policy operative, sistema di comunicazioni delle emergenze, assetto delle risorse assegnate alla vigilanza interna, contatti e collaborazione operativa con le FF.OO.

Piani di sicurezza particolareggiati (safety e security) per la protezione delle risorse umane più esposte, e che conoscono le peculiarità e le vulnerabilità infrastrutturali.

Una misura di sicurezza quest'ultima che non è così stravagante come si potrebbe pensare, tant'è vero che alcune agenzie d'intelligence sono convinte che gli attentati di Parigi e Bruxelles del 2016, altro non siano altro che un test apripista, per una serie di attacchi terroristici di più ampia portata, proprio contro gli asset nucleari. Il sospetto che il nucleo eversivo avesse come obiettivo la centrale nucleare era concreto, e si è concentrato proprio sugli attentati di Bruxelles del marzo 2016. Secondo gli analisti dell'intelligence, i piani della cellula terroristica franco-belga sarebbe saltato a causa dell'arresto di uno dei terroristi, e del rinvenimento il giorno successivo agli attentati di Parigi, di un file video definito interessante dagli stessi agenti; registrazioni in cui i componenti del commando monitoravano gli spostamenti di un esperto nucleare belga, operativo all'interno della centrale; imprevisti che avrebbero spinto poi il commando a optare per obiettivi più facili, l'aeroporto e il metrò, anticipando peraltro, gli attacchi di oltre una settimana rispetto alla pianificazione iniziale.

L'altra criticità tipicamente fisica emersa negli ultimi anni, è rappresentata dalla miniaturizzazione degli esplosivi, dall'espansione e l'uso sempre più globale di sistemi SAPR (sistemi di aeromobili a pilotaggio remoto), sistemi droni sempre più performanti, ma che costituiscono un altro importante elemento di rischio aggiuntivo per la sicurezza dei siti nucleari. Un drone armato con materiale esplosivo potrebbe essere pilotato verso le piscine di raffreddamento delle barre di combustibile esaurito; parliamo di strutture edili che non sono state progettate per resistere a esplosioni di una certa entità.

Sulla falsa riga dei SAPR, non dobbiamo sottovalutare un altro possibile vettore utilizzabile come strumento di penetrazione: uno attacco attivato mediante l'utilizzo di un aeromobile dirottato (World Trade Center insegna), che fatto precipitare volontariamente sul sito attiverebbe il rischio di un incidente nucleare.

Ma un efficace, quanto efficiente, programma di security deve essere opportunamente integrato a un funzionale protocollo di sicurezza logica (logical security), che protegga il sistema dall'altro tipo di minacce tipicamente informatiche (hackeraggi, worm, accesso illegale ai dati, ai sistemi scada che governano gli impianti, etc).

Infatti, negli odierni scenari di rischio, in cui la minaccia assume sempre più la caratterizzazione asimmetrica, la minaccia cyber sta diventando la tipologia predominante di eventi malevoli contro le IC, ed in particolare di tutte quelle in cui vi è la presenza di agenti CBRNe (Chimici, Biologici, Radiologico-Nucleari ed esplosivi), come ad esempio negli insediamenti industriali nucleari.

In questi siti la sicurezza informatica assume un ruolo predominante, una funzione diretta a ridurre la vulnerabilità, e nel contempo, aumentarne la capacità resiliente.

Infatti, tutto il complesso insieme dei sistemi logici che assicurano il sicuro funzionamento di una centrale nucleare, devono appartenere a un sistema di tipo chiuso separato dal mondo web, utilizzando specifici dispositivi hardware di isolamento. Non solo: gli impianti parti integrante dei sistemi di security e safety viaggeranno su rete dati chiusa, fisicamente e logicamente scollegata dalla rete infrastrutturale, in modo tale da essere insensibili e protetti da qualsiasi cyber-attacco basato sulla rete, proveniente dall'esterno.

Altra difesa chiave, quale contrasto alle cd minacce interne, è rappresentata dal severo controllo sull'uso dei device portatili (smartphone, tablet, notebook, etc), utilizzati per interfacciarsi con le apparecchiature operanti all'interno dei siti atomici; in questo specifico caso la formazione continua e l'osservazione comportamentale delle risorse che lavorano con apparecchiature digitali interfacciate agli impianti, è di vitale importanza nell'esercizio della sicurezza informatica.

Un altro aspetto insostituibile nel settore dell'energia nucleare, e parte fondamentale del programma di sicurezza cd cyber, è la condivisione continua delle informazioni con le agenzie governative di intelligence, per prevenire specifiche azione di hackeraggio funzionali agli attacchi distruttivi verso i sistemi SCADA-PLC (worm Stuxnet).

Ora, tutto ciò detto ci porta ad affermare, in linea di principio generale, come i molteplici livelli di protezione applicati agli insediamenti nucleari fin qui descritti, e che vanno dall'isolamento funzionale dei sistemi rispetto al web, fino alla gestione e controlli tecnici sulle risorse tecniche e su quelle umane, rappresentano concretamente una sufficiente politica di prevenzione dalle minacce provenienti da cd cyberspazio.

Dando poi uno sguardo agli eventi del settore avvenuti in questi ultimi anni, abbiamo un quadro di insieme più chiaro a riprova di come la sicurezza nucleare vada gestita.

Gli incidenti hanno fatto scuola in un'epoca in cui si generano, ogni giorno, oltre 300.000 nuovi sample di malware: la prima offensiva cyber ai danni di una IC CBRNe si registrò nella metà degli anni novanta; ma il reale problema emerse nella sua complessità agli inizi del 2002, quando la centrale nucleare Ohio's Davis-Besse fu l'obiettivo di un attacco cyber a causa del quale il virus Slammer disattivò per cinque ore il sistema di monitoraggio dei parametri di sicurezza, con l'impossibilità di controllare il corretto funzionamento dell'intera struttura.

Poi fu la volta di un impianto atomico tedesco, infettato (tramite chiavette USB) da diversi malware tra cui W32.Ramnit e Conficker, ma fortunatamente i sistemi della centrale erano isolati dal collegamento esterno al web, di conseguenza non si verificarono particolari problemi funzionali; altro esempio fu un attacco a una centrale statunitense, che portò una turbina al blocco operativo, dopo che un dipendente inserì nella sua postazione di lavoro una chiavetta USB risultata poi infetta da migliaia di virus, infezione che attaccò gli impianti di governo (SCADA) della turbina stessa.

E' perciò evidente, in ultima analisi, come gli asset nucleari siano fortemente esposti al rischio hacker. Abbiamo visto come negli ultimi tempi si sono materializzati diverse aggressioni cyber in danno di infrastrutture atomiche, in varie parti del mondo, per fortuna sventati: ma ciò non significa che non ce ne saranno altri.

La recente escalation di minacce informatiche a livello globale portate a termine con ransomware tipo WannaCry, PetYa e le sue varianti, tanto per citarne altri ancora, dimostrano come tali attacchi siano stati malevolmente efficaci, nonostante le rassicurazioni del caso, e che tutto era sotto controllo.

Eppure è accaduto di nuovo.

domande?

ivan.rizzolo@unipd.it