VALUTAZIONE PROBABILISTICA DELLA VULNERABILITÀ DI INFRASTRUTTURE CRITICHE LOCALI AD ATTACCHI INTENZIONALI

Squellati G.,[1] e Contini S.[2]
1. **Consulente, Via Poerio 9, Busto Arsizio (VA), 21052**
2. **Commissione Europea, Centro Comune Ricerca, Via E. Fermi 1, Ispra (VA), 21020**

SOMMARIO

La valutazione della sicurezza di infrastrutture critiche richiede l'impiego di metodologie sistematiche per la identificazione dei potenziali attaccanti, per il calcolo della frequenza di attacco, per la determinazione della vulnerabilità dell'infrastruttura e delle conseguenze degli eventi causati. L'analisi di sicurezza, ossia di protezione dell'infrastruttura, richiede l'uso di metodologie sistematiche in grado di fornire tutti gli elementi necessari per una presa di decisioni. Le metodologie consolidate per l'analisi di rischio di impianti nucleari e chimici richiedono adattamenti per la loro applicazione alla soluzione di problemi di security. L'obiettivo del presente lavoro è mostrarre, per mezzo di un semplice esempio, come le note metodologie dell'Albero dei Guasti e Albero degli Eventi possono essere applicate per la quantificazione probabilistica di sequenze di attacco.

1.0 INTRODUZIONE

Nei Paesi industrializzati una qualsiasi installazione il cui guasto possa comportare danni ingenti alla popolazione e/o all'ambiente e' sottoposto ad una approfondita analisi di rischio. A partire dalla fine degli anni '90 l'attenzione agli aspetti di sicurezza è cresciuta notevolmente, in particolare dopo l'11 settembre 2001 ed i successivi attentati a Madrid e a Londra.

Security Risk (SR) è il termine entrato recentemente in uso per indicare di rischio di incidente in infrastrutture critiche dovuto ad azioni umane deliberate. Pertanto le attività relative a studi di Security hanno l'obiettivo di raggiungere un adeguato livello di protezione dell'infrastruttura. Rispetto all'analisi di rischio da incidenti causati da eventi random, nella security risk l'aspetto importante è l'analisi della vulnerabilità dell'infrastruttura ad attacchi esterni, il che richiede l'identificazione dei potenziali obiettivi dell'attacco, lo studio degli scenari di attacco e la valutazione dell'adeguatezza delle difese esistenti. Essenziale è la determinazione della probabilità di attacco, problema delicato che richiede l'identificazione degli attaccanti, delle loro motivazioni, degli obiettivi più appetibili.

Per l'analisi di vulnerabilità le metodologie per l'analisi di sicurezza dei sistemi, quali l'albero degli eventi e l'albero dei guasti, sono certamente applicabili, ma devono essere opportunamente adattate.

Per l'identificazione dei possibili scenari di attacco è stato recentemente proposto l'Attack Tree derivato dall'albero dei guasti. Il Top event è relativo al successo dell'attacco a un particolare obiettivo; gli eventi primari rappresentano le azioni deliberate di sabotaggio, il malfunzionamento dei sistemi di sicurezza, le azioni degli addetti alla sicurezza. Le combinazioni di guasto minime altro non sono che gli scenari di attacco. Ogni scenario di attacco viene poi esaminato mediante l'albero degli eventi con il quale possono essere rappresentate le diverse sequenze di attacco. La quantificazione di tali sequenze, nelle quali occorre considerare la durata delle azioni e l'intervento dei servizi di sicurezza, richiede metodi probabilistici più complessi di quelli correntemente utililizzati.

Nel presente lavoro si mostra, con riferimento a un semplice esempio, come le sequenze di attacco potrebbero essere quantificate per individuare i punti relativamente più critici del sistema di sicurezza. Tale esempio sarà preceduto da un breve esame dello stato dell'arte e delle metodologie utilizzabili.

La metodologia che ne deriva può essere facilmente implementata in uno strumento informatico di supporto basato su piattaforma GIS in grado di integrare il layout dell'infrastruttura con i risultati della modellistica per la quantificazione della vulnerabilità e delle conseguenze.

2.0 BREVE STATO DELL'ARTE

2.1 Il quadro metodologico per la Security Risk.

Security Risk è il nuovo termine che contraddistingue l'analisi di rischio in cui gli eventi iniziatori di sequenze incidentali sono azioni umane eseguite deliberatamente allo scopo di provocare conseguenze gravi. Le differenze fra Risk (R) e Security Risk (SR) sono facilmente individuabili partendo dalle loro formulazioni.

Il rischio R e' definito come danno incerto:

R = Σ_i probabilità incidente i-esimo x danno conseguente all'i-esimo incidente.

Generalmente l'entità' del danno e' inversamente proporzionale alla probabilità di incidente. Scenari incidentali ad alta probabilità presentano danni limitati; scenari con più gravi conseguenze corrispondono a minori probabilità di accadimento.

Il rischio da attacchi intenzionali è invece definito come:

SR = Σ_i probabilità attacco i-esimo x vulnerabilità infrastruttura all'attacco i-esimo x danno conseguente all'i-esimo attacco.

Analogamente all'analisi di rischio da incidente rilevante possiamo porci le seguenti domande:

- Quale attacco può essere presumibilmente portato alla infrastruttura?
- Da parte di chi, per quali motivi?
- Con quale probabilità?
- Qual e' la vulnerabilità della struttura, ossia la probabilità di successo dell'attacco?
- Quali le conseguenze?

Da queste considerazioni possiamo concludere che:

- la relazione di proporzionalità inversa tra la probabilità e le conseguenze, propria di R, potrebbe non valere per SR poiché presumibilmente l'obiettivo di un attacco consisterà nel provocare il massimo danno cercando di far verificare proprio gli incidenti con conseguenze più elevate. Avremmo in queste ipotesi probabilità di incidente non trascurabili associate a danni ingenti.
- la probabilità di incidente di SR e' determinata dalla frequenza dell'attacco e dalla vulnerabilità dell'infrastruttura.
- la probabilità di attacco in SR e' difficilmente determinabile, diversamente dalla probabilità di incidente in R dovuta a malfunzionamenti e errori umani
- la vulnerabilità dell'infrastruttura ad azioni intenzionali è maggiore della stessa ai malfunzionamenti
- contrastare un incidente causato da guasti casuali o errori umani (R) richiede una gestione dell'emergenza diversa da quella necessaria in caso di attacco all'infrastruttura (SR). Infatti, nel primo caso l'emergenza avviene quando l'incidente è già accaduto e si cerca di limitarne le conseguenze. Nel secondo caso l'emergenza potrebbe iniziare prima e consentire di evitare l'incidente bloccando gli attaccanti. Di conseguenza diventa importante quantificare la probabilità di successo di un attacco tenendo conto delle azioni dei servizi di sicurezza e dell'intervento delle forze dell'ordine.
- R e SR hanno in comune la quantificazione del danno.

Come per l'analisi di rischio anche per la sicurezza la metodologia di analisi dipende dal tipo di struttura, dalla sua complessità, dalle modalità di funzionamento, ecc. Le differenze concettuali e metodologiche fra R e SR non devono tuttavia far pensare a due analisi distinte in quanto entrambi gli aspetti sono relativi alla protezione dell'infrastruttura. Occorrerà quindi definire un'unica metodologia che integri gli aspetti di rischio con quelli di sicurezza e la cui applicazione garantisca il raggiungimento di un adeguato livello di protezione.

I requisiti generali di una qualsiasi metodologia consistono nella "credibilità" e nella "comparabilità".

Una metodologia è definita "credibile" se indirizza l'analisi delle conseguenze, della vulnerabilità e dei possibili attacchi attraverso i principi della risk e vulnerability analysis, se è *completa*, nel qual caso deve fornire risultati quantitativi, e se è *difendibile*, e cioè se impiega metodi di analisi universalmente riconosciuti nell'ambito delle discipline professionali.

Una metodologia è "comparabile" se è *documentata*, *trasparente* (facilmente comprensibile), se consente a persone esterne di *riprodurre e verificare* i risultati, e se è *accurata*, e cioè se non contiene errori od incompletezze logiche, e se costituisce un reale strumento per la presa di decisioni.

Nella bibliografia specialistica pubblicata nei tempi più recenti sono state presentate diverse proposte metodologiche derivate dalle metodologie già largamente applicate per le analisi di rischio. Il primo studio autorevole sull'estensione dei metodi della risk analysis alla Security Risk è stato pubblicato nel 2004 [1]. Altre organizzazioni hanno proposto metodi sistematici per l'analisi di vulnerabilità, alcuni calati sulle specificità dei vari settori, come ad esempio quello petrolifero (SVA – Security Vulnerabilità Assessment Method) di API (American Petroleum Institute) e NPRA (National Petrochemical & Refiners Association) [2], o quello chimico (VAM-CF, Vulnerability Assessment Methodology for Chemical Facilities, o RAMCAP (Risk Analysis Method for Critical Asset Method), presentata da ASME [3], ed altre ancora, che forniscono un preciso quadro metodologico, spesso completo di modulistica e check list. Altre metodologie sono state messe a punto per altri tipi di infrastrutture, come ad esempio le reti elettriche e le reti informatiche [4].

Le metodologie proposte di fatto suddividono le attività da svolgere durante uno studio di Security Risk nelle seguenti fasi:

- Analisi delle infrastrutture considerate: il risultato di questa fase e' l'elenco dei possibili obiettivi (targets), identificando:
  - le parti critiche e potenzialmente più soggette ad attacchi,
  - le "contromisure" esistenti (sistemi di sicurezza, barriere passive, presidio di personale addetto alla sicurezza) in grado di prevenire o mitigare gli attacchi
  - la "severità" degli impatti di possibili attacchi, in termini sia economici che di conseguenze per l'uomo e per l'ambiente.
- La definizione dei possibili aggressori. Questa fase, fondamentale per lo studio, richiede un'analisi delle motivazioni di eventuali gruppi terroristici o criminali che si ritengono potenzialmente interessati ad attaccare l'infrastruttura e comprende:
  - la definizione del tipo di aggressori
  - la caratterizzazione degli aggressori
  - le tipologie di obiettivi preferiti dagli aggressori, nel contesto dell'infrastruttura considerata
- L'analisi di vulnerabilità, che comprende:
  - la definizione di possibili scenari di attacco, e la valutazione delle possibili conseguenze
  - la valutazione dell'efficacia degli attuali sistemi di sicurezza
  - la valutazione e la quantificazione della vulnerabilità
- Security Risk Assessment, in termini di:
  - valutazione dei risultati di ogni attacco considerando sia le conseguenze che la vulnerabilità
  - valutazione dell'opportunità di rafforzare le contromisure esistenti
- Analisi per il rafforzamento delle contromisure, che consiste nella:
  - Identificazione delle varie opzioni di miglioramento della sicurezza
  - valutazione della riduzione del rischio per ciascuna opzione
  - valutazione delle varie opzioni in funzione di un'analisi di costo e di efficacia.

In funzione dei risultati potrebbe essere necessario ritornare alle fasi precedenti per rivedere e migliorare il livello di security, con l'implementazione di misure atte a dissuadere gli aggressori,

anticipare le loro decisioni, ritardare le loro azioni e reagire per tempo, allo scopo di prevenire l'incidente e/o minimizzare i danni.

2.2 Metodi, Tecniche e modelli applicabili per la valutazione della Vulnerabilità.

Come visto, la Security Risk Analysis di una determinata infrastruttura locale richiede la individuazione dei targets (obiettivi) e la *definizione dei corrispondenti scenari* di attacco, dei quali si valuta la *probabilità di successo* delle azioni svolte dagli aggressori in funzione *degli interventi degli addetti alla sicurezza* e dei *sistemi di protezione e di allarme*.

Per un determinato target possono essere individuati uno o più scenari di attacco. Uno scenario è costituito da una o più sequenze di attacco e dall'insieme di azioni intraprese dal "sistema" aggredito per difendersi. Una sequenza è pertanto costituita da un insieme ordinato di eventi successo / insuccesso associati alle azioni svolte dagli attaccanti, dagli addetti al presidio della sicurezza, dallo stato dei sistemi di sicurezza esistenti. Infine per quantificare gli effetti derivanti da ciascuna sequenza si debbono determinare le probabilità di accadimento e le possibili conseguenze.
Per formalizzare uno scenario occorre quindi impiegare strumenti che permettano di descrivere lo spettro delle sequenze di attacco e di contro-reazione, e per ciascuna di esse determinare i tempi, valutare le conseguenze e quantificare le probabilità di successo.

Le tecniche, universalmente riconosciute nel campo della safety e risk analysis, che si possono impiegare per la determinazione *"logica"* delle sequenze di attacco e di contro-reazione dei servizi di sicurezza, consistono nei noti metodi deduttivi (es. Master Logic Diagram, introdotti in campo nucleare per la individuazione degli eventi iniziatori di sequenze incidentali; Albero dei guasti), e induttivi (es. Albero degli Eventi, Diagrammi Cause Conseguenze, utilizzati per la descrizione dell'articolazione logica delle sequenze considerando il successo/insuccesso dei sistemi di protezione e mitigazione). Tuttavia questi metodi devono essere opportunamente modificati per tener conto dei tempi di esecuzione delle azioni da parte degli aggressori, dei tempi di reazione dei servizi/sistemi di sicurezza, oltre a considerare indicatori per valutare la convenienza, da parte di un aggressore, di attaccare un particolare target.

Un recente adattamento dell'albero dei guasti nel campo della security per la descrizione delle possibili modalità di attacco è l'Attack Tree [5, 6].

Si definisce Attack Tree un albero dei guasti nel quale il Top event è relativo al successo dell'attacco a un particolare obiettivo. Gli eventi primari rappresentano azioni deliberate di sabotaggio, malfunzionamento dei sistemi di sicurezza, azioni degli addetti alla sicurezza, ecc. A ciascun evento primario, relativo ad un'azione deliberata, può essere associata non solo la probabilità di accadimento, ma anche altri indicatori quali la durata dell'azione, la necessità di fare uso di strumenti particolari, il costo, ecc. Di conseguenza oltre gli operatori logici AND e OR è possibile utilizzare diversi operatori matematici. In un attack tree vi possono essere azioni mutualmente esclusive la cui modellizzazione corretta richiede l'introduzione dell'operatore NOT.

Il complemento dell'albero dei guasti fornisce la probabilità di successo del sistema di sicurezza; il complemento dell'attack tree fornisce la probabilità di successo del sistema di protezione, che comprende sia l'organizzione dei servizi, sia i sistemi preposti alla salvaguardia della security.

L'analisi logica di un attack tree può essere effettuata utilizzando metodi diversi in funzione della disponibilità di programmi di calcolo in grado di analizzare solo alberi AND-OR o anche alberi con eventi negati. Tali metodi sono descritti in [7]. L'analisi logica fornisce tutti i possibili scenari di successo dell'attacco. Tali scenari (equivalenti ai Minimal Cut Set di un albero dei guasti) possono essere caratterizzati mediante specifici indicatori (es. probabilità, costo attrezzature, grado di difficoltà, tempo totale di esecuzione, ecc.).
L'analisi critica degli scenari consente di ricavare utili indicazioni sugli scenari più "convenienti" per gli attaccanti, e quindi più probabili, e sul livello di vulnerabilità dell'infrastruttura.

L'analisi probabilistica fornisce la probabilità del verificarsi dei possibili scenario di attacco.

Il valore esatto del Top event rappresenta allo stesso tempo la probabilità di successo dei possibili attacchi e la probabilità di insucesso del sistema di protezione. Qualora si disponesse di un programma in grado di calcolare esclusivamente i due bounds (upper , lower) allora occorrebbe porre molta attenzione nel trarre conclusioni nell'interpretazione dei risultati.
Infatti, il lower bound (valore probabilistico minore del valore esatto) è cautelativo dal punto di vista del successo dell'attacco (cautelativo per l'aggressore) e non cautelativo dal punto di vista della protezione. Viceversa l'upper bound (valore probabilistico maggiore del valore esatto) è cautelativo per la valutazione dell'adeguatezza del sistema di sicurezza ed invece non lo è per l'aggressore.
Anche con l'Attack Tree è possibile eseguire analisi di importanza degli eventi primari allo scopo di individuare i punti relativamente più critici del sistema di sicurezza.

L'aleatorietà dei tempi di esecuzione delle attività umane, che può essere trascurata in una prima fase dell'analisi, deve necessariamente essere considerata per il calcolo della probabilità di successo di un attacco. Purtroppo i modelli solitamente utilizzati in risk analysis non sembrano efficacemente applicabili, in quanto non supportano distribuzioni di probabilità diverse dall'esponenziale, che mal si presta alla rappresentazione della variabilità di azioni umane, che viene normalmente descritta attraverso distribuzioni di tipo Log-normale o Gamma.
Pertanto per la quantificazione delle sequenze di attacco dovranno essere applicati altri modelli, per esempio quelli basati sulla teoria della trasformazione delle variabili stocastiche (metodi di convoluzione) o altri equivalenti.

3.0 ESEMPIO DI ANALISI DI VULNERABILITA'

In questo esempio illustreremo come si possano applicare i principi sopra esposti per la quantificazione della vulnerabilità con riferimento ad un caso semplice, ma concreto, rappresentato da un'aggressione ad un Terminal Container Portuale, svolta da una organizzazione di trafficanti di armi.

3.1 Il caso di considerato

Assumeremo che l'organizzazione criminale abbia spedito armi all'interno di un container che é stato sbarcato da una nave, e che si trova nel depositato della zona doganale di temporanea custodia del Terminal (Piazzale Inbound). La Figura 1 mostra il layout della struttura. I documenti doganali del container denunciano un carico di rottami di ferro. L'organizzazione intende trasferire nottetempo le armi, prima che vengano effettuate le ispezioni da parte della guardia di Finanza, dalla zona di temporanea custodia all'esterno dell'area doganale, in un uno dei container vuoti depositati nel Piazzale di Export (Piazzale Outbound) non soggetto a controlli.

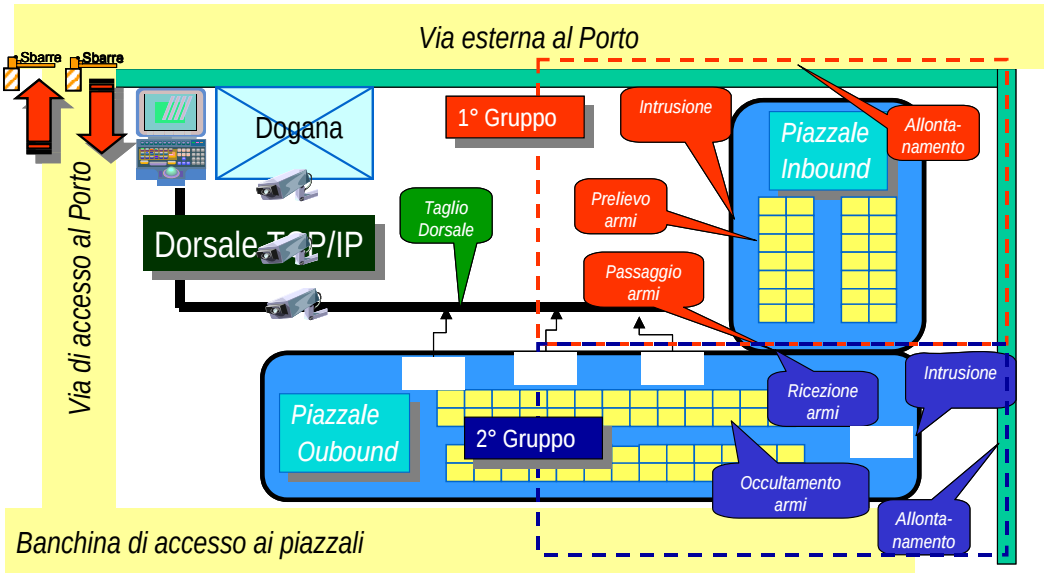

Figura 1. Layout dell'infrastruttura di riferimento.

Da questo piazzale i containers vuoti, su richiesta di un cliente, vengono prelevati su automezzi, escono dal porto, giungono presso il cliente, vengono caricati di merce e ritrasferiti in porto per essere spediti. L'intento dell'organizzazione consiste nell'asportare le armi dal container, fuori dal porto, prima che lo stesso arrivi al cliente.

3.2 L'analisi della infrastruttura

Il Piazzale di Temporanea Custodia, nel quale vengono sbarcati i container è adiacente al Piazzale di Export nel quale vengono depositati i container in attesa di imbarco e quelli vuoti in attesa di prelievo. Le due aree sono delimitate da cancellate alte 3 metri.

Presso il terminal container è installato un sistema di video-sorveglianza, basato su videocamere digitali, in parte fisse ed in parte brandeggiabili. Le telecamere sono posizionate sul perimetro all'interno dei piazzali, in modo che lo stesso punto sia osservabile da più di una telecamera, e collegate con le postazioni di monitoraggio attraverso una dorsale a fibra ottica.

Sono previste due postazioni operatore, la prima presso gli uffici della società che gestisce il Terminal Container, che è presidiata da personale interno nell'orario di svolgimento delle operazioni, la seconda presso la Postazione del Presidio della Guardia di Finanza (GdF) situata nel varco di ingresso/uscita del porto, che è permanentemente presidiata.

3.3 Esame dei possibili scenari di attacco

L'evento di interesse è l'asportazione di armi dal porto. Si assumono le seguenti ipotesi semplificative:

- l'organizzazione criminale è informata sulla natura del sistema di video-sorveglianza, ed è quindi consapevole che qualsiasi manomissione di una sua componente genera allarme;
- è in possesso dell'informazione sul posizionamento del container nel piazzale di temporanea custodia;
- il sistema di video-sorveglianza è funzionante al momento dell'attacco;
- l'azione di sabotaggio della dorsale provoca l'allarme con probabilità 1;
- l'allarme è segnalato presso la postazione della GdF ubicata all'entrata del porto.

Assumiamo che lo scenario di attacco sia stato individuato mediate l'uso di una metodologia deduttiva (Attack tree). Dall'albero si possono individuare tre fasi sequenziali che presumibilmente saranno realizzate da altrettanti gruppi operanti secondo un piano che minimizza la durata totale dell'intera operazione.

Si studierà pertanto uno scenario nel quale si ipotizza che l'organizzazione criminale decida di dividere le forze in tre parti: un gruppo saboterà il sistema di sicurezza, in modo da rendere impossibile l'osservazione dell'azione degli altri due gruppi che effettueranno il prelievo ed il trasferimento delle armi, operando rispettivamente nel Piazzale Export e nel piazzale di Temporanea Custodia Doganale. In particolare:

- Il gruppo incaricato del sabotaggio del sistema di sicurezza:
  - accederà ad un punto, esterno all'area dei piazzali e fuori dal campo visivo normale delle telecamere, nel quale è possibile sabotare la dorsale di rete.
  - interromperà la dorsale di rete: di conseguenza verranno eliminate le funzioni di monitoraggio, ma la logica di sistema emetterà subito un allarme.
  - si allontanerà.
- Il gruppo che opera nel piazzale di temporanea custodia
  - Scavalcherà la recinzione del piazzale di temporanea custodia (tempo medio stimato:2 minuti)
  - Raggiungerà il container e ne aprirà i sigilli (tempo medio stimato: 4 minuti)
  - Asporterà le armi e le porterà al recinto che separa il piazzale di temporanea custodia da quello di export, consegnandole al gruppo che opera in questo piazzale (tempo medio stimato: 6 minuti)

- Scavalcherà il recinto che separa il piazzale di temporanea custodia da una pubblica via, retrostante alla zona portuale, e si allontanerà (tempo medio stimato: 4 minuti)

o Il gruppo che opera nel piazzale export:
- Scavalcherà la recinzione del piazzale export (tempo medio stimato 2 minuti)
- Raggiungerà il punto di contatto convenuto con il primo gruppo, presso il recinto che separa le due zone (tempo stimato: 6 minuti)
- Resterà in attesa del contatto con il primo gruppo (tempo medio stimato: 6 minuti)
- Riceverà le armi dal primo gruppo, e le posizionerà all'interno di un determinato container vuoto (tempo medio stimato: 8 minuti)
- Scavalcherà il recinto che separa il piazzale da una pubblica via, retrostante alla zona portuale, e si allontanerà (tempo medio stimato 4 minuti).

Le varie fasi dello scenario di attacco sono ricavate a partire dall'Attack Tree e schematizzate nella Figura 2 (in forma di diagramma di Gannt), nella quale sono riportati i tempi richiesti dalle attività di ciascun gruppo di attacco e la loro fasatura:

Azioni	Tempo di azione (minuti)										
	2	4	6	8	10	12	14	16	18	20	22
Interruzione dorsale											
1° Gruppo Piazzale Temporanea Custodia											
o Scavalcamento											
o Raggiungimento container e rimozione sigilli											
o Trasferimento armi											
o Allontanamento											
2° Gruppo piazzale Export											
o Scavalcamento											
o Posizionamento											
o Attesa nel punto di contatto											
o Ricezione e caricamento armi container											
o Allontanamento											

Figura 2. Diagramma dei tempi di esecuzione delle diverse fasi di attacco.

3.4 Lo scenario dell'intervento del servizio di vigilanza

Lo scenario di intervento del servizio si sorveglianza si articola nelle seguenti attività:

o All'insorgere dell'allarme, che costituisce l'evento iniziatore delle possibili sequenze di attacco e difesa, l'addetto alla postazione della GdF:
- impiega mediamente 2 minuti per interpretare la situazione che gli viene segnalata dall'allarme.
- impiega mediamente 1 minuto per richiedere l'intervento delle Forze dell'Ordine
- Le Forze dell'Ordine intervengono sul posto mediamente dopo 12 minuti, senza conoscere esattamente cosa sia accaduto ed iniziano le ispezioni dei due piazzali.

Complessivamente le forze dell'ordine iniziano le ricerche mediamente dopo 15 minuti dall'allarme. Queste azioni si articolano come illustrato nel diagramma di Gannt di Figura 3.

Azioni	Tempo di azione (minuti)														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Addetto alla guardiania															
o Interpretazione dell'allarme															
o Chiamata forze dell'Ordine															
Forze dell'Ordine															
o Intervento presso il Terminal															

Figura 3. Diagramma dei tempi di intervento.

3.5 La costruzione dell'albero degli eventi

Per brevità di trattazione considereremo in questa sede, solo le sequenze di attacco del gruppo che opera nel piazzale di temporanea custodia e quella del servizio di vigilanza.

Le Sequenze di attacco

Riassumiamo le azioni che il gruppo che opera sul Piazzale di Temporaneoa Custodia deve compiere:

- accesso al piazzale
- raggiungimento del container pieno e rimozione sigilli
- trasferimento armi nel piazzale di export
- allontanamento e uscita dall'area portuale

Assumiamo, per semplicità di esposizione, che il solo errore che il gruppo possa compiere derivi da una errata informazione sul posizionamento del container nel piazzale. Ipotizziamo anche che la probabilità di questo evento sia del 20% e che per ritrovare il container contenente le armi sia necessaria una attività addizionale di ricerca di 5 minuti.

In questa ipotesi si individuano due serie di sequenze, la prima che comprende la 4 attività sopra elencate, la seconda che, oltre a queste, contiene l'attività addizionale di ricerca per ritrovare il container contenente le armi.

Le sequenze del servizio di vigilanza

Le attività che devono essere svolte dal servizio di vigilanza, a seguito dell'emissione di un allarme da parte del sistema di sicurezza, sono invece:

- Interpretazione dell'allarme
- Chiamata forze dell'Ordine
- Intervento delle stesse presso il Terminal

Per semplicità di trattazione assumiamo che il servizio di vigilanza non possa compiere significativi errori nello svolgimento dei suoi compiti, e che quindi il suo intervento blocchi l'azione di attacco nel 100% dei casi

L'albero degli eventi

L'albero degli eventi dovrà descrivere, oltre agli eventi considerati nelle due sequenze dello scenario di attacco, l'intervento delle forze dell'ordine:

- prima dell'accesso al piazzale,
- prima dell'apertura del container,
- prima del passaggio delle armi nel piazzale di export,
- prima dell'uscita dall'area portuale del gruppo attaccante

La Figura 4, che descrive l'albero degli eventi per il caso considerato, riporta nelle colonne gli eventi considerati, e sulle righe le possibile combinazioni di eventi, le conseguenze ed il tempo medio di esecuzione.

Nella testata della tabella sono riportati i valori dei tempi medi delle azioni di attacco; i tempi medi delle sequenze si differenziano a partire dalla colonna relativa alla attività di ricerca del container non trovato, che, come visto, riguarda solo la seconda sequenza di attacco, per la quale le combinazioni di eventi sono descritte nel riquadro azzurro riportato in basso a destra della figura. Le conseguenze derivanti dallo spettro di sequenze considerate nell'event tree consistono nel pieno successo dell'attacco, nell'arresto del gruppo di criminali senza che le forze dell'ordine abbiano la possibilità di comprendere il motivo dell'attacco, e nell'arresto del gruppo e contemporaneo sequestro delle armi.

3.6 Calcolo delle probabilità

Consideriamo una generica sequenza di attacco: il suo tempo di realizzazione è dato dalla somma di tempi di completamento di ciascuna attività; i tempi di esecuzione delle azioni sono di fatto variabili

di tipo aleatorio, caratterizzate da un propria funzione di densità di probabilità (fdp) tipicamente di tipo lognormale, gamma.

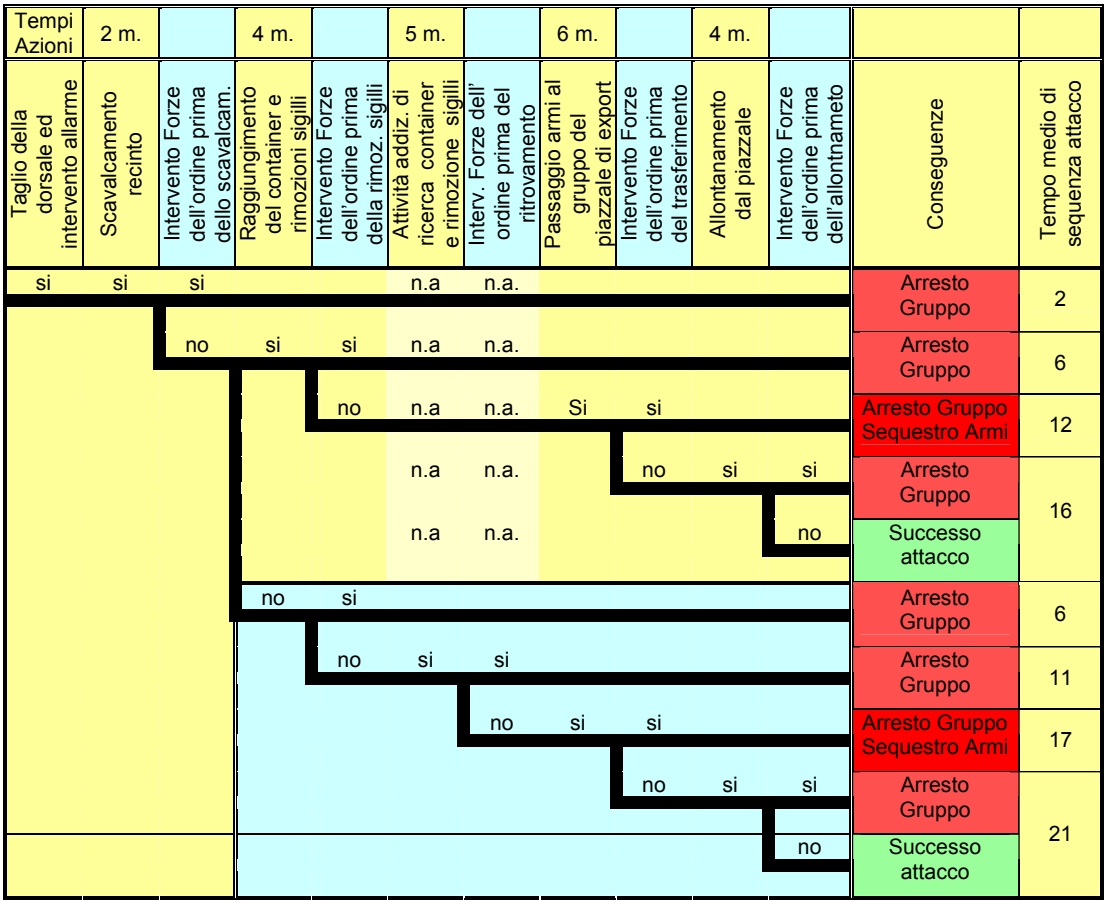

Figura 4. Event tree dello scenario di attacco.

I tempi di realizzazione di ciascuna sequenza sono a loro volta una variabile aleatoria, la cui fdp può essere determinata, a partire da quelle dei tempi delle singole attività, applicando il metodo di convoluzione, che è costituito da un caso particolare del più generale metodo di trasformazione delle variabili. Ad esempio, nel caso di una sequenza costituita da due azioni i cui tempi di realizzazione siano detti x ed y, denominate f(x) e g(y) le rispettive fdp, la fdp della variabile somma z = x+y è data dalla seguente formula:

$$h(z) = \int_0^z f(x)\, g(z-x)\, dx \quad (\text{per } z>0)\ ; \qquad h(z) = 0 \text{ per } z < 0$$

In generale la risoluzione dell'integrale di convoluzione non ammette soluzioni analitiche chiuse, ma richiede l'applicazione di metodi numerici o di simulazione Monte-Carlo. Tuttavia per alcuni casi specifici, la fdp della variabile z = x + y assume forma analitica: ad esempio, qualora x ed y abbiano fdp normale, la fdp. della loro somma è anch'essa di tipo normale.

Inoltre ricordiamo che, di qualunque tipo siano le fdp dei tempi di realizzazione delle singole attività, valgono le seguenti regole:

- la media della somma dei tempi delle attività corrisponde alla somma dei tempi medi delle attività. Questi tempi medi e le relative somme si possono determinare automaticamente impiegando gli strumenti GIS oggi disponibili per rappresentare il lay-out dettagliato del sito e gli itinerari percorsi dagli attaccanti durante le sequenze di attacco.
- la deviazione standard della somma dei tempi delle varie attività, corrisponde alla radice quadrata della somma dei quadrati delle deviazioni standard dei tempi delle singole attività.

Tenendo conto di quanto sopra esposto, per semplificare la trattazione del calcolo delle probabilità delle varie sequenze assumeremo che la fdp dei tempi delle azioni svolte dal gruppo di attaccanti e dal servizio di vigilanza siano di tipo normale, con deviazione standard pari al 30% del valore medio. Nella Tabella 1 sono riportati i valori medi e le deviazioni standard delle attività e quelle delle sequenze, calcolate con le regole sopra riportate:

Tabella 1. Tempi medi e deviazioni standard delle attività e delle sequenze.

	Tempi delle attività		***Tempi delle sequenze***	
	Valore medio	*Deviazione standard*	*Valore medio*	*Deviazione standard*
Prima sequenza di attacco				
Scavalcamento recinto	2	0,6	2	0,6
Raggiungimento del container e rimozione sigilli	4	1,2	6	1,34
Passaggio armi al gruppo del piazzale di export	6	1,8	12	2,24
Allontanamento dal piazzale	4	1,2	16	2,55
Seconda sequenza di attacco				
Scavalcamento recinto	2	0,6	2	0,6
Mancato raggiungimento del container	4	1,2	6	1,34
Ricerca container non trovato	5	1,5	11	2,01
Passaggio armi al gruppo del piazzale di export	6	1,8	17	2,70
Allontanamento dal piazzale	4	1,2	21	2,95
Sequenza del servizio di vigilanza				
Interpretazione situazione al Posto di Guardia	2	0,6	2	0,6
Attivazione delle stazioni FF.OO	1	0,3	3	0,67
Intervento sui Piazzali	12	3,6	15	3,66

A questo punto abbiamo a disposizione tutti i parametri richiesti per il calcolo delle probabilità di successo di ciascuna singola sequenza di attacco, che è definita come:

P = P (tempo sequenza attacco < tempo intervento servizio di vigilanza) =

= P [(tempo sequenza attacco – tempo intervento servizio di vigilanza) < 0]

= 1- P [(tempo sequenza attacco – tempo intervento servizio di vigilanza) > 0]

Per le ipotesi fatte sulla fdp dei tempi di ciascuna singola azione, la fdp dei tempi delle sequenze considerate sarà di tipo normale.

Quindi per il metodo di convoluzione, che si applica anche a differenze di variabili stocastiche, la probabilità di successo di ciascuna sequenza sarà a sua volta di tipo normale:

$$P = 1 - \int_0^{\infty} \text{Norm}\,[\text{Med}(\text{Tsa}-\text{Tsr}), \text{Dev}(\text{Tsa}, \text{Tsr})]\,dt = 1 - \int_0^{\infty} [\,1 / (\sqrt{2\pi}\,\sigma)\,]\, e^{-[(t-\mu)/\sigma]^2/2}\,dt$$

dove:

- P = Probabilità della sequenza
- Norm = Funzione di densità di probabilità Normale
- Tsa = tempo della sequenza di attacco considerata nello specifico scenario
- Tsr = tempo di intervento delle Forze dell'Ordine
- Med (Tsa-Tsr) = μ = valore medio di Norm, corrispondente alla differenza tra il tempo medio di Tsa e di Tsr
- Dev (Tsa, Tsr) = σ = deviazione standard di Norm = $\sqrt{\sigma^2(\text{Tsa}) + \sigma^2(\text{Tsr})}$
- σ(Tsa), σ(Tsr) = deviazioni standard del tempo della sequenza di attacco considerata e del tempo di intervento delle Forze dell'Ordine

I valori delle probabilità associati agli eventi compresi nell'albero degli eventi dello scenario considerato sono riportati nella Tabella 2.

Tabella 2. Probabilità associate agli eventi dell'event tree in figura 4.

Eventi	Descrizione enenti	Parametri		Probabilità
		μ	σ	
Prima sequenza di attacco				
1	Taglio della dorsale	-	-	**1**
2	Scavalcamento recinto	-		**1**
3	Intervento delle F.O. prima dello scavalcamento	-13	3,71	**0.0002**
4	Raggiungimento del container e rimozione sigilli			**0,8**
5	Intervento delle F.O. prima dall'apertura sigilli del container	- 9	3,90	**0,0105**
6	Passaggio armi al gruppo del piazzale di export			**1**
7	Intervento delle F.O. prima del passaggio armi tra il 1° e 2° gruppo,	- 3	4,30	**0,2425**
8	Allontanamento dal piazzale			**1**
9	Intervento delle F.O prima dell' allontanamento del 1° gruppo	1	4,46	**0,5887**
Seconda sequenza di attacco (attività da 1 a 5 e da 8 a11). Attività 6,7 alternative a 4,5				
1	Taglio della dorsale	-	-	**1**
2	Scavalcamento recinto	-	-	**1**
3	Intervento delle F.O. prima dello scavalcamento	-13	3,71	**0.0002**
4	Raggiungimento del container e rimozione sigilli			**0,2**
5	Intervento delle F.O. prima dall'apertura sigilli del container	- 9	3,90	**0,0105**
6	Attività addizionale di ricerca del container e rimozione dei sigilli			**1**
7	Intervento Forze dell'ordine prima del completamento dell'attività addizionale	-4	4,18	**0,1692**
8	Passaggio armi al gruppo del piazzale di export			**1**
9	Intervento delle F.O. prima del passaggio armi tra il 1° e 2° gruppo,	2	4,55	**0,6699**
10	Allontanamento dal piazzale			**1**
11	Intervento delle F.O prima dell' allontanamento del 1° gruppo	6	4,71	**0,8989**

Infine, associando le probabilità riportate nella precedente tabella all'albero degli eventi di figura 4, vengono calcolate le probabilità complessive delle varie combinazioni di eventi. Il risultato finale è riportato in figura 5.

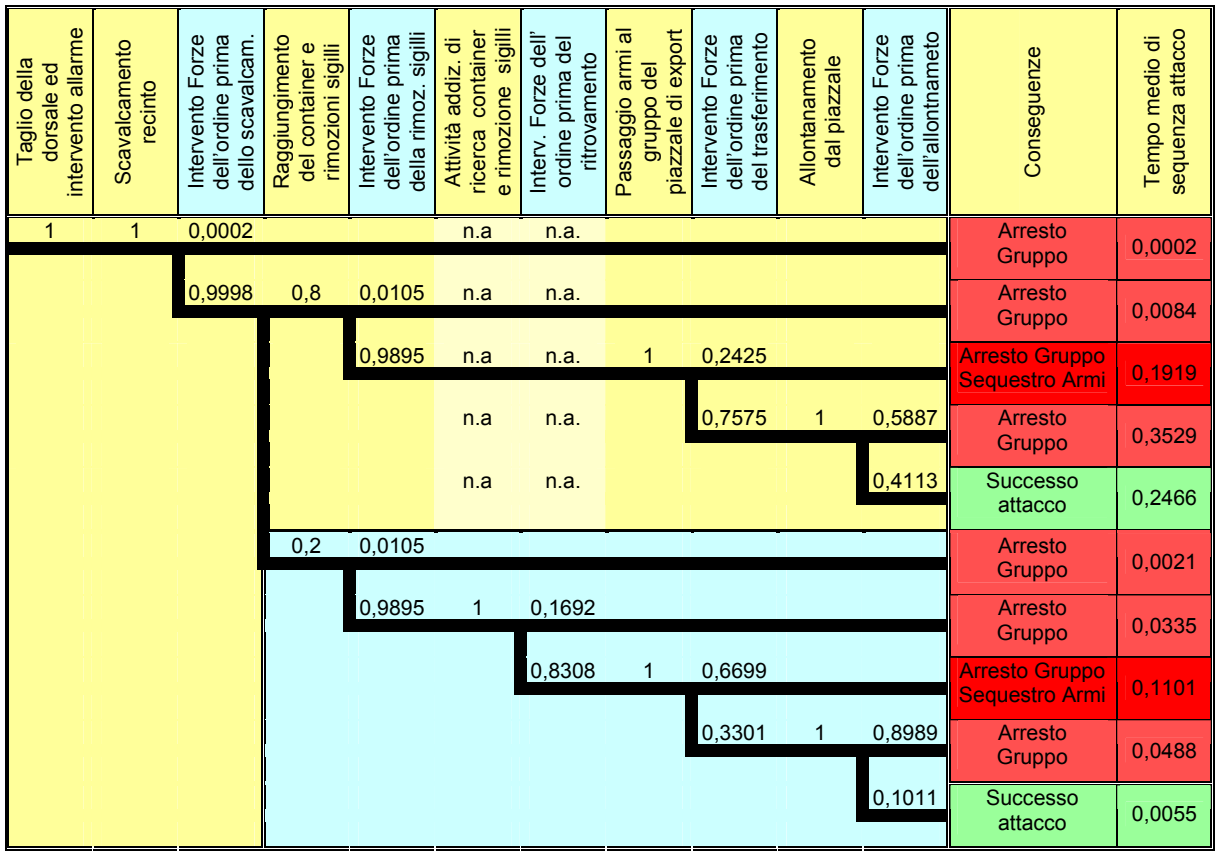

Figura 5. Risultati della quantificazione dello scenario di attacco.

3.7 Analisi dei risultati

Dall'analisi effettuata appare evidente che l'attacco ipotizzato può portare a 3 differenti esiti:

- Il pieno successo dell'attacco, ottenuto dal Gruppo, con probabilità di circa il 25 %
- L''insuccesso dell'attacco, con l'arresto del gruppo durante l'azione, con probabilità di circa il 45 %
- Il completo insuccesso dell'attacco con l'arresto del gruppo ed il sequestro delle armi, con probabilità di circa il 30 %

La probabilità di successo dell'attacco fornisce una misura oggettiva della vulnerabilità della infrastruttura considerata, e costituisce il punto di partenza per le successive analisi di valutazione delle opportunità di miglioramento della sicurezza, che sono tuttavia fuori dello scopo di questa trattazione.

4.0 PUNTI APERTI ED ULTERIORI SVILUPPI

Il presente articolo costituisce il punto di partenza di un programma di attività che, auspicabilmente anche con l'apporto di organizzazioni industriali, dovrà consentire di raggiungere i seguenti obiettivi:

- Completamento e sistematizzazione dell'impostazione metodologica per la valutazione della vulnerabilità
- Adattamento degli strumenti esistenti per la modellazione logica alla rappresentazione di sequenze temporali
- Adattamento di strumenti GIS per la rappresentazione grafica delle infrastrutture locali e delle azioni svolte dagli attaccanti e dal servizio di vigilanza
- Sviluppo o potenziamento di strumenti per il calcolo numerico delle probablità delle sequenze, e loro integrazione con gli strumenti di modellazione logica
- Test di metodologie e strumenti su di casi reali in ambito industriale.

RIFERIMENTI BIBLIOGRAFICI

1. Garrick, B.J. et. al., Confronting the risk of terrorism: making the right decision, ReliabilityEgineering and System Safety, 86, 2004, pp. 129-176.

2. Moore D.A., Application of the API/NPRA SVA methodology to transportation security issues, Journal of Hazardous Materials, 130, 2006, 107-121

3. REMCAP, Risk Assessment Methodology for Critical Assets Protection, www.asme.org

4. Masera M, Nai Fovino I., Sgnaolin R., A Framework for teh Security Assessment of Remote Control Applications of Critical Infrastructures, ESReDA 29th Seminar, Systems Analysis for a More Secure World. Application of System Analysis and RAMS to Security of Complex Systems, 2005, JRC, Ispra, Italy.

5. Pullen, R., Attack Tree+ - A Computer Tool for Modelling Attack Scenarios, ESReDA 29th Seminar, Systems Analysis for a More Secure World. Application of System Analysis and RAMS to Security of Complex Systems, 2005, JRC, Ispra, Italy.

6. Nicol, M.D., Trivedi K.S., Model Based Evaluation: from Dependability to Security, IEEE Transaction on Dependable and Secure Computing, 1, No. 1, 2004, 48-65.

7. Cojazzi, G.G.M., Contini, S., Renda, G., FT Analysis in Security related Applications: Challenges and Needs, ESReDA 29th Seminar, Systems Analysis for a More Secure World. Application of System Analysis and RAMS to Security of Complex Systems, 2005, JRC, Ispra, Italy.