Elementi di CYBERSECURITY e CYBERINTELLIGENCE
Angelo Gaeta, 13/02/2023

Università degli Studi di Salerno
agaeta@unisa.it

Sommario

Intelligence: finalità, obiettivi e processi

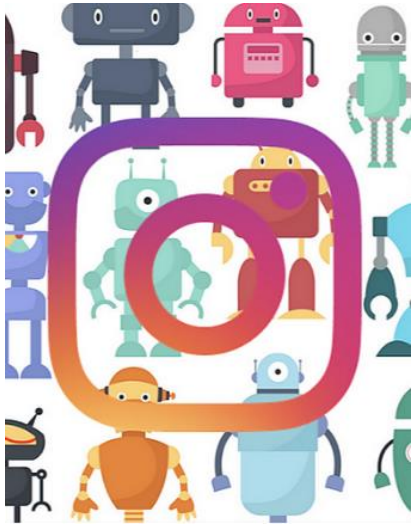
Tecniche di Analisi Strutturata per cyber-intelligence e cyber-security

I fattori determinanti nei conflitti del XXI Secolo

Networks: le nuove forme di comunicazioni e le tecnologie dell'informazione hanno avuto un forte impatto sulle strutture, le dottrine e le strategie militari. Sono stati coniati termini quali *netwar ed hybrid war*.

I gruppi criminali, ribelli e terroristici hanno le proprie reti che conducono attività economiche, politiche e militari su scala globale. La loro capacità di accedere a finanziamenti, armi avanzate ecc. li rende attori potenti negli affari internazionali, più potenti di molti stati. Anche la loro abilità nell'adattarsi ai mutevoli ambienti e alle minacce supera quella della maggior parte dei governi.

La netwar si è spostata sui **social media**, che sono diventati un potente strumento per ottenere un vantaggio nei conflitti. È nota l'operazione russa per influenzare le elezioni presidenziali statunitensi del 2016.



Netwar - Definizione

Azioni intraprese da governi o **attori non statali** organizzati per distorcere il sentimento politico nazionale o estero, più frequentemente per ottenere un risultato strategico e/o geopolitico.

Queste operazioni possono utilizzare una combinazione di metodi, come notizie false, disinformazione o reti di account falsi (**amplificatori**) volti a manipolare l'opinione pubblica.

Attori non statali

Molte reti, coinvolte nei conflitti recenti, sono composte da attori non statali: gruppi criminali, imprese commerciali, ecc.

Alcune imprese commerciali, ad esempio, si dedicano al traffico illecito di armi, sostengono il traffico di stupefacenti e facilitano il riciclaggio di denaro.

Questi gruppi operano con proprie regole e norme che differiscono notevolmente dalle regole tradizionali osservate dai governi.

Strumenti di conflitto

Sono state riconosciute quattro leve (**DIME**) ampiamente utilizzate e applicate anche in modalità innovative da attori non statali:

- Diplomatica (o politica)
- Informativa
- Militare
- Economica

Sinergia tra le leve

Gli interessi dell'intelligence oggi non sono strettamente militari

Quasi tutti i tipi di conflitto fanno uso di dimensioni diplomatiche, economiche e informative, solitamente applicate in modo sinergico

Sinergia tra le leve: un esempio basato sui negoziati tra le potenze occidentali e l'Iran sulla limitazione del programma di armi nucleari iraniano nel 2014-2015

Entrambe le parti hanno sviluppato coalizioni politiche per il sostegno, con gli Stati Uniti, le potenze europee, diversi paesi del Medio Oriente e alcune ONG da una parte; e dall'altro gli iraniani, i russi e alcune ONG.

Le leve economiche includevano embarghi commerciali contro l'Iran. L'Iran, a sua volta, ha utilizzato i suoi legami economici e politici per eludere in una certa misura le sanzioni.

Entrambe le parti hanno utilizzato lo strumento informativo per raccogliere sostegno politico e sociale: le potenze occidentali si sono concentrate sui timori di un Iran dotato di armi nucleari e il governo iraniano, da parte sua, ha alimentato la rabbia contro gli Stati Uniti e ha fatto appello all'orgoglio iraniano per l'indipendenza dalle pressioni straniere.

I negoziati si sono conclusi con un accordo nucleare raggiunto nel 2015 tra l'Iran e sei potenze mondiali: Stati Uniti, Regno Unito, Russia, Francia, Cina e Germania.

Riepilogo

Il contesto che abbiamo delineato da vita a scenari operativi complessi

- Compresenza di reti attori statali e non statali
- Uso di reti
- Confluenza di diversi domini (cielo, terra, mare, cyber…)
- Uso sinergico degli strumenti (leve)

Tali scenari sono caratterizzati da elevata incertezza

Intelligence

Ha l’obiettivo di *ridurre l'incertezza nei conflitti*.

- Poiché il conflitto può consistere in qualsiasi azione competitiva o contraria risultante dalla divergenza delle idee o degli interessi di due o più parti, non include necessariamente la guerra fisica.
- Se esiste concorrenza o negoziazione, allora due o più gruppi sono in conflitto.

Ridurre l'incertezza richiede l’acquisizione di informazioni che l'avversario preferisce nascondere. Questa definizione non esclude l'uso di fonti pubblicamente disponibili, come i supporti cartacei (giornali e riviste) o Internet.

L'intelligence, in generale, può essere pensata come il complesso processo di **comprensione del significato delle informazioni disponibili**. Un tipico obiettivo dell'intelligence è stabilire fatti e quindi sviluppare inferenze precise, affidabili e valide (ipotesi, stime, conclusioni o previsioni) da utilizzare nel processo decisionale strategico o nella pianificazione operativa.

Intelligence

Il cliente principale dell'intelligence è la persona che agirà in base alle informazioni e ad i report che un’analista le/gli fornirà:

- l'esecutivo
- il decisore
- il comandante in un combattimento
- l'ufficiale delle forze dell'ordine.

L'intelligence può essere anche definita come *actionable information*.

- Ma non viceversa (e.g., un report delle previsioni metereologiche non è intelligence)

Ciò che distingue l'intelligence dalle semplici notizie è il supporto alle operazioni. Il cliente fa (o dovrebbe fare) qualcosa in risposta all'intelligence.

Le stesse informazioni possono essere sia intelligence che notizie.

Intelligence Analysis

Processo per la trasformazione dell'informazione «grezza» in intelligenza «finale».

- Le informazioni sono semplicemente dati grezzi di qualsiasi tipo
- L'intelligenza si ottiene processando i dati (i.e., tramite una valutazione) per attribuire loro un valore aggiunto o un significato.

INFORMATION + EVALUATION = INTELLIGENCE

- L'intelligenza ottenuta deve supportare il decision-making

Intelligence Analysis

Capacità di collezionare, processare ed interpretare dati sensibili riguardo un obiettivo.

Non è connessa soltanto ad operazioni di spionaggio o agenzie governative.

- Analisti di intelligence sono richiesti anche nel settore privato, ad esempio, per attività di business intelligence.

Un professionista di intelligence analysis sfrutta le informazioni raccolte per predire il comportamento futuro del proprio obiettivo target.

I ruoli dell'Intelligence

09 AGOSTO 2021 12:10

Covid, nelle mani dell'intelligence americana 22mila documenti sui segreti di Wuhan

Un catalogo enorme di informazioni che, una volta decifrate, serviranno a fare chiarezza sull'ipotesi della fuga accidentale del virus

How open-source intelligence is disrupting statecraft

Our weekly podcast on the science and technology making the news. This week: John Brennan, a former director of the CIA, on how open-source techniques affect secret intelligence

CHINA'S SILOS: NEW INTELLIGENCE, OLD PROBLEMS

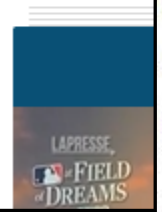
Gli attacchi informatici sono sempre di più

In molti se ne sono accorti dopo il caso della Regione Lazio, ma le cose peggiorano da tempo: e ora il governo ha creato un'Agenzia per la cybersicurezza nazionale

Talebani inarrestabili, l'intelligence Usa: «Kabul può cadere in 90 giorni»

di Lorenzo Cremonesi

La capitale afghana invasa da migliaia di profughi. Biden ribadisce: «Il Paese deve difendersi da solo»



Intelligence e controlli mirati contro stragi lavoro

Arriva rifroma Ispettorato. Giordano, guerra infinita.Orlando,azione è priorità

Redazione ANSA

ROMA

Intelligence Analyst

La funzione principale dell'analista può essere suddivisa in un processo di tre fasi:

- Raccolta delle informazioni, interpretazione e comprensione della rilevanza o relazione tra di esse.
- Sviluppo oggettivo delle informazioni per arrivare a una comprensione complessiva.
- Comunicazione della comprensione maturata agli altri e quindi messa in pratica del processo di intelligence.

Più informazioni vengono raccolte, più l'analisi e il processo decisionale migliorano.

- Tuttavia, aumenta anche il carico di lavoro successivo, che a sua volta costringe a un aumento del personale e della produttività o a una perdita di efficacia.

Tipologie di raccolta dei dati

Osint (*Open Source intelligence* – attività di raccolta delle informazioni mediante l'analisi di fonti aperte)

Imint (*Imagery intelligence* – attività di raccolta delle informazioni mediante l'analisi di fotografie aeree o satellitari)

Humint (*Human intelligence* – attività di raccolta delle informazioni mediante contatti interpersonali)

Sigint (*Signal intelligence* – attività di raccolta delle informazioni mediante l'intercettazione e analisi di segnali, sia tra persone sia tra macchine)

Techint (*Technical intelligence* – riguardante armi ed equipaggiamenti militari)

Masint (*Measurement and Signature intelligence* – attività di raccolta delle informazioni non classificabili nelle precedenti categorie)

OSINT

https://www.youtube.com/watch?v=g5UHijJ_Jo0

OSINT- Challenges

Impatto delle leggi sulla sicurezza dei dati

Filtraggio dei contenuti

Elevata quantità di dati da validare e potenzialmente scartabile

Sfide geopolitiche

Problematiche relative alle indagini

Solitamente, la guida iniziale che i clienti forniscono agli analisti su un problema risulta a ***grana grossa, spesso incompleta e può anche essere involontariamente fuorviante***.

Ci sono alcune domande preliminari a cui è necessario rispondere all'inizio di un progetto:

1. ***Chi è il cliente?*** Identificare i clienti dell'intelligence e cercare di capire le loro esigenze. Il processo tradizionale di comunicazione dei bisogni in genere coinvolge diversi intermediari, tanto da generare inevitabili distorsioni. Ciò può essere evitato tramite un'interazione diretta con il cliente.
2. *Qual è lo scopo?* Gli sforzi di intelligence di solito hanno uno scopo principale che dovrebbe essere chiaro a tutti i partecipanti (compreso il cliente). Ad esempio, lo scopo potrebbe essere quello di fornire informazioni per supportare i negoziati commerciali tra gli Stati Uniti e l'Unione Europea. Un certo numero di scopi di intelligence più specifici supportano questo principale, come identificare probabili tattiche negoziali e individuare problemi che potrebbero dividere i negoziatori avversari o minare il loro sostegno popolare. Ancora una volta, il coinvolgimento del cliente aiuta a chiarire lo scopo principale.

Problematiche relative alle indagini

3. *Quali sono le vere richieste?* Ottenere quante più conoscenze di base possibili per capire il problema e come esso influisce sulle decisioni politiche o operative. Una richiesta di informazioni formulata in modo vago è solitamente fuorviante e il risultato non sarà quasi mai quello che il cliente desiderava.
4. *Quando è necessaria la risposta?* Determinare quando il prodotto deve essere consegnato. Nel tradizionale ciclo di intelligence, molti report vengono consegnati troppo tardi, molto tempo dopo che sono state prese le decisioni che hanno generato la necessità, in parte perché il cliente è isolato dal processo. ***L'approccio incentrato sul target può ridurre drasticamente il tempo*** necessario per fornire al cliente informazioni fruibili perché il cliente è parte del processo.
5. ***Quale forma di output o prodotto sarà più efficace****?* I rapporti scritti (in formato elettronico) sono standard nel settore dell'intelligence perché persistono e possono essere distribuiti prontamente a più clienti. Quando il risultato va a un singolo cliente o è estremamente sensibile, un briefing verbale può essere la forma di output. I briefing hanno il vantaggio dell'interazione e del feedback del cliente, insieme alla certezza che il destinatario previsto riceva il messaggio.

Una volta risposto a tali quesiti, ci si potrà concentrare più facilmente sulla risposta alle richieste del cliente. Ma una buona definizione del problema richiede due ulteriori passaggi: **definizione** e **scomposizione**.

Clienti - Tipologie

La varietà di clienti dell'intelligence è cresciuta costantemente nel corso dell'ultimo secolo rispetto ai due gruppi tradizionali (leadership nazionale e militare), fino ad includerne un insieme diversificato.

Negli Stati Uniti, dall'11 settembre, le forze dell'ordine e le squadre di risposta alle emergenze, ad esempio, sono diventate clienti abituali dell'intelligence.

In molti paesi, come la Cina e la Francia, le società commerciali sono i principali clienti dell'intelligence commerciale fornita dal governo a causa del vantaggio competitivo che tale intelligence offre loro a livello internazionale.

Clienti – Pricipali *concern* dei clienti

La maggior parte dei clienti ha un'idea dei punti di forza e di debolezza interni della propria struttura, anche se spesso *un'idea distorta*

La loro incertezza di solito riguarda le **opportunità** che hanno e le **minacce** che devono affrontare. I clienti a livello nazionale, le forze dell'ordine e i leader aziendali tendono tutti a **concentrarsi sulle minacce** nel guardare l'intelligence, a causa della loro pervasiva paura della sorpresa

Ma l'intelligenza serve anche (ed, in alcuni casi, meglio) quando può fornire un’idea delle **opportunità**

Clienti - Policymakers

I clienti d'élite dell'intelligence nazionale sono generalmente i decisori politici («policymaker»).

Generalmente i «policymaker» lavorano in ***condizioni di forte pressione***. Hanno bisogno di intuizioni analitiche di qualità che li aiutino ad affrontare problemi complessi, spesso in un breve lasso di tempo.

Molti decisori politici setacciano le informazioni disponibili, selezionando quegli elementi che supportano il loro «mindset».

Un problema insidioso in questo senso è che i subordinati del cliente (inclusi sia gli analisti che gli intermediari) potrebbero essere tentati di assecondarlo.

Un potenziale problema nel rapporto cliente-analista: frame effect

La maggior parte dei politici (ma non solo di tale categoria) è abbastanza competente nell'applicare il **frame effect** quando pone le domande, in modo da ottenere le risposte desiderate.

E’ inteso che, nei processi comunicativi, se la domanda è mal definita in anticipo, anche la migliore delle analisi successive non aiuterà.

Inoltre, anche se non è il cliente ad «inquadrare» deliberatamente la domanda, gli analisti inesperti possono incapparvi a causa della scarsa comunicazione.

Un potenziale problema nel rapporto cliente-analista: frame effect

La maggior parte dei politici (ma non solo di tale categoria) è abbastanza competente nell'applicare il **frame effect** quando pone le domande, in modo da ottenere le risposte desiderate.

E' inteso che, nei processi comunicativi, se la domanda è mal definita in anticipo, anche la migliore delle analisi successive non aiuterà.

Inoltre, anche se non è il cliente ad «inquadrare» deliberatamente la domanda, gli analisti inesperti possono incapparvi a causa della scarsa comunicazione.

Cosa è il Frame Effect?

Un potenziale problema nel rapporto cliente-analista: frame effect

Il modo in cui viene rappresentato un problema ha influenza sulla decisione che prenderà un individuo

Un individuo risponde in maniera differente a differenti descrizioni dello stesso problema, nonostante siano perfettamente equivalenti in termini di payoff e di probabilità di ottenere tale payoff

- *E, di conseguenza, richiederebbero una decisione identica*

Questo fenomeno viene denominato framing effect

Un potenziale pericolo nel rapporto cliente-analista: frame effect

Nel decision making caratterizzato da rischio, (Kahneman- Tversky, 1984) riportano il seguente esempio:

Gli Stati Uniti devono affrontare una strana malattia, che in media ucciderà 600 persone. Vengono proposti due programmi differenti per intervenire, le cui conseguenze sono le seguenti

If Program A is adopted, 200 people will be saved. (72%)

If Program B is adopted, there is a one-third probability that 600 people will be saved and a two-thirds probability that no people will be saved. (28%)

Problem 2 ($N = 155$): If Program C is adopted, 400 people will die. (22%)

If Program D is adopted, there is a one-third probability that nobody will die and a two-thirds probability that 600 people will die. (78%)

Un potenziale problema nel rapporto cliente-analista: frame effect

Nel decision making caratterizzato da rischio, (Kahneman- Tversky, 1984) riportano il seguente esempio:

Gli Stati Uniti devono affrontare una strana malattia, che in media ucciderà 600 persone. Vengono proposti due programmi differenti per intervenire, le cui conseguenze sono le seguenti

If Program A is adopted, 200 people will be saved. (72%)

If Program B is adopted, there is a one-third probability that 600 people will be saved and a two-thirds probability that no people will be saved. (28%)

Problem 2 (N = 155): If Program C is adopted, 400 people will die. (22%)

If Program D is adopted, there is a one-third probability that nobody will die and a two-thirds probability that 600 people will die. (78%)

Clienti - Leadership Militare

L'establishment militare degli Stati Uniti ha molti clienti per l'intelligence strategica, perché molte organizzazioni all'interno del Dipartimento della Difesa, dei capi di stato maggiore congiunti e dei servizi conducono la pianificazione strategica.

I clienti militari di solito sono chiari su cosa vogliono dall'intelligence. L'intelligenza è parte integrante del loro mondo; sono abituati a vederne e comprenderne il valore. Tuttavia, i leader militari, come i politici, variano notevolmente nell'articolazione delle esigenze.

Clienti - Leader aziendali

I clienti aziendali, come i politici, affrontano pressioni costanti e sono orientati all'azione. ***Ma poiché i dirigenti aziendali pagano direttamente gli analisti, sono più inclini a fornire una guida specifica e a prestare attenzione al prodotto analitico. Sono anche più inclini a rimproverare l'analista per gli scarsi risultati.***

In generale, il supporto alla strategia aziendale riguarda questioni quali acquisizioni; identificazione di nuovi mercati o tendenze nei mercati esistenti; sviluppo di prodotti; e valutazione di minacce da parte di concorrenti ed elementi criminali.

Processo di analisi: Overview

L’analisi delle informazioni è eseguita tramite un **processo** che può essere utilmente scomposto in una serie di fasi, o domande da porsi:

- Qual è esattamente il **problema**; quale decisione dobbiamo prendere e perché risulta significativa?
- Quali informazioni abbiamo già o potremmo ragionevolmente ottenere e che potrebbero essere **rilevanti** per il problema in questione? Dove si trovano/come possiamo ottenerle?
- Quale significato possiamo estrarre dalle informazioni? Cosa ci dicono rispetto a quello che sta accadendo?
- C'è solo una possibile spiegazione o ci sono altre alternative o opzioni. Alcune sono più probabili di altre?
- In che modo queste influiscono sulla decisione che dobbiamo prendere? Alcune opzioni sono potenzialmente migliori di altre? Alcune comportano un rischio maggiore di successo e/o fallimento?
- Siamo pronti ad agire con un **ragionevole livello di fiducia** o dobbiamo prima raccogliere maggiori informazioni? In tal caso, di cos'altro abbiamo bisogno e dove/come possiamo ottenerlo?

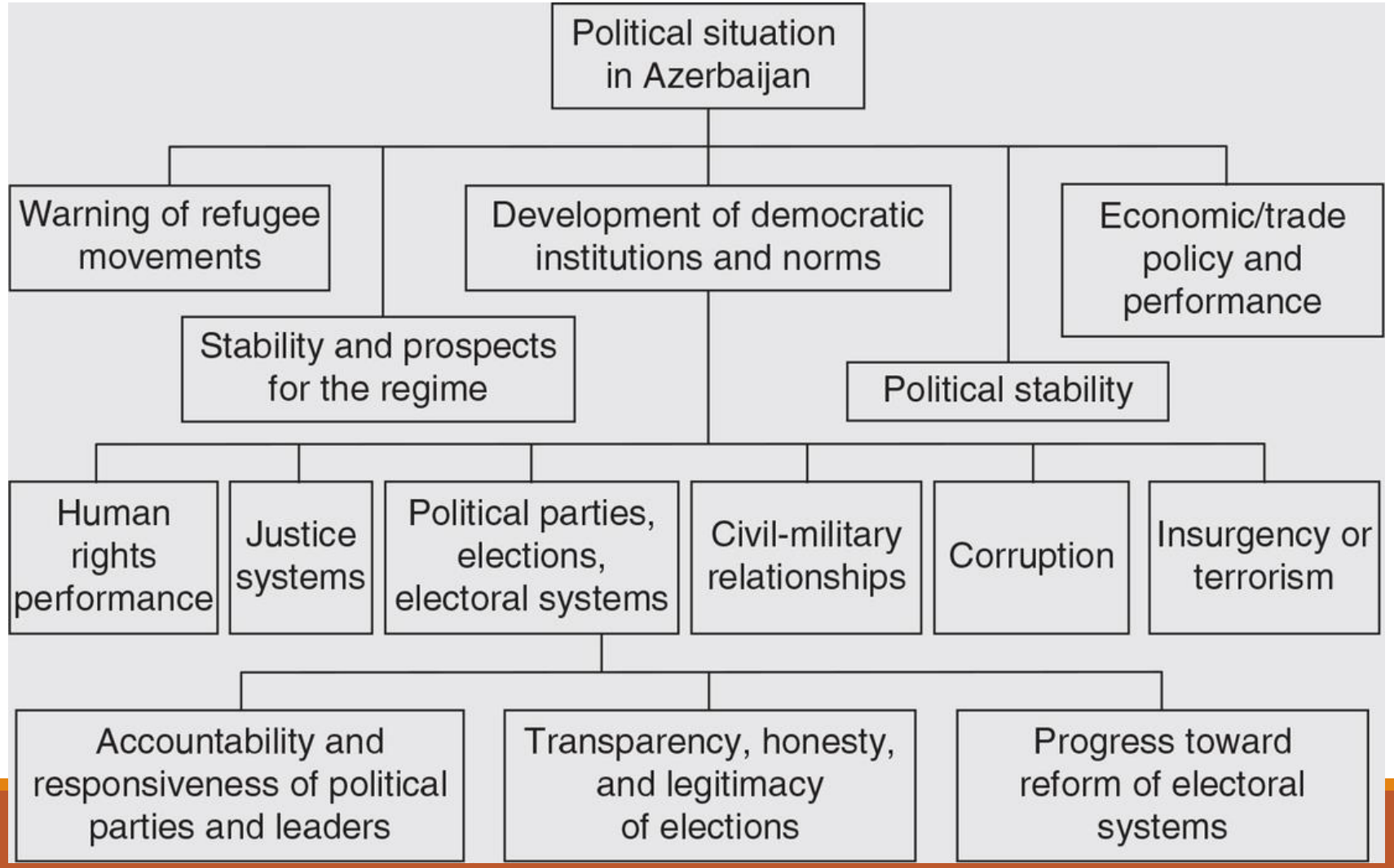
Scomposizione del Problema – Esempio Situazione Politica

Domanda del cliente:

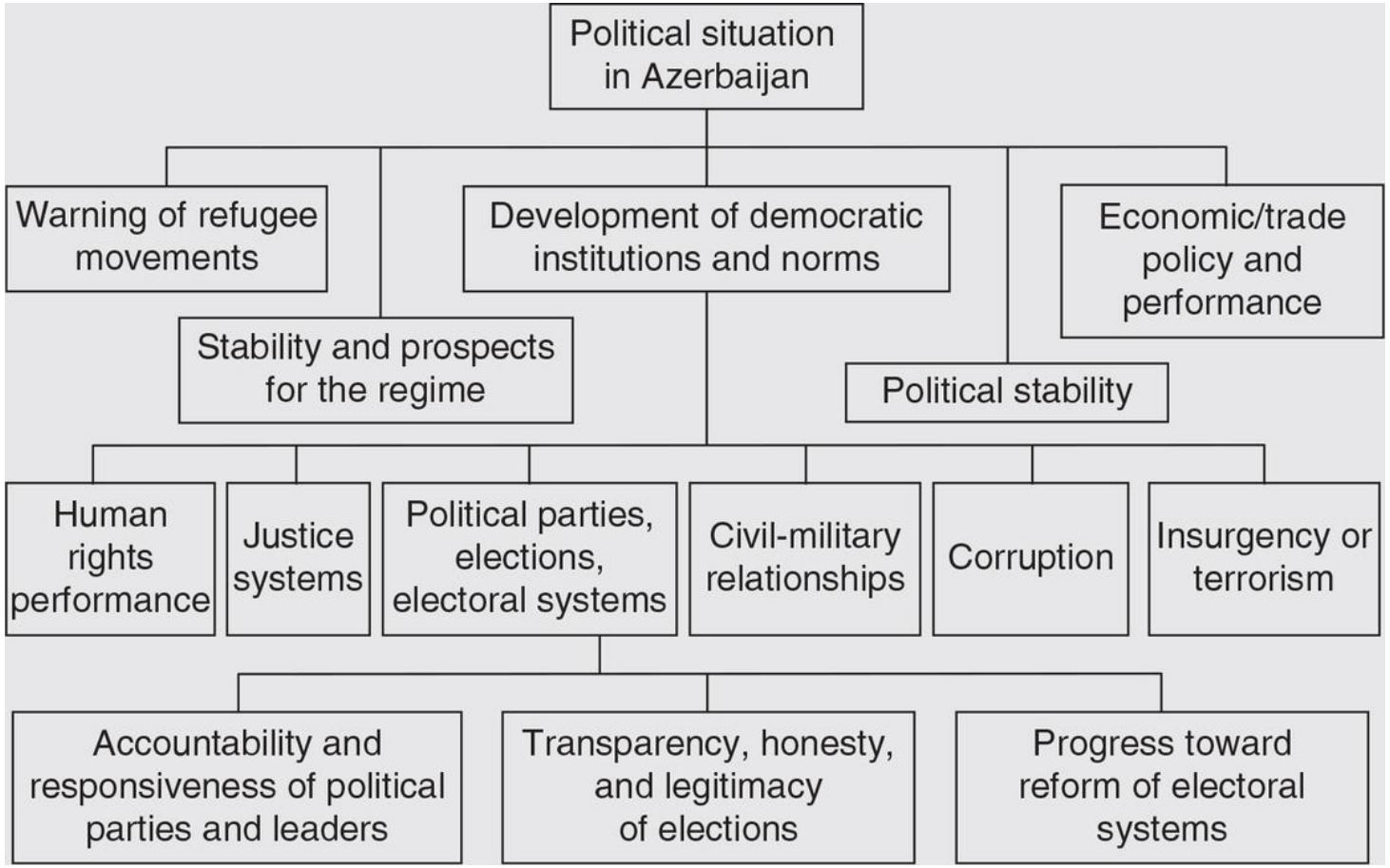
Quale è la situazione politica in una determinato paese?

Dovete provare ad interagire con il cliente, chiedere di specificare meglio la prospettiva, il periodo, etc. etc. etc.

Scomposizione del Problema – Esempio Situazione Politica

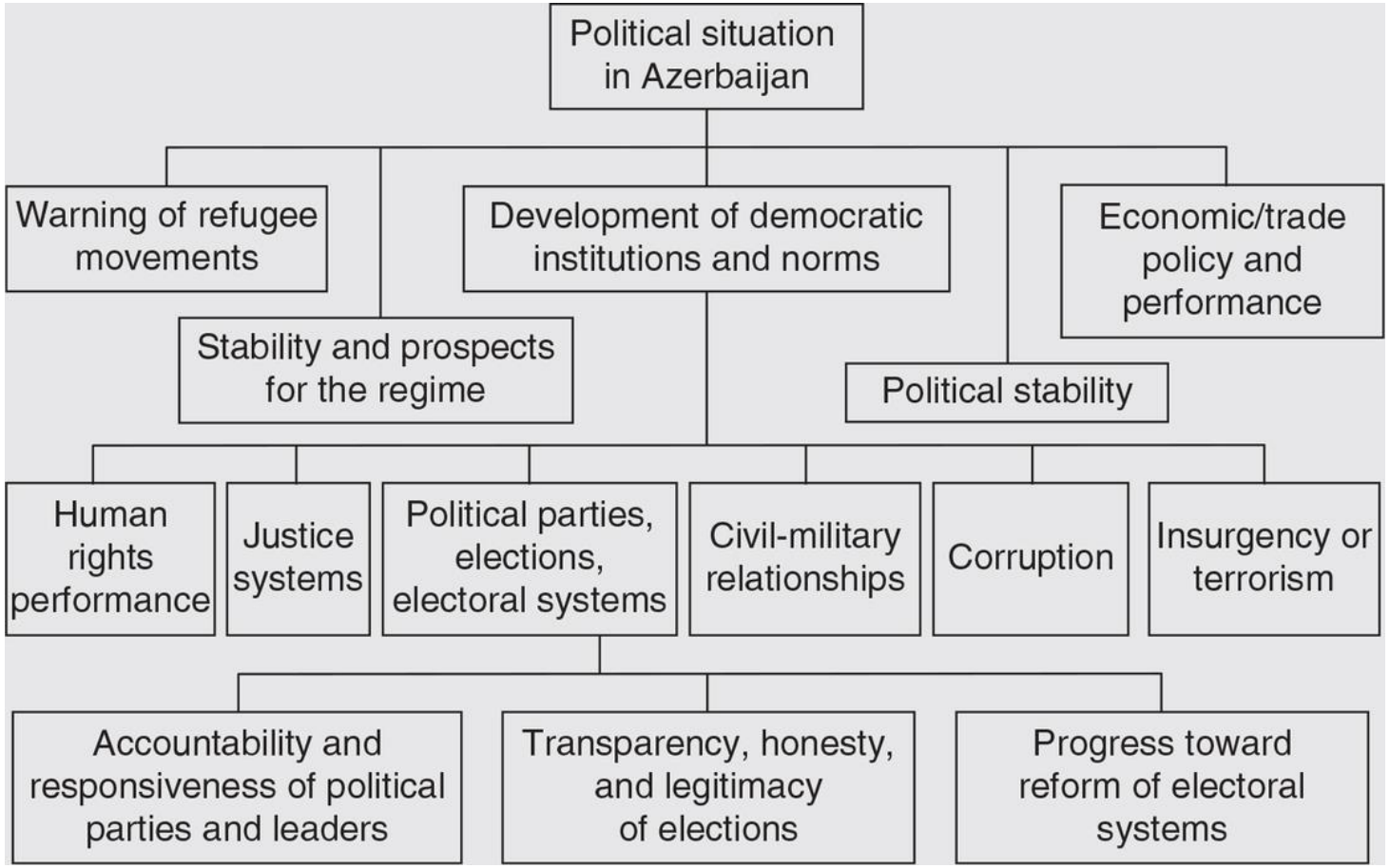


Scomposizione del Problema – Esempio Situazione Politica



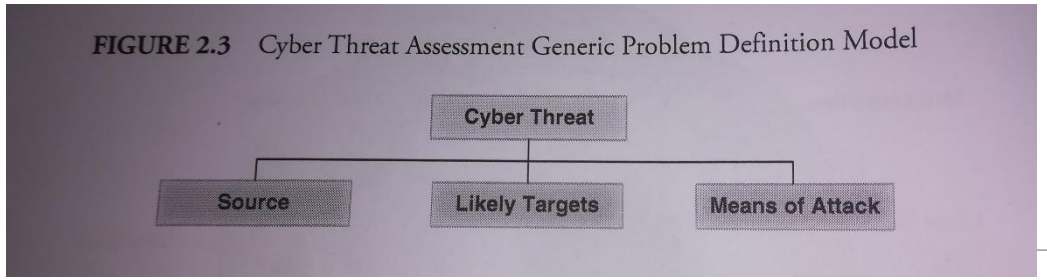
Alla domanda di primo livello "Qual è la situazione politica in Azerbaigian?" è difficile rispondere senza prima rispondere alle domande più specifiche più in basso nella gerarchia, come "Quali progressi si stanno facendo verso la riforma dei sistemi elettorali?"

Scomposizione del Problema – Esempio Situazione Politica



Alla domanda di primo livello "Qual è la situazione politica in Azerbaigian?" è difficile rispondere senza prima rispondere alle domande più specifiche più in basso nella gerarchia, come "Quali progressi si stanno facendo verso la riforma dei sistemi elettorali?“

E’ difficile valutare quanto bene un'organizzazione di intelligence stia rispondendo alla domanda "Qual è la situazione politica in Azerbaigian?" È molto più facile valutare le prestazioni dell'unità di intelligence nella ricerca sulla trasparenza, l'onestà e la legittimità delle elezioni, perché si tratta di questioni ben definite.



Modello generico per una cyber minaccia

Source: sono le potenziali sorgenti di attacco. Devono avere motivazioni, capacità ed intenzioni di attaccare.

Targets: sono gli obiettivi dell'attacco. Vanno individuati tra soggetti che possono essere oggetto della minaccia.

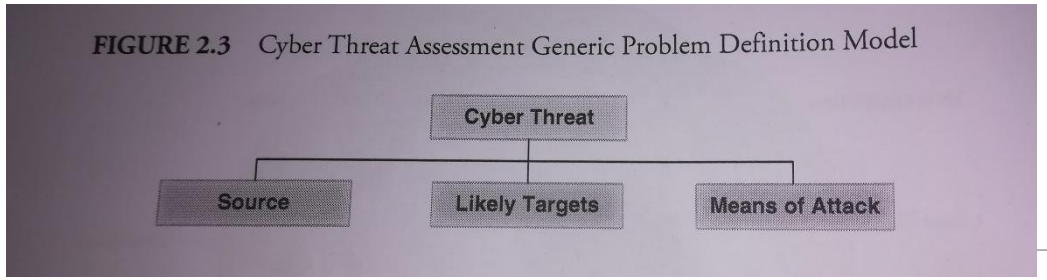
Modi in cui può attuarsi la minaccia: indicano le modalità di esecuzione.

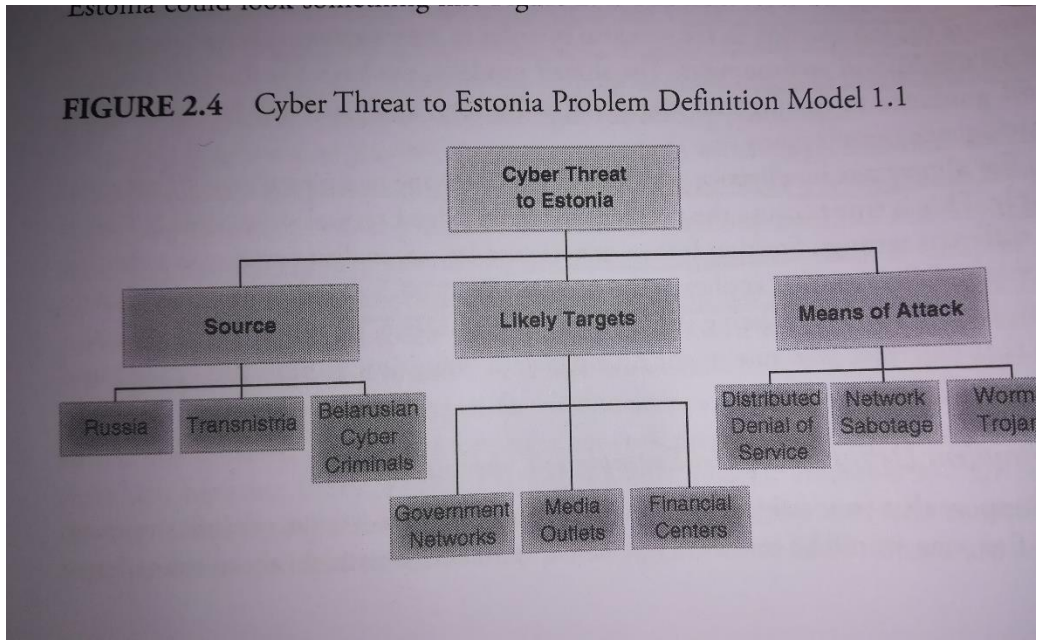
Modelli ed evoluzioni

Possono essere usati per «facilitare» la decomposizione di un problema

Spesso un modello è definito in maniera iterative in differenti fasi.

Si parte da un modello di descrizione del problema generale



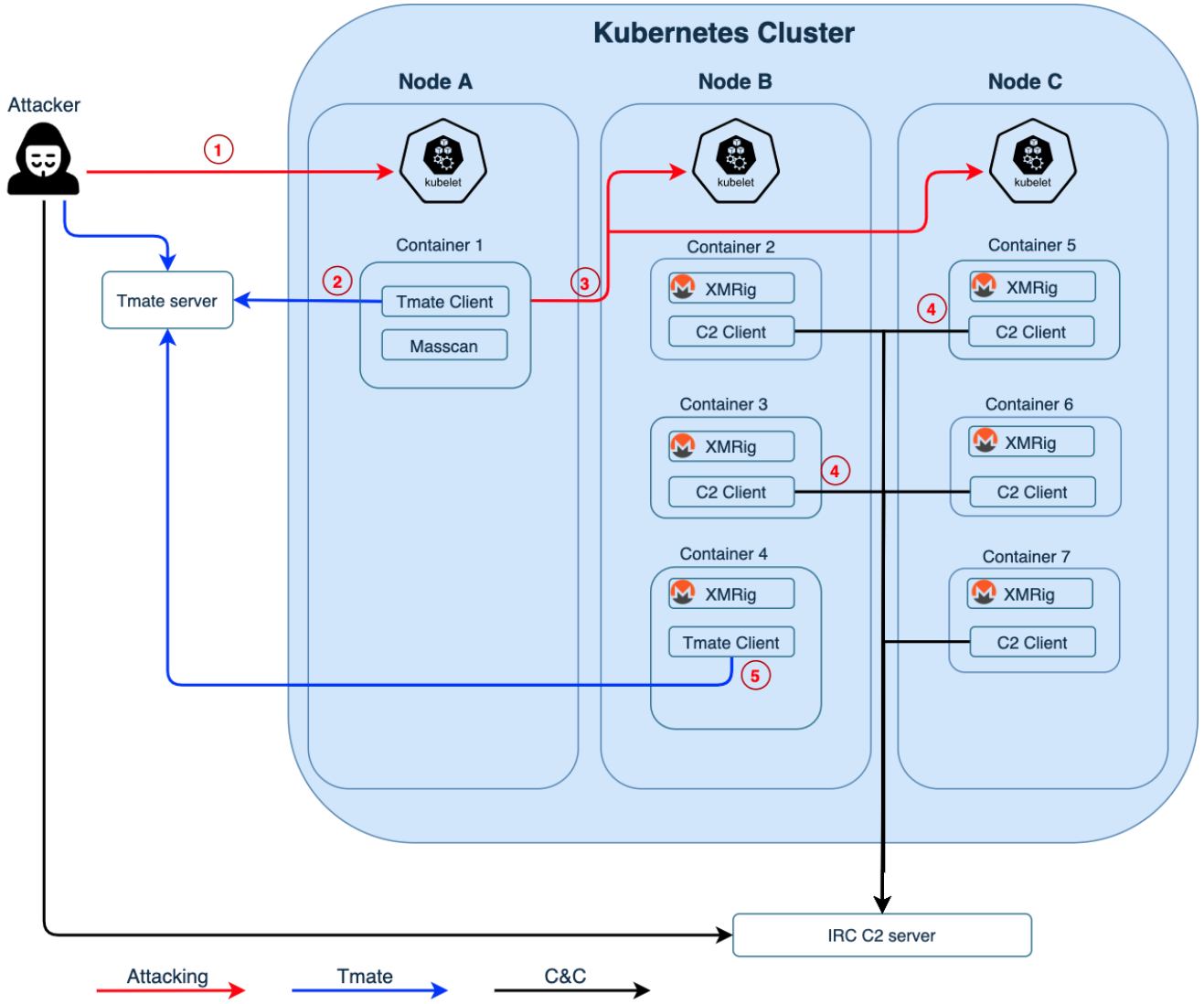


Modelli ed evoluzioni

Il modello generale viene esteso (o customizzato) per le concrete indagini.

Nel 2007 l'Estonia è stata vittima di una serie di cyber attacchi. Parlamento, banche e giornali on-line sono stati colpiti con attacchi informatici tra cui il DDoS (Distributed Denial of Services).

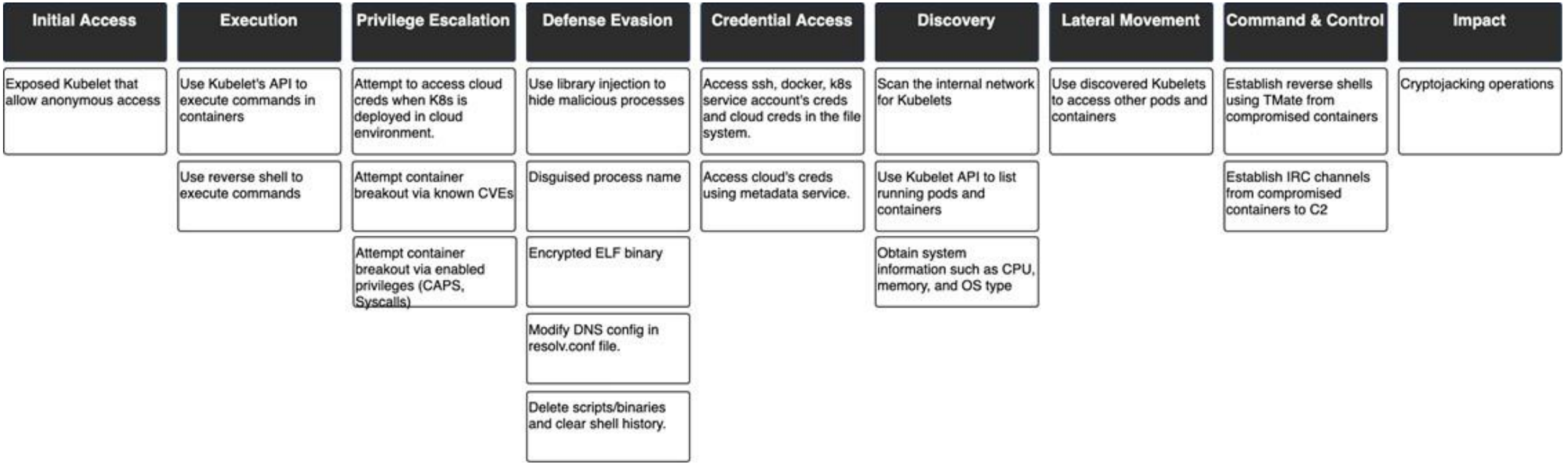
Ad una granularità più fine, il modello in figura potrebbe essere espanso con specifici gruppi hacker bielorussi, etc.

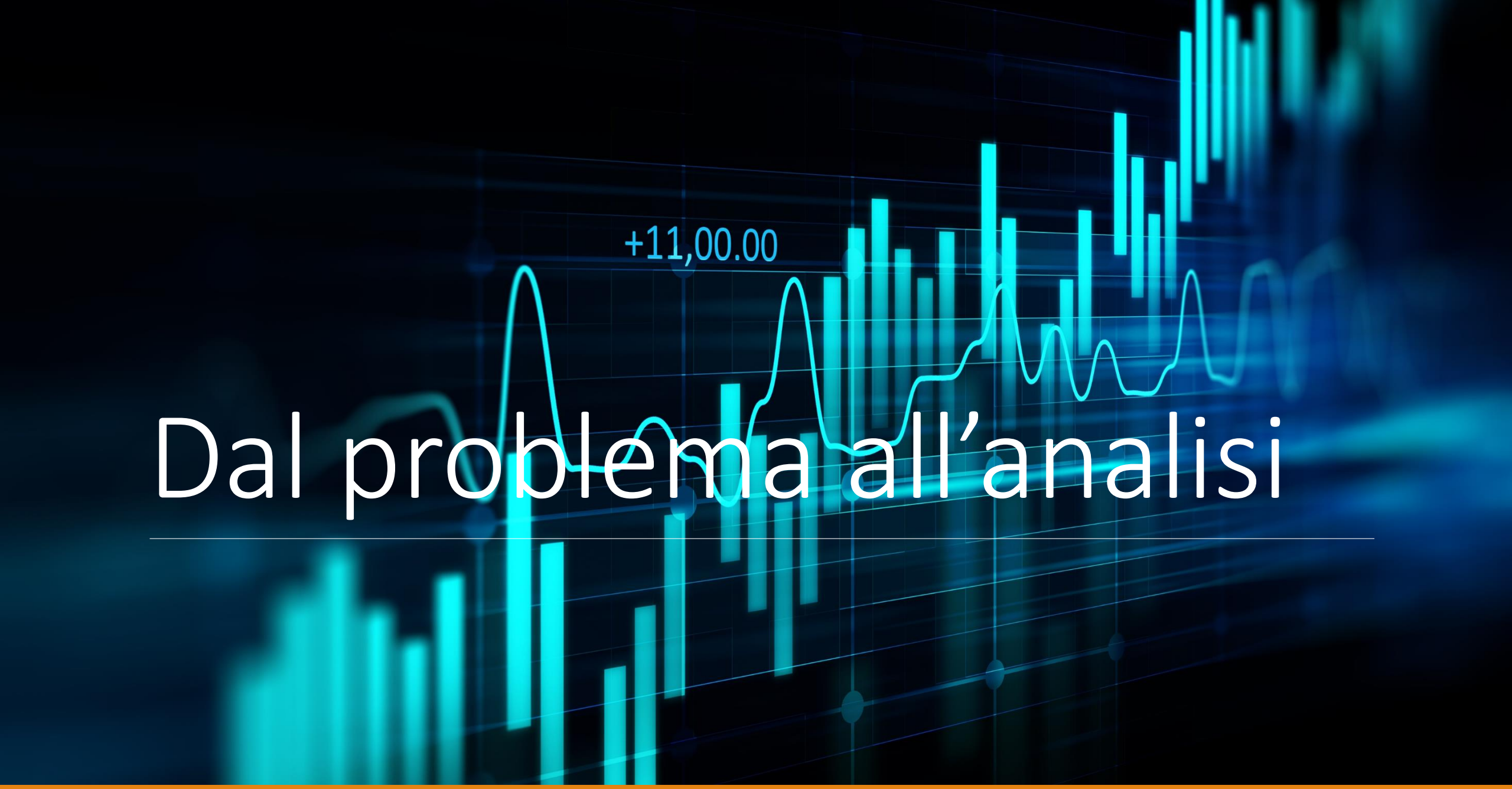


Sub-modelli – Es. Metodi di Attacco

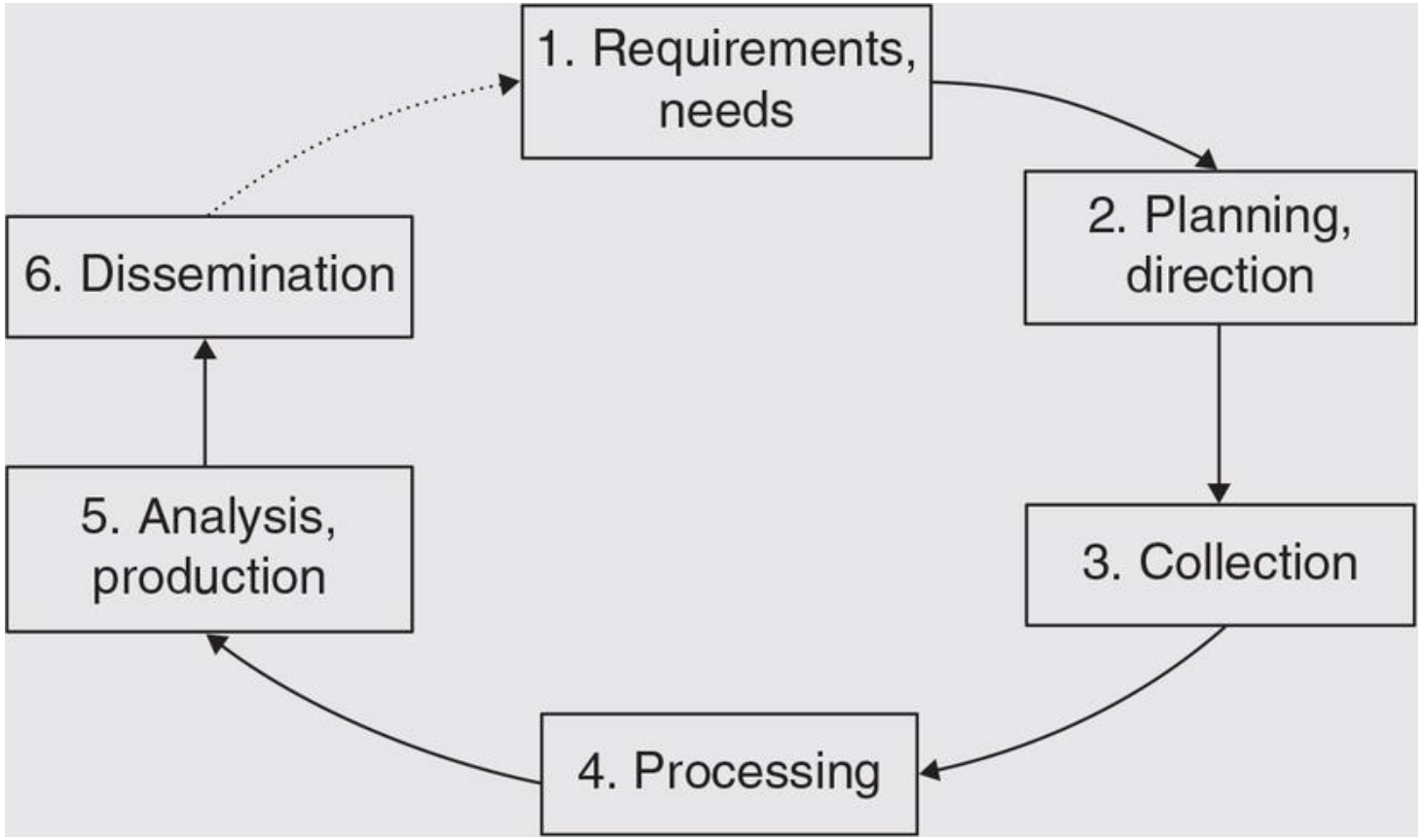
Source: https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/

Sub-modelli – Es. Percorsi di attacco





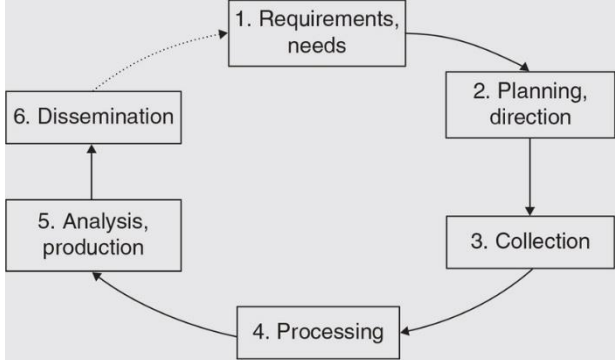
Dal problema all’analisi



Intelligence cycle (tradizionale)

L'intelligence si occupa sempre di un ***target*** (obiettivo), il fulcro del problema per il quale il cliente vuole risposte. Il compito principale dell'analista è sviluppare un livello di comprensione del target e comunicare tale conoscenza al cliente.

Fasi



Il ciclo inizia con uno step sui **requisiti**, che equivale a una definizione del problema. Di solito prende la forma di una domanda piuttosto generica da parte di un cliente

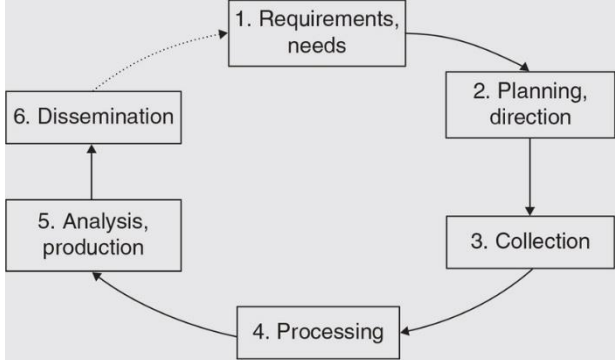
- Ad esempio: "Quanto è stabile il governo dell'Etiopia?"

La **pianificazione**, o **direzione**, determina come (e dove) si andrà a sviluppare la soluzione. I collezionisti devono essere incaricati di raccogliere le informazioni mancanti. Gli analisti devono essere incaricati di fare ricerca e produrre un rapporto sulla stabilità del governo etiope.

Il ciclo procede quindi con la **raccolta** di informazioni. È necessario accedere a materiale apertamente disponibile come giornali stampati e media elettronici.

- L'intelligence sulle comunicazioni (COMINT) deve essere focalizzata sulle informazioni relative al governo etiope.

Fasi



Le informazioni devono essere **elaborate**.

- Esempi di processing riguardano le seguenti attività: Il materiale in lingua straniera deve essere tradotto. I segnali crittografati devono essere decifrati. I segnali digitali devono essere tradotti in immagini visibili. Le risposte dalle fonti HUMINT devono essere convalidate e organizzate in un rapporto.

Nella fase di **analisi**, il materiale appena raccolto ed elaborato deve essere unito a materiale storico rilevante.

- L'analista deve generare i profili dei leader etiopi e valutare le loro probabili risposte a possibili eventi. Creerà modelli basati sull'attuale situazione etiope e produrrà scenari di risultato.

L'intelligence finale deve essere **diffusa** al cliente in un rapporto scritto (di solito inviato elettronicamente) o in un briefing. Dunque, vi può essere una transizione verso nuovi requisiti o bisogni, e il ciclo ricomincia.

Intelligence cycle (tradizionale)

Negli anni, il ciclo dell'intelligence è diventato quasi un concetto teologico: nessuno ne ha messo in dubbio la validità.

Tuttavia, il difetto di questo **approccio lineare** alla risoluzione dei problemi è che **oscura** il reale ***processo cognitivo*** *s*ottostante:

- la mente non funziona in modo lineare e di solito
- passa da una parte all'altra del problema nel processo di raggiungimento di una soluzione.
  - Gli analisti potrebbero saltare dall'analisi alla raccolta, quindi ai requisiti, alla raccolta di nuovo, quindi di nuovo all'analisi, in quello che sembra un processo molto disordinato e che non assomiglia in alcun modo a un ciclo.

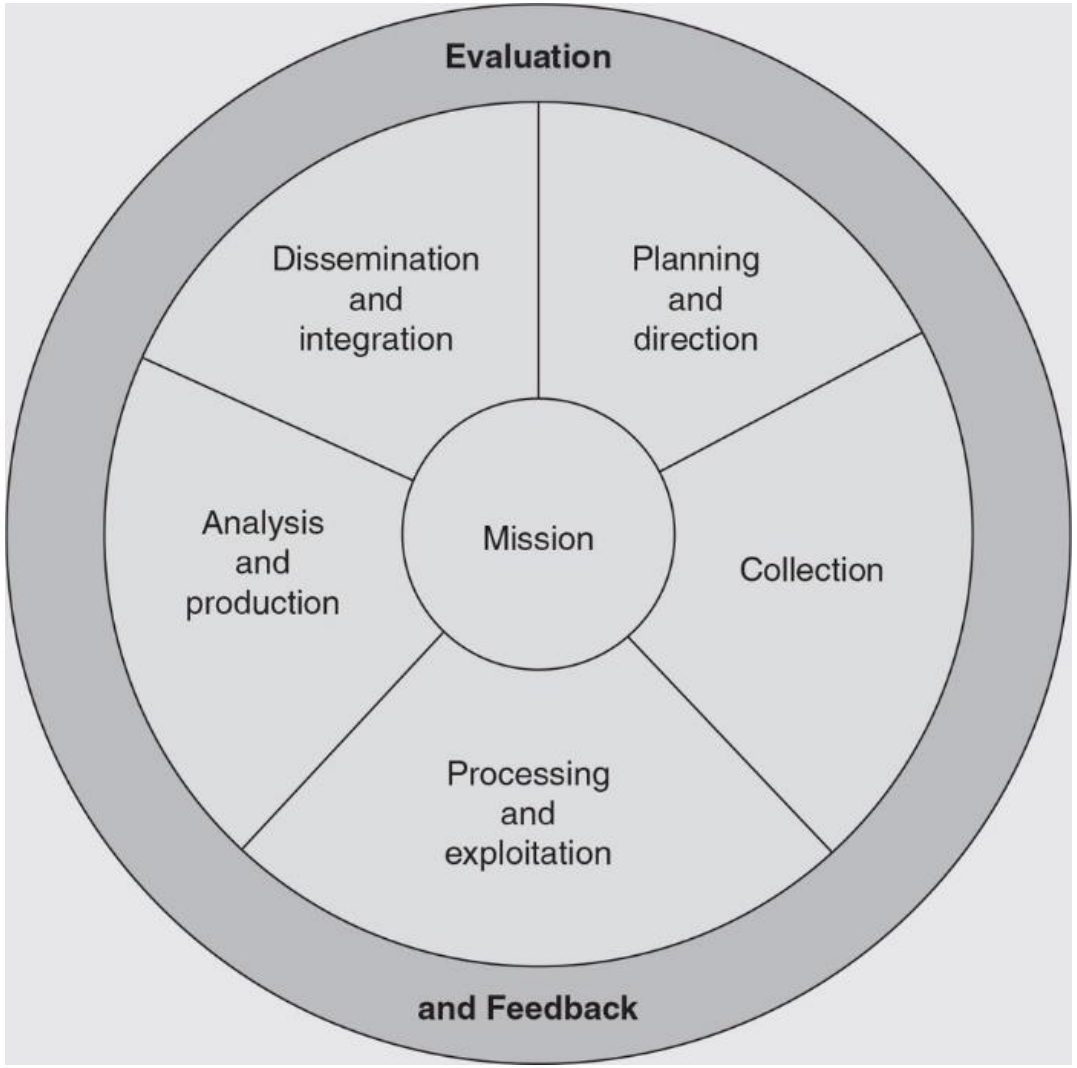
Alcune limitazioni del ciclo di intelligence

Il ciclo definisce una serie di passaggi *anti-sociali*.

Separa i ***collezionisti*** dai ***processori*** dagli analisti e troppo spesso si traduce in «lanciare le informazioni oltre il muro» affinché il compito passi alla prossima persona. Ognuno evita nettamente la responsabilità per la qualità del prodotto finale.

Poiché un tale processo si traduce in requisiti formalizzati e relativamente rigidi in ogni fase, ***è più prevedibile*** e quindi più vulnerabile alle contromisure di un avversario. Nell'intelligence, come nella maggior parte delle forme di conflitto, se puoi prevedere cosa faranno i tuoi avversari, puoi sconfiggerli.

La vista definita dal ciclo, quando considera il cliente, ***tende a trattare il cliente in astratto come un'entità monolitica***; in pratica esiste un divario tra disseminazione e bisogni. I clienti, essendo fuori dal giro, non possono rendere note le loro mutevoli esigenze.



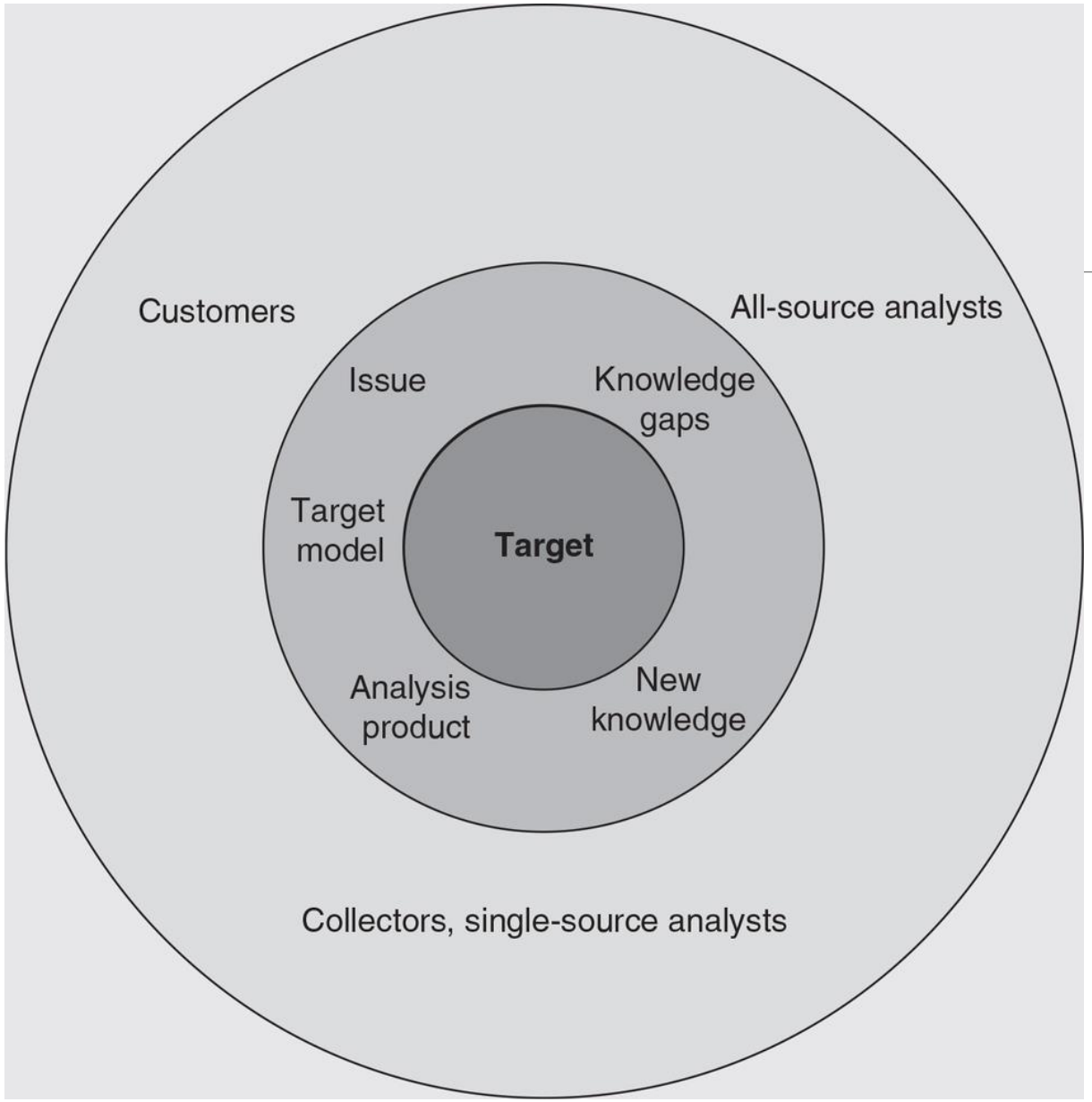
Dal Ciclo al Processo di Intelligence

Dal ciclo al processo

Un'alternativa al tradizionale ciclo di intelligence è ***rendere tutti gli stakeholder, inclusi i clienti, parte del processo di intelligence.*** Le parti interessate all'interno della comunità dell'intelligence riguardano collezionisti, processori, analisti e le persone che pianificano e costruiscono sistemi per supportarli.

I clienti su un determinato problema potrebbero includere, ad esempio, il presidente, il personale del Consiglio di sicurezza nazionale, il quartier generale del comando militare, i diplomatici, il Dipartimento per la sicurezza interna, le forze dell'ordine statali o locali e i comandanti della Marina Militare e della Guardia Costiera.

Per includerli nel processo di intelligence, ***il ciclo deve essere ridefinito in modo che il processo possa sfruttare appieno l'evoluzione della tecnologia dell'informazione e gestire problemi complessi.***



Intelligence as a Target-Centric Process

Visione incentrata sul *target* del processo di intelligence.

L'obiettivo è costruire **un'immagine condivisa del target**, a cui tutti i partecipanti possono contribuire con le proprie risorse o conoscenze, e da cui tutti possono estrarre gli elementi di cui hanno bisogno per svolgere il proprio lavoro.

Non è una sequenza lineare, né un ciclo (sebbene contenga molti cicli o cicli di feedback); è un processo di rete, un processo sociale, con tutti i partecipanti focalizzati sull'obiettivo.

È stato accuratamente descritto all'interno della comunità di intelligence degli Stati Uniti come un "**processo di collaborazione incentrato sulla rete**".

Target-Centric Process

Nel processo, i clienti che hanno problemi operativi esaminano lo stato attuale delle conoscenze sull'obiettivo (l'immagine dell'obiettivo attuale) e identificano le informazioni di cui hanno bisogno.

Gli analisti di intelligence, lavorando con collezionisti che condividono lo stesso target model, traducono le esigenze in «knowledge gaps» o "richieste di informazione" che i collezionisti devono affrontare.

Quando i collezionisti ottengono le informazioni necessarie, queste vengono incorporate nel target model condiviso.

Da questa immagine, analisti e collezionisti estraggono informazioni fruibili, che forniscono ai clienti, che possono a loro volta aggiungere le proprie intuizioni. Cioè, *i clienti dell'intelligence possono anche essere fonti di informazioni.*

I clienti, inoltre, possono anche aggiungere nuove esigenze informative.

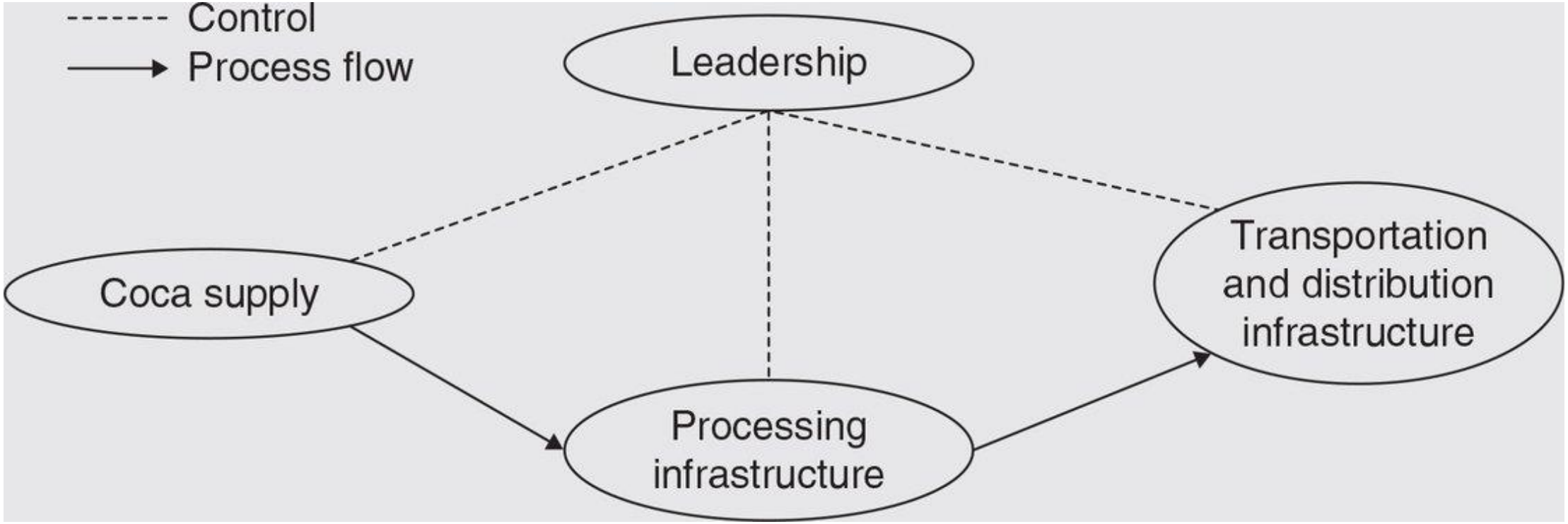
Il Target

Solitamente si tratta di un sistema.

Un sistema comprende:

- Struttura: componenti di un sistema e relazioni tra di esse
- Funzione: effetti o risultati prodotti -> output
- Processo: sequenza di eventi o attività che producono risultati

Target: Esempio basato su cartello della droga



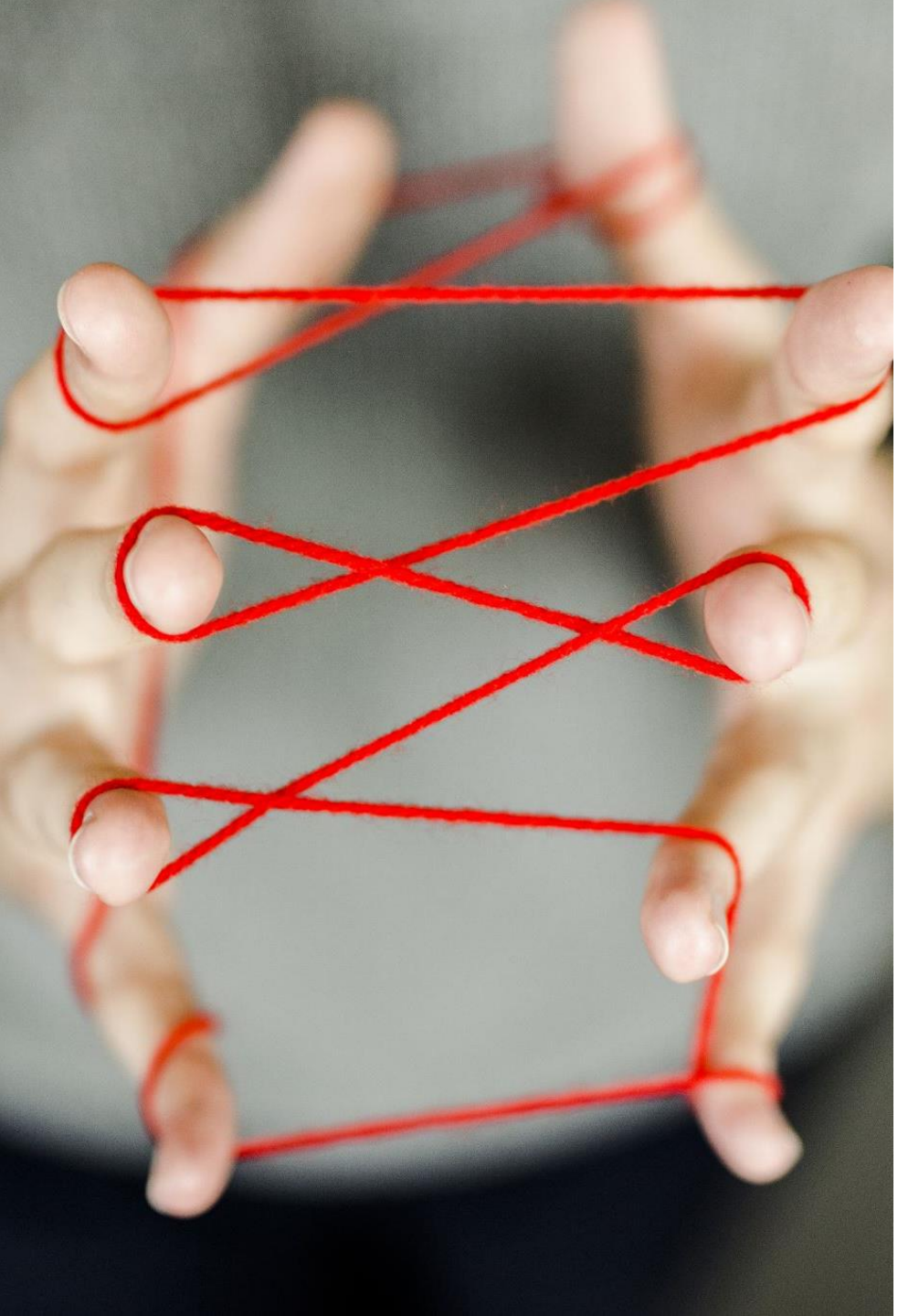
- La maggior parte degli obiettivi di intelligence sono sistemi che hanno, a loro volta, sistemi subordinati, chiamati anche *sottosistemi*.
- Spesso si tratta di sistemi complessi perché:
  - dinamici e in evoluzione.
  - non lineari, poiché non descritti adeguatamente da una struttura semplice come un diagramma ad albero o una struttura lineare come quella dell'intelligence cycle.

Esempi di Sistema Target

Un'entità geografica non è un sistema.

Un paese è un concetto troppo astratto per essere trattato come sistema. *Non ha struttura, funzione o processo, sebbene contenga al suo interno molti sistemi che li hanno tutti e tre*. Di conseguenza, un'entità geografica non può essere considerata un obiettivo dell'intelligence.

Il **governo** di una regione **è un sistema**: ha struttura, funzione e processo.



Target Network

Le reti, per definizione, comprendono *nodi* e *collegamenti* tra essi.

Per noi, una rete indica una *target network* in cui i nodi possono rappresentare qualsiasi tipo di entità: persone, luoghi, cose o concetti.

I collegamenti definiscono le relazioni tra i nodi e, talvolta, le quantificano.

Target Network

Nell’intelligence analysis, una target network può essere composta da:

- una combinazione di governi;
- attori non statali come gruppi ambientalisti, estremisti, religiosi, etc.;
- individui;
- imprese commerciali;
- organizzazioni illecite, insieme alle risorse a loro disposizione, tutte interconnesse perché hanno uno scopo condiviso (o in qualche modo si supportano a vicenda).

Nei conflitti, l'obiettivo dell'intelligence è sviluppare una comprensione della rete avversaria, e contemporaneamente di ostacolare il lavoro di comprensione da parte del nemico.

Ed, ovviamente, *creare una rete per contrastare la rete avversaria*.

FIGURE 1.1 Intelligence Sharing in Network Versus Network

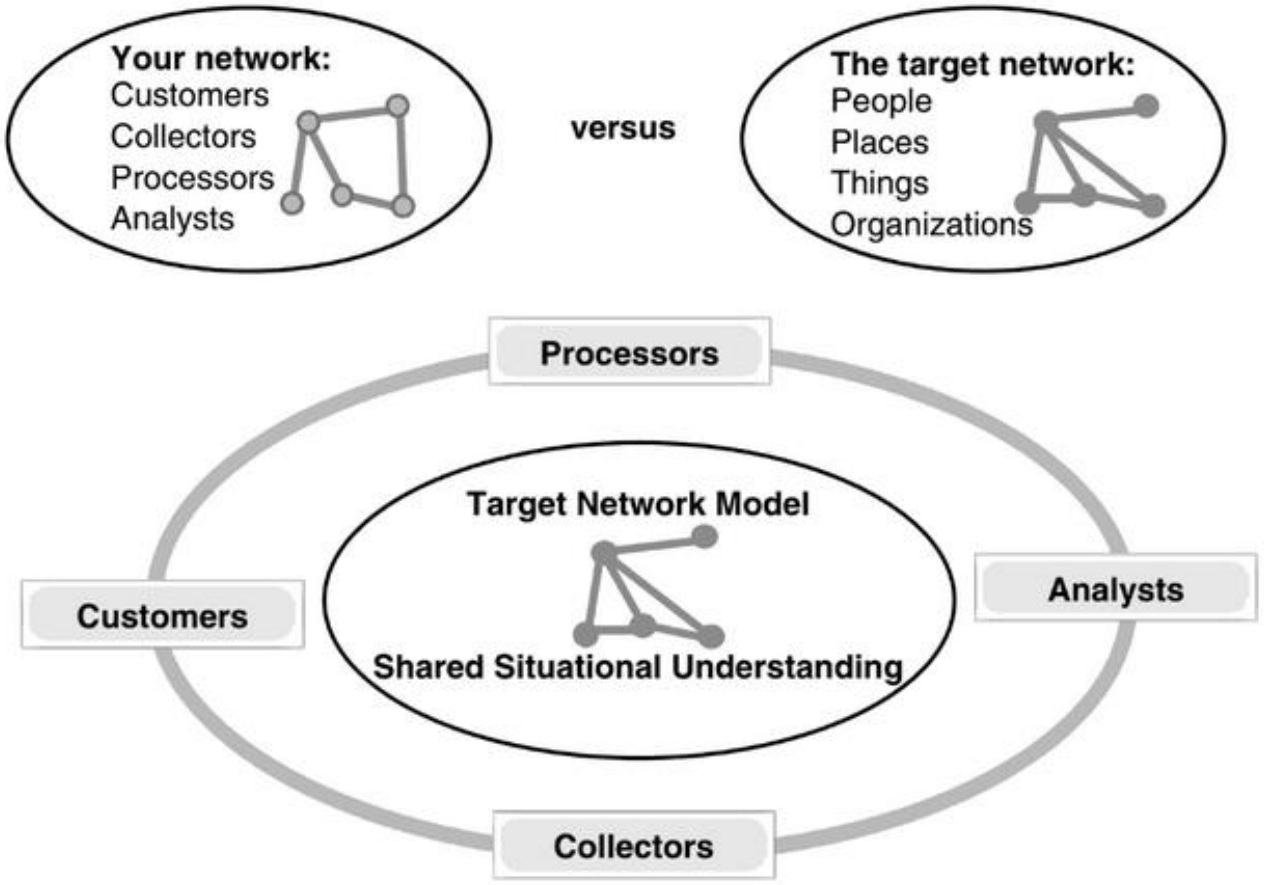
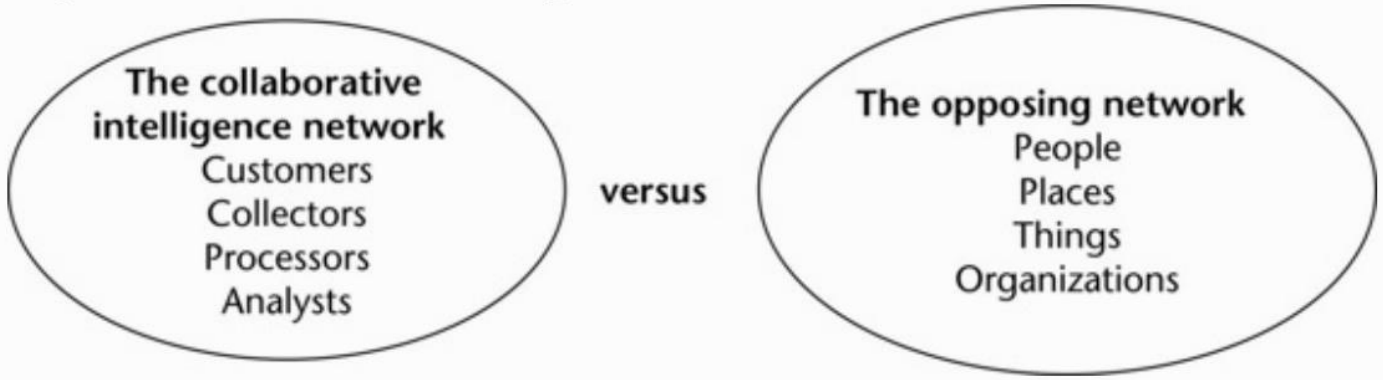
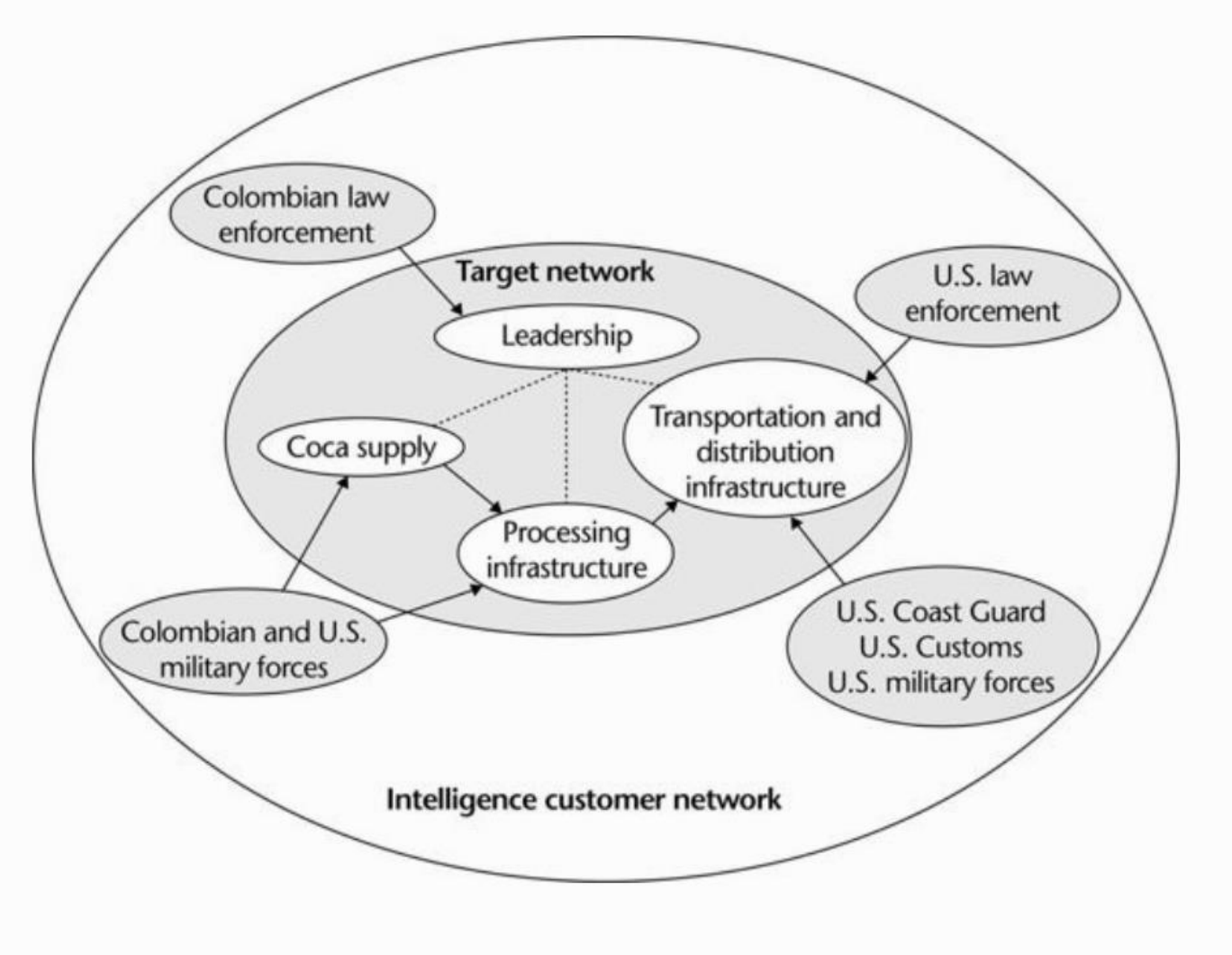


Figure 3-4 Netwar Competition: Network versus Network



Networks vs Networks



Netwar example against Coca Network

Tecniche di Analisi Strutturata - SAT

Biases comuni

Heuer: The Psychology of

Intelligence Analysis

Fonte: A Tradecraft Primer:

Structured Analytic Techniques

for Improving Intelligence Analysis

Common Perceptual and Cognitive Biases

Perceptual Biases

Expectations. We tend to perceive what we expect to perceive. More (unambiguous) information is needed to recognize an unexpected phenomenon.

Resistance. Perceptions resist change even in the face of new evidence.

Ambiguities. Initial exposure to ambiguous or blurred stimuli interferes with accurate perception, even after more and better information becomes available.

Biases in Evaluating Evidence

Consistency. Conclusions drawn from a small body of consistent data engender more confidence than ones drawn from a larger body of less consistent data.

Missing Information. It is difficult to judge well the potential impact of missing evidence, even if the information gap is known.

Discredited Evidence. Even though evidence supporting a perception may be proved wrong, the perception may not quickly change.

Biases in Estimating Probabilities

Availability. Probability estimates are influenced by how easily one can imagine an event or recall similar instances.

Anchoring. Probability estimates are adjusted only incrementally in response to new information or further analysis.

Overconfidence. In translating feelings of certainty into a probability estimate, people are often overconfident, especially if they have considerable expertise.

Biases in Perceiving Causality

Rationality. Events are seen as part of an orderly, causal pattern. Randomness, accident and error tend to be rejected as explanations for observed events. For example, the extent to which other people or countries pursue a coherent, rational, goal-maximizing policy is overestimated.

Attribution. Behavior of others is attributed to some fixed nature of the person or country, while our own behavior is attributed to the situation in which we find ourselves.

Effetti delle bias

1941 World War II

Japan would avoid all-out war because it recognized US military superiority.

Given that US superiority would only increase, Japan might view a first strike as the only way to knock America out of the war.

1950s Korean War

China would not cross the Yalu River in support of the North Korean government.

Red China could make good on its threats to counter "US aggression" against the North.

1962 Cuban Missile Crisis

The Soviet Union would not introduce offensive nuclear weapons into Cuba.

The Kremlin could miscalculate and believe it could create a fait accompli that a young US President would not be prepared to reverse.

1973 Yom Kippur War

Arabs knew they could not win because they had failed to cooperate in the past and still lacked sufficient air defenses to counter Israeli airpower.

A surprise Arab attack, even if repelled, could wound Israel psychologically and prompt international calls for cease-fires and diplomatic negotiations.

1989 German Unification

East Germany could not unify with the West Germany against the wishes of the Soviet Union.

The Soviet Union—under Gorbachev—might not be prepared to intervene militarily in Eastern Europe as it had in the past.

1998 Indian Nuclear Test

Conducting a nuclear test risked international condemnation and US sanctions and would threaten a newly elected coalition government.

A successful and surprise nuclear test could boost Indian nationalist pride and solidify public support for a shaky coalition government.

2003 Iraq's WMD Programs

Saddam failed to cooperate with UN inspectors because he was continuing to develop weapons of mass destruction.

If Iraqi authorities had destroyed their WMD stocks and abandoned their programs, they might refuse to fully acknowledge this to the UN to maintain Iraq's regional status, deterrence, and internal regime stability.

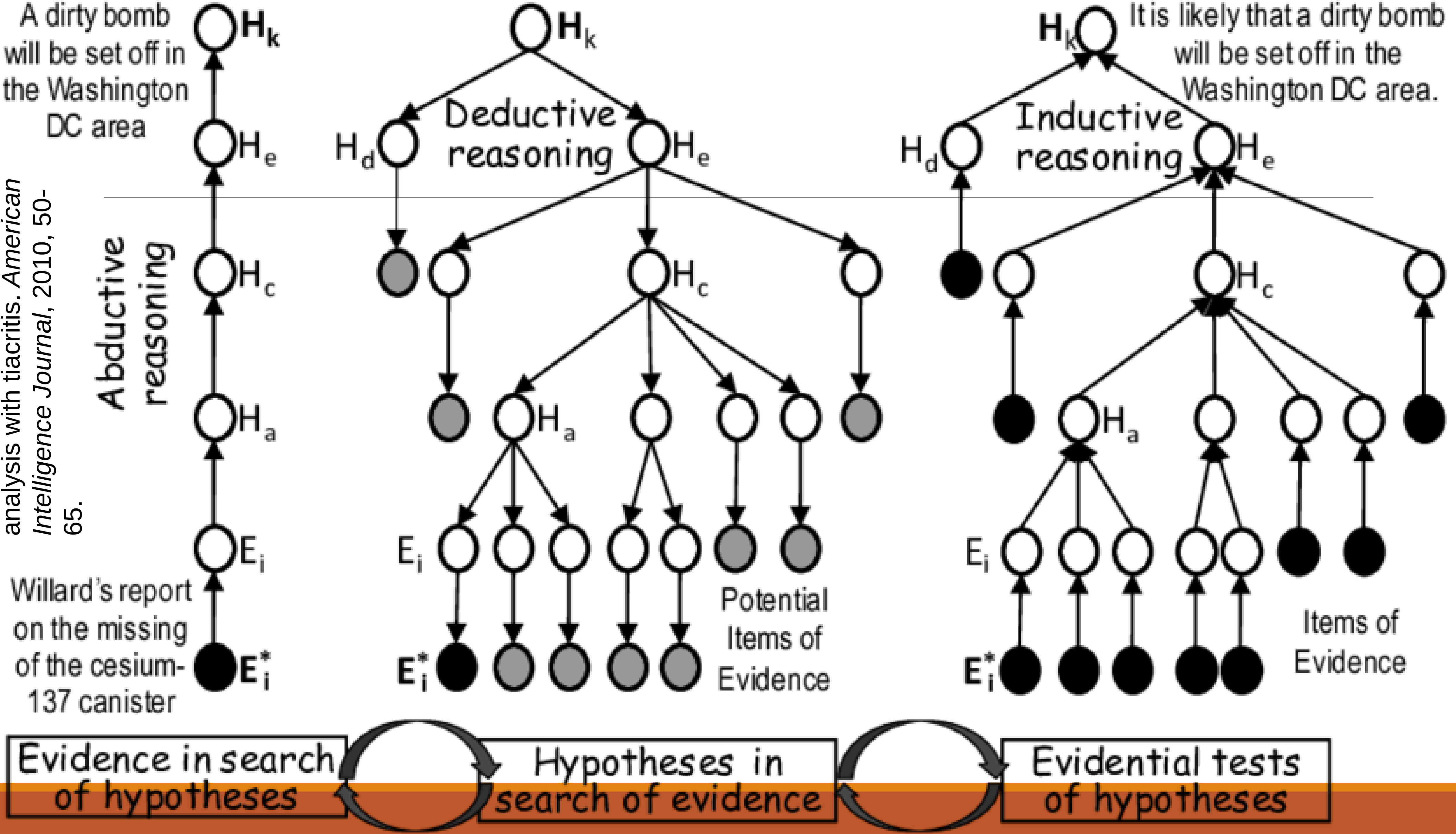
Fonte: A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis

Ragionamento ed Analisi

Ragionamento: il modo in cui l'analista redige il prodotto (nuova informazione/conoscenza)

Alcuni meccanismi di ragionamento

- Induzione
- Deduzione
- Abduzione
- Intuizione, Aporia, Diairesi, …



Fonte: TECUCI, Gheorghe, et al. Teaching intelligence analysis with tiacritis. *American Intelligence Journal*, 2010, 50-65.

Ragionamento ed Analisi

Analisi: il modo di validare i risultati del ragionamento dell'analista

L'insieme dei metodi usati per l'analisi prende il nome di *Analytic Tradecraft*

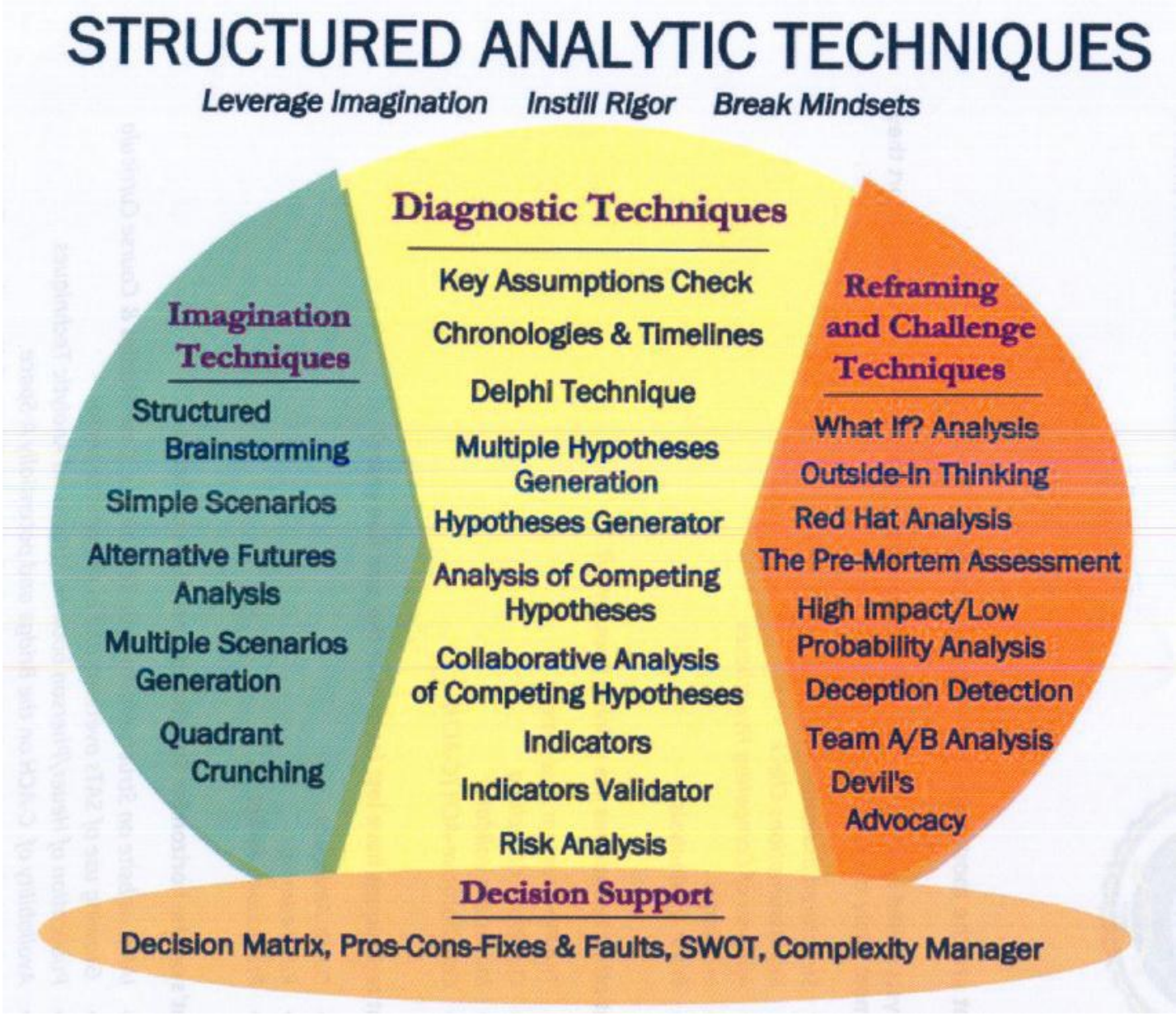
Un tradecraft molto adottato è quello delle *Strcutured Analytic Techniques* (SAT) definito da Richards Heuer

- A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis-March 2009 (https://www.stat.berkeley.edu/~aldous/157/Papers/Tradecraft%20Primer-apr09.pdf)

SAT

Obiettivo: supportare **l'esternalizzazione** del ragionamento in modo che i risultati possano essere condivisi e analizzati anche da altri analisti

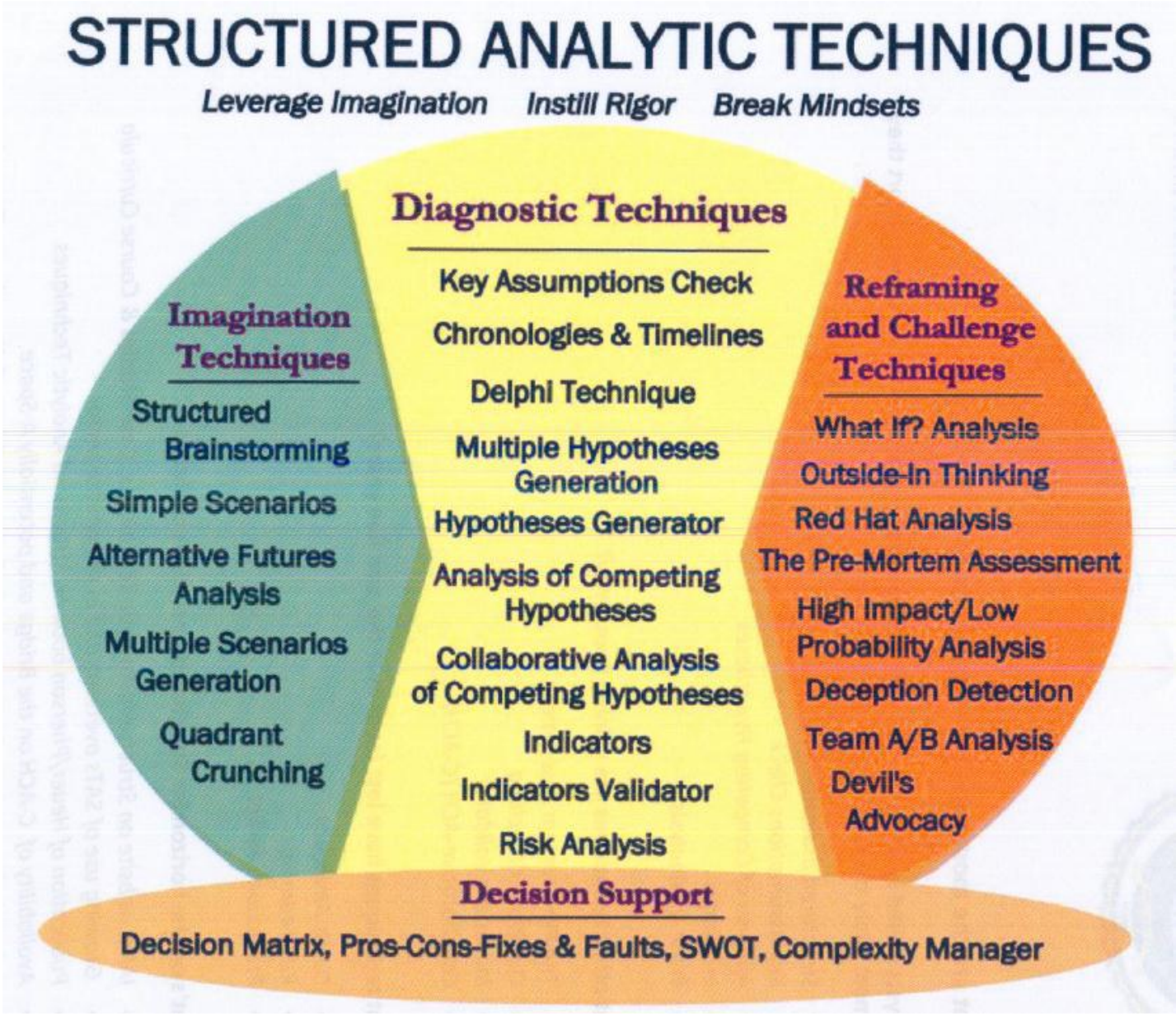
SAT: overview delle tecniche



Fonte: http://www.personal.psu.edu/ejg8/class/sra111/StructuredAnalytics_v1.pdf

SAT: overview delle tecniche

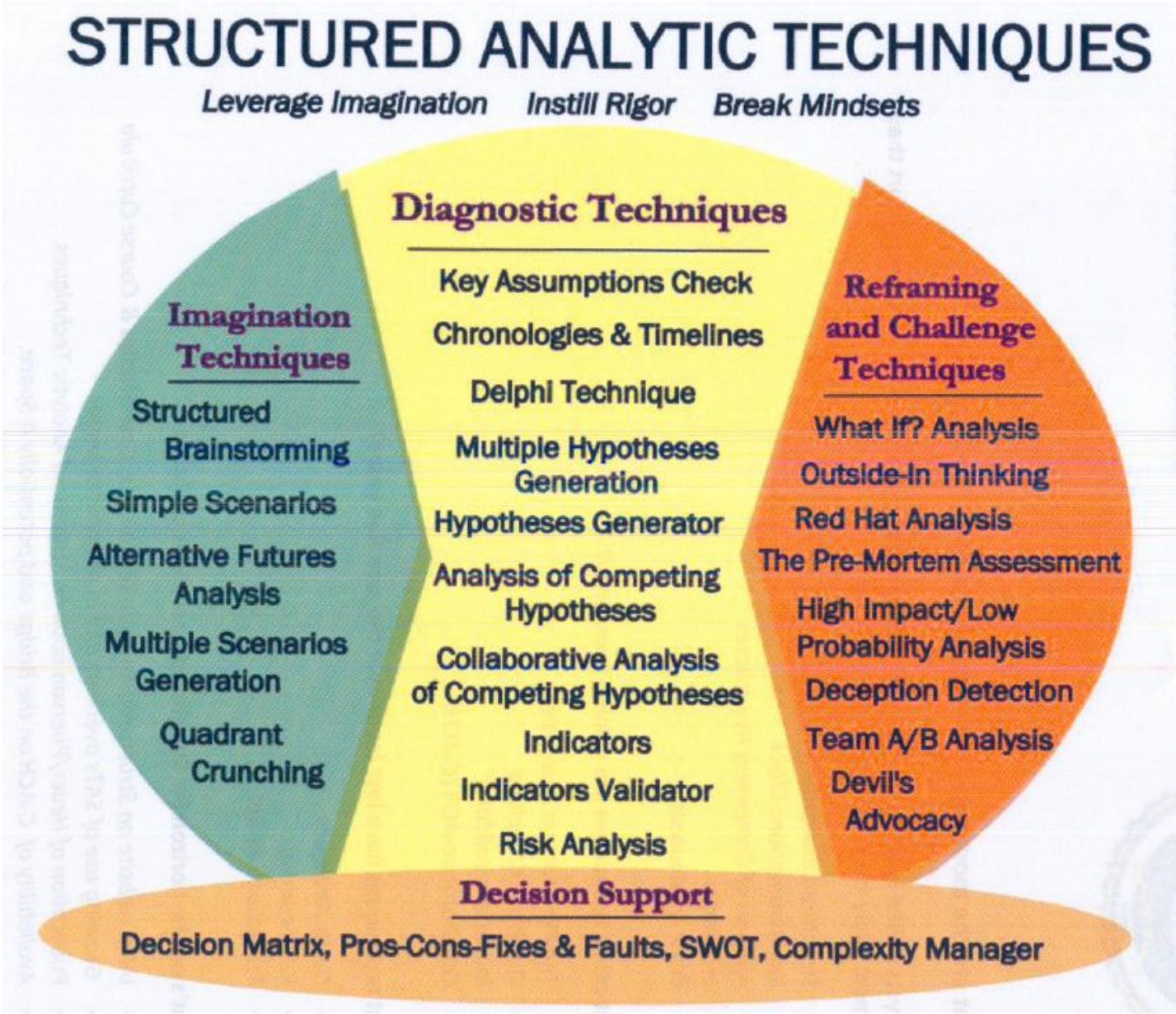
Diagnostiche: finalizzate a confermare le convinzioni attuali (ad esempio, rendere più trasparenti le argomentazioni analitiche, le ipotesi o le lacune)



SAT: overview delle tecniche

Diagnostiche: finalizzate a confermare le convinzioni attuali (ad esempio, rendere più trasparenti le argomentazioni analitiche, le ipotesi o le lacune)

Contrarie (Reframing): finalizzate a sfidare esplicitamente il pensiero attuale

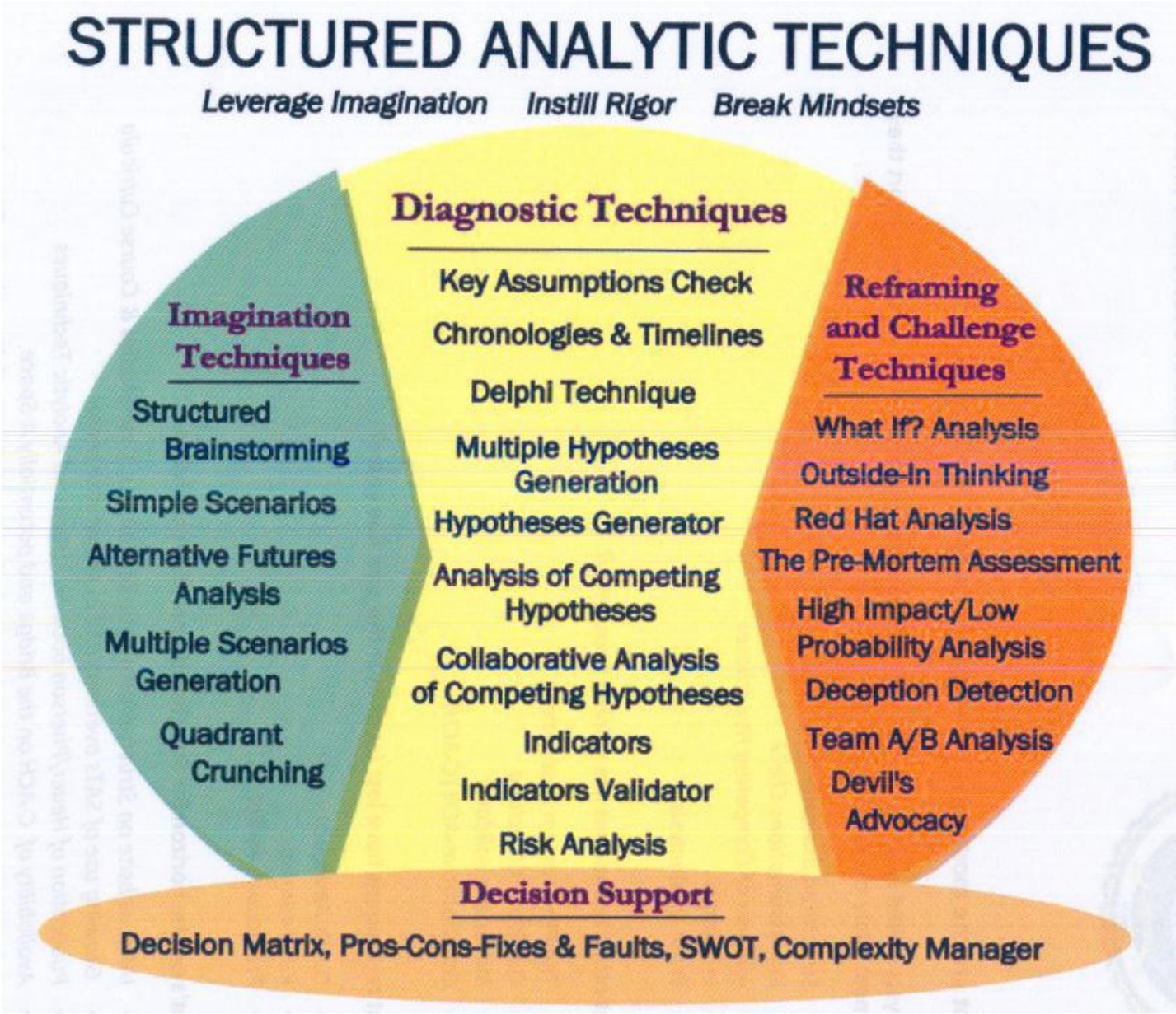


SAT: overview delle tecniche

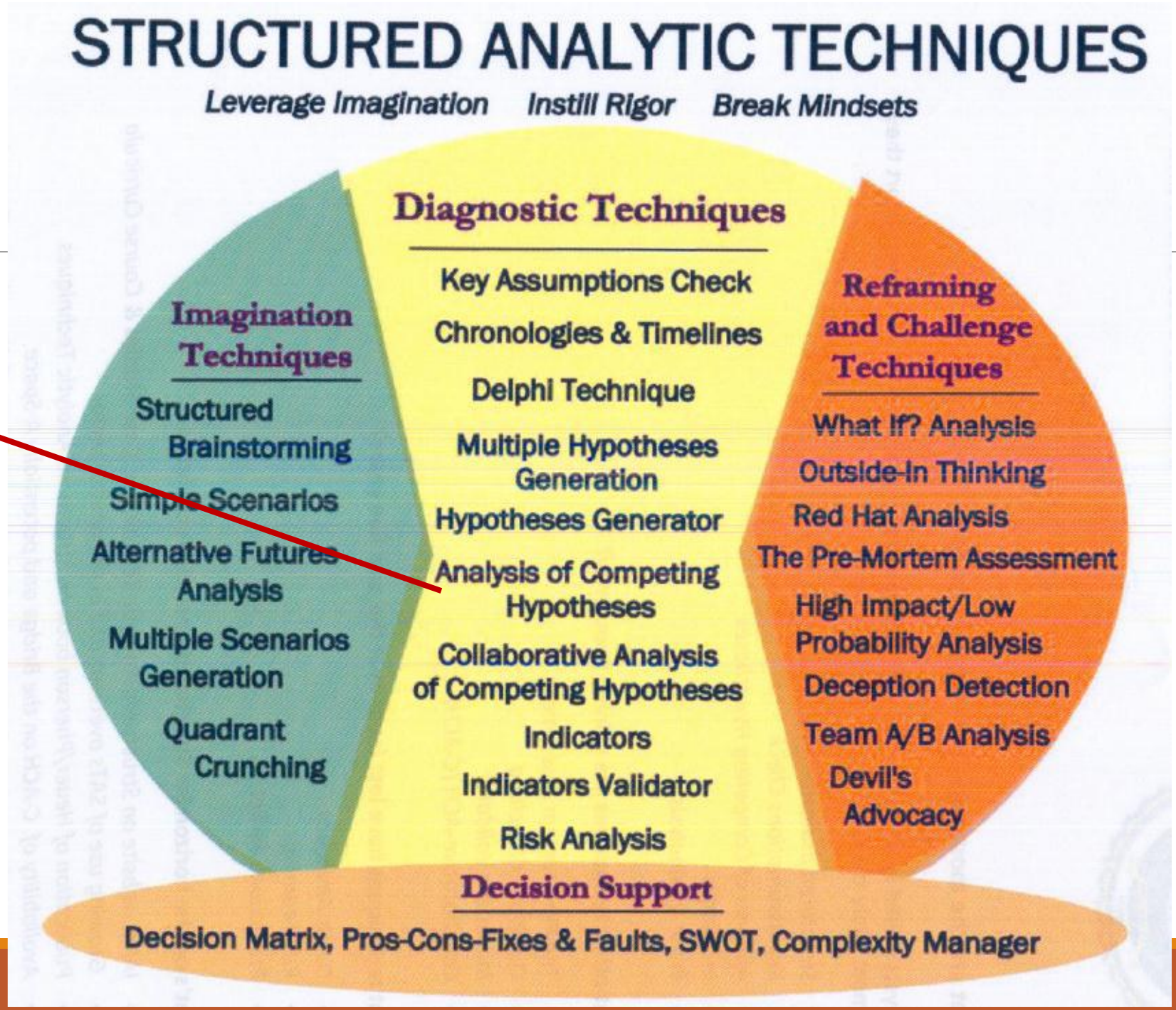
Diagnostiche: finalizzate a confermare le convinzioni attuali (ad esempio, rendere più trasparenti le argomentazioni analitiche, le ipotesi o le lacune)

Contrarie (Reframing): finalizzate a sfidare esplicitamente il pensiero attuale

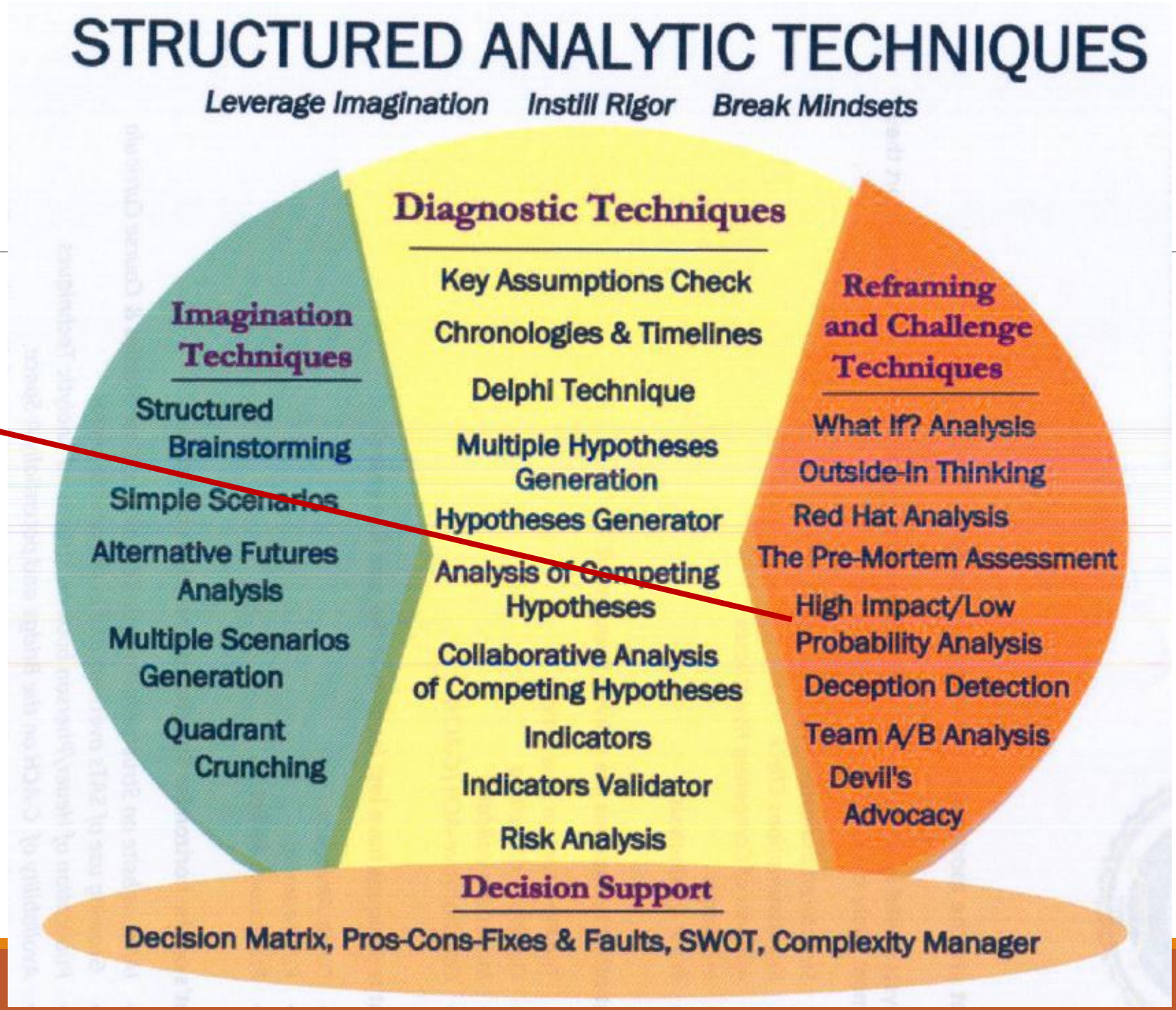
Immaginative: mirano allo sviluppo di nuove intuizioni, prospettive diverse e/o allo sviluppo di scenari alternativi

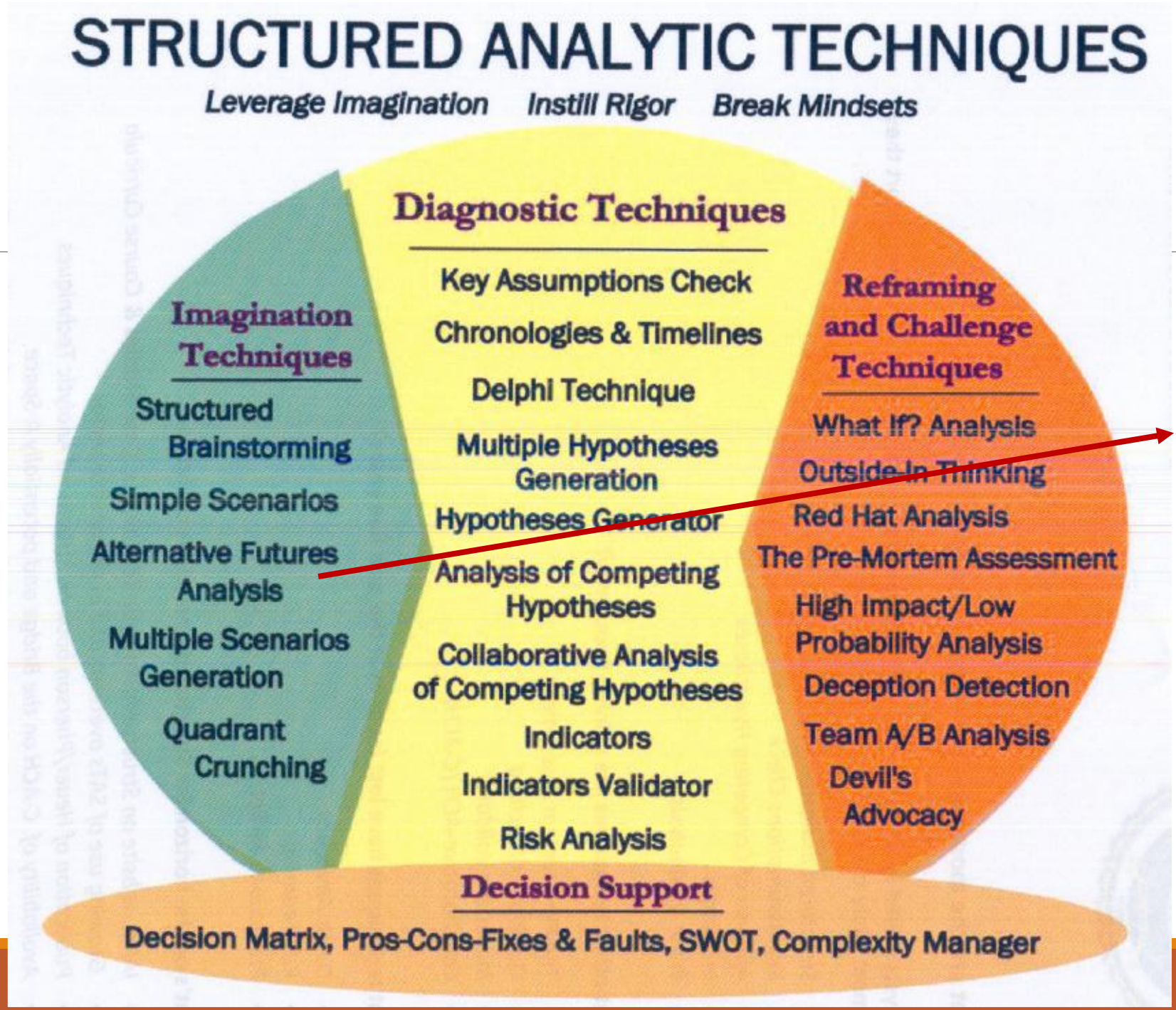


Identification of alternative explanations (hypotheses) and evaluation of all evidence that will disconfirm rather than confirm hypotheses



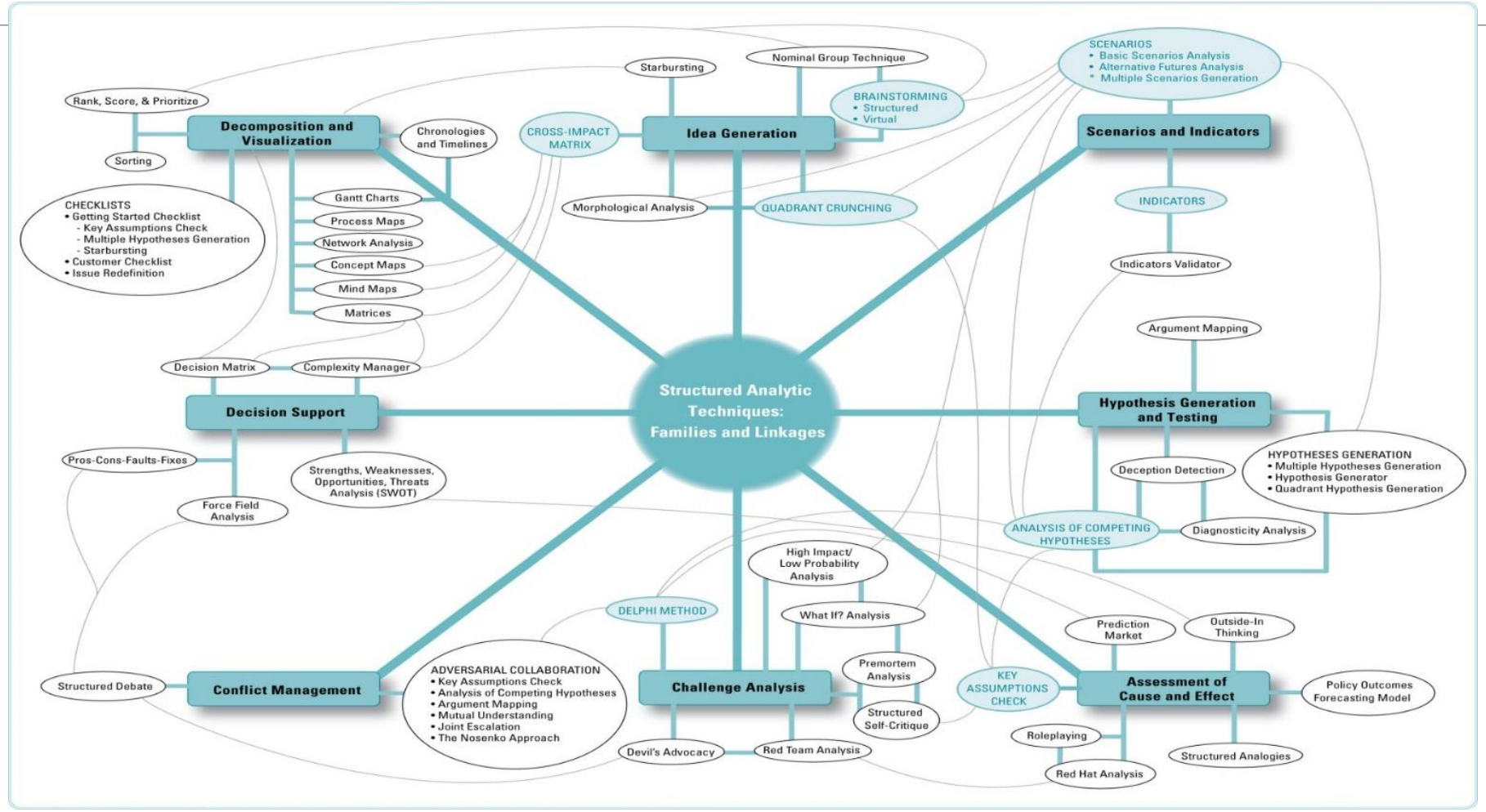
Highlights a seemingly unlikely event that would have major policy consequences if it happened.

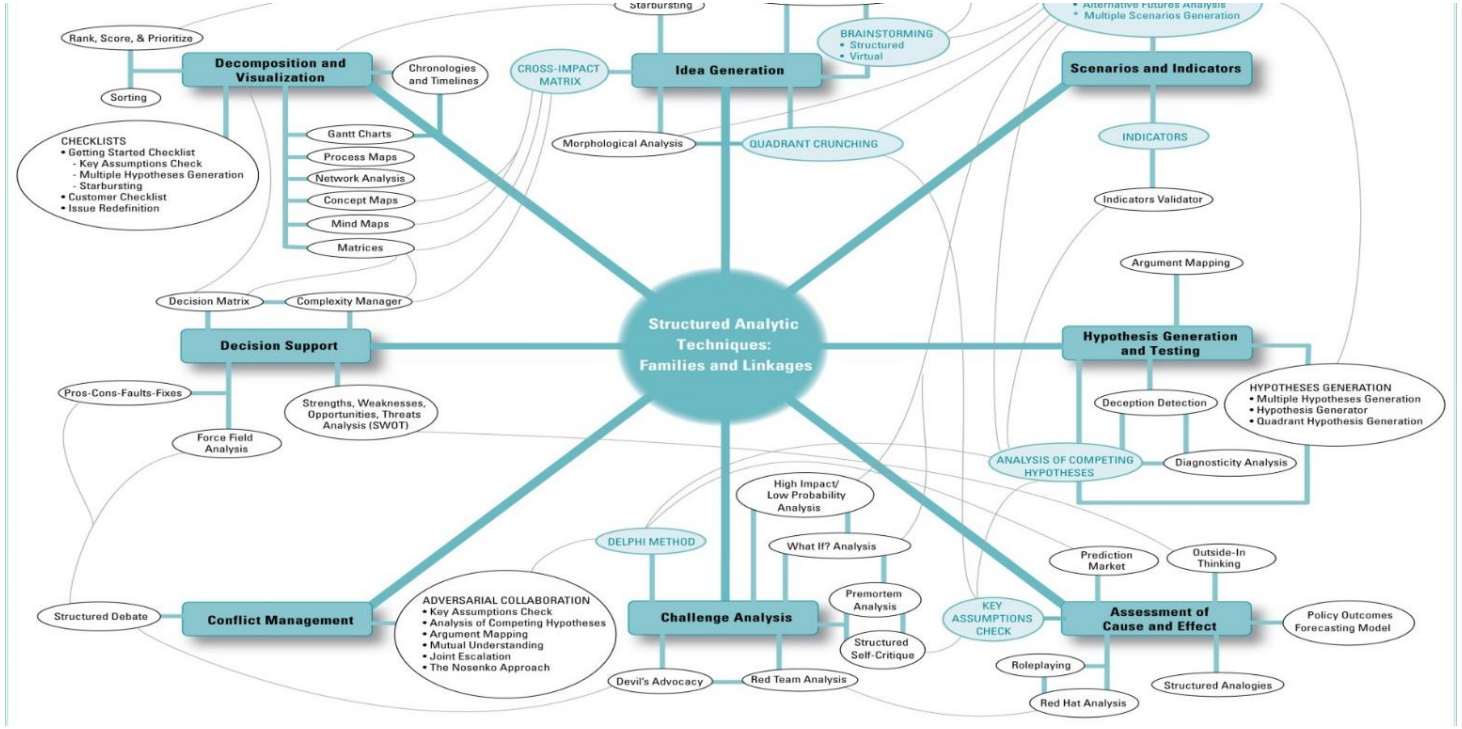




Systematically explores multiple ways a situation can develop when there is high complexity and uncertainty.

Quale tipo di SAT?





Quale tipo di SAT? Le famiglie

Decomposition & Visualization. Queste tecniche sono volte a semplificare un problema complesso: a) scomponendolo in parti più piccole che possono essere considerate e analizzate separatamente e b) visualizzando queste parti in modo organizzato con alcuni tipi di mappe o grafici per facilitare la comprensione di come le parti sono correlate tra loro.

Idea Generation: Questa famiglia di tecniche mira a facilitare l'emergere di idee nuove e non ovvie con il supporto di strumenti collaborativi

Scenarios and Indicators. Queste tecniche consentono agli analisti di identificare e monitorare gli scenari per capire quale scenario si sta sviluppando.

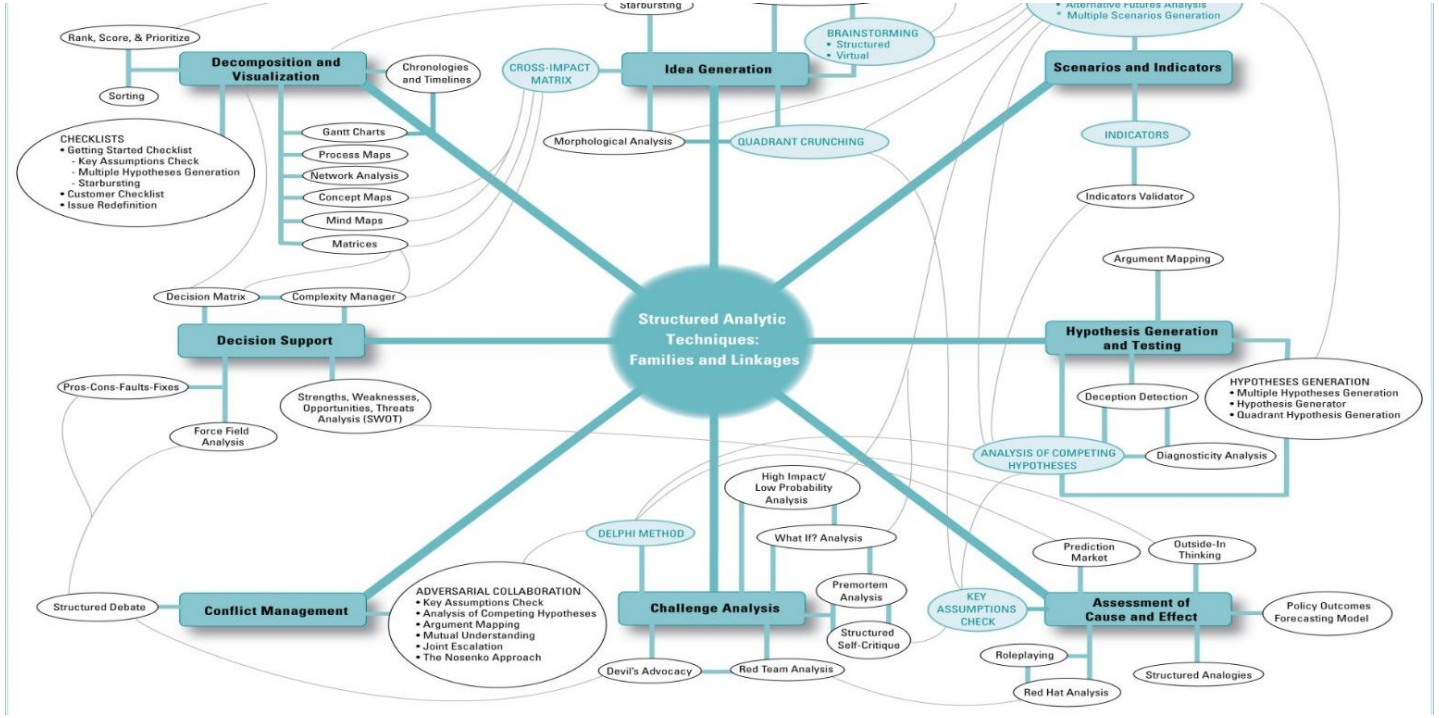
Quale tipo di SAT? Le famiglie

Hypotheses Generation and Testing. Lo scopo di queste tecniche è di supportare gli analisti in una funzione centrale dell'Intelligence Analysis: la generazione e la verifica di ipotesi.

Assessment of Cause and Effect. Tali tecniche hanno l'obiettivo di valutare la causa degli eventi attuali e gli effetti previsionali che potrebbero verificarsi in futuro,

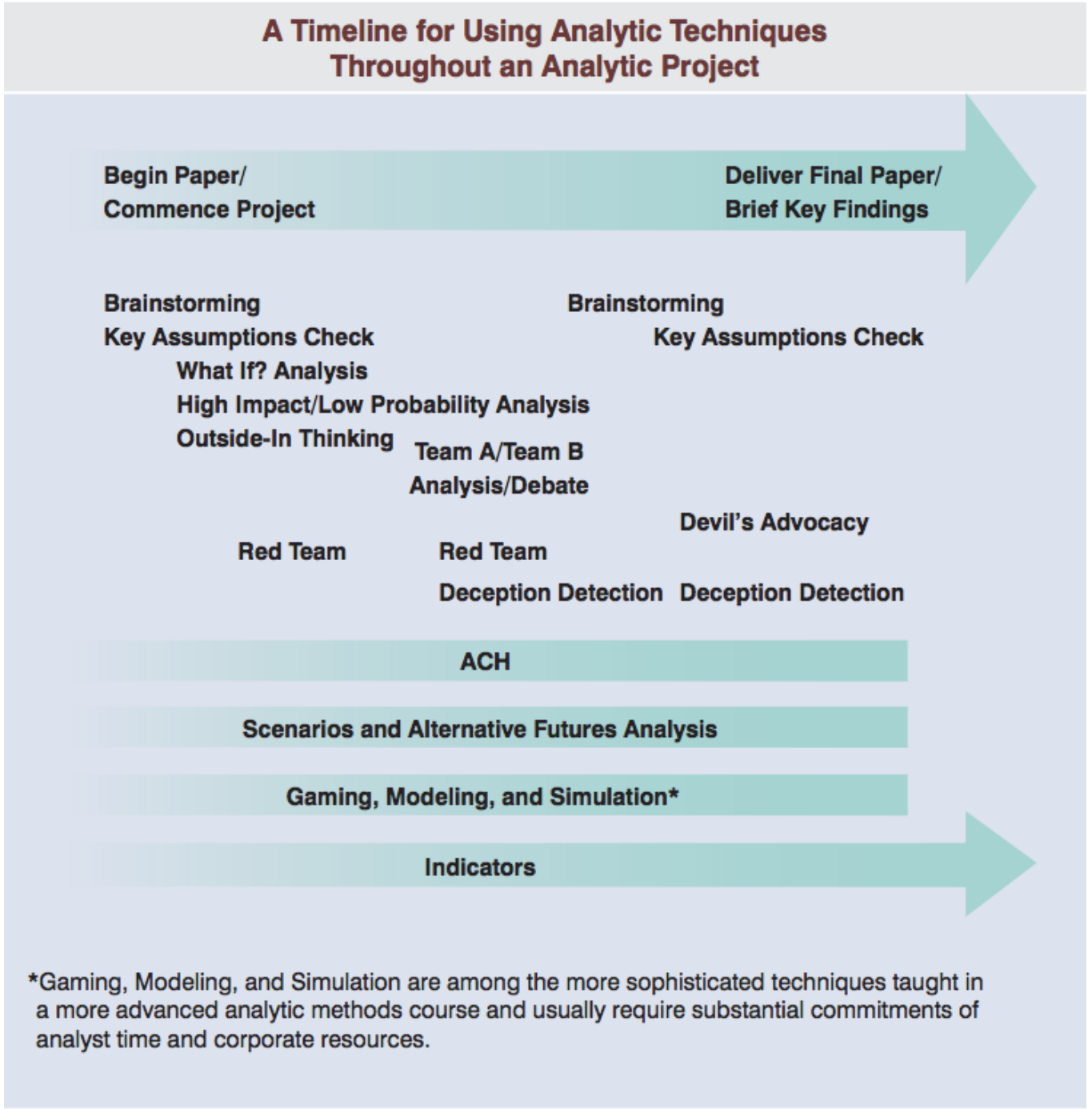
Challenge Analysis. Questa famiglia si riferisce a un insieme di tecniche dedicate a sfidare la mentalità attuale con tre tipi di sfide: autocritica, critica degli altri, critica dagli altri.

Conflict Management. L'obiettivo è incoraggiare, gestire e governare i conflitti di opinioni.

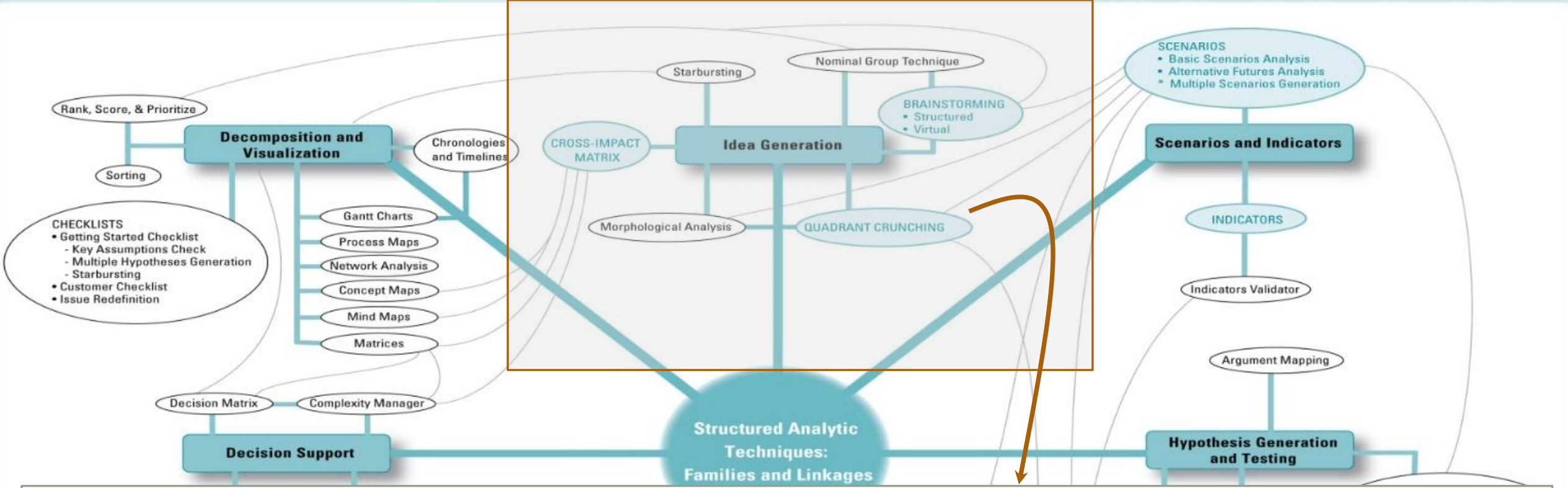


Come usare le SAT

Fonte: A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis



Esempi applicativi



Quadrant Crunching: serve ad identificare tutte le combinazioni potenzialmente fattibili tra diversi insiemi di variabili. Ciò aiuta a evitare sorprese esaminando più combinazioni possibili di variabili chiave selezionate e contrando le ipotesi.

Questa tecnica combina Key Assumptions Check e Multiple Scenarios Generation per generare una serie di scenari o storie alternative

Esempio: The DC Sniper

Il caso si riferisce ad una serie di aggressioni con armi da fuoco, pianificate, coordinate e messe in atto nell'arco di tre settimane dell'ottobre 2002 in Maryland, Virginia e Washington.

Dieci persone furono uccise e tre gravemente ferite in luoghi diversi e apparentemente privi di collegamento nell'area metropolitana di Washington D.C. e lungo la Interstate 95 in Virginia.

Dai dati inizialmente in possesso degli inquirenti prese subito piede l'ipotesi che l'aggressore, un singolo cecchino, inizialmente identificato come un uomo bianco con precedenti nell'esercito, si spostasse lungo la Interstate 495 (la Capital Beltway), probabilmente su un furgone o un camion di colore bianco.

Si veda: https://en.wikipedia.org/wiki/D.C._sniper_attacks per una descrizione del caso

Esempio: The DC Sniper

Il caso si riferisce ad una serie di aggressioni con armi da fuoco, pianificate, coordinate e messe in atto nell'arco di tre settimane dell'ottobre 2002 in Maryland, Virginia e Washington.

Dieci persone furono uccise e tre gravemente ferite in luoghi diversi e apparentemente privi di collegamento nell'area metropolitana di Washington D.C. e lungo la Interstate 95 in Virginia.

Dai dati inizialmente in possesso degli inquirenti prese subito piede l'ipotesi che l'aggressore, un singolo cecchino, inizialmente identificato come un uomo bianco con precedenti nell'esercito, si spostasse lungo la Interstate 495 (la Capital Beltway), probabilmente su un furgone o un camion di colore bianco.

Si veda: https://en.wikipedia.org/wiki/D.C._sniper_attacks per una descrizione del caso

L'assunzione inziale può essere considerata come risultato del ragionamento (connessione di punti)
Si pone il problema di valutarla

Esempio: The DC Sniper

Quadrant Crunching: si usa per valutare e contrastare le assunzioni chiave

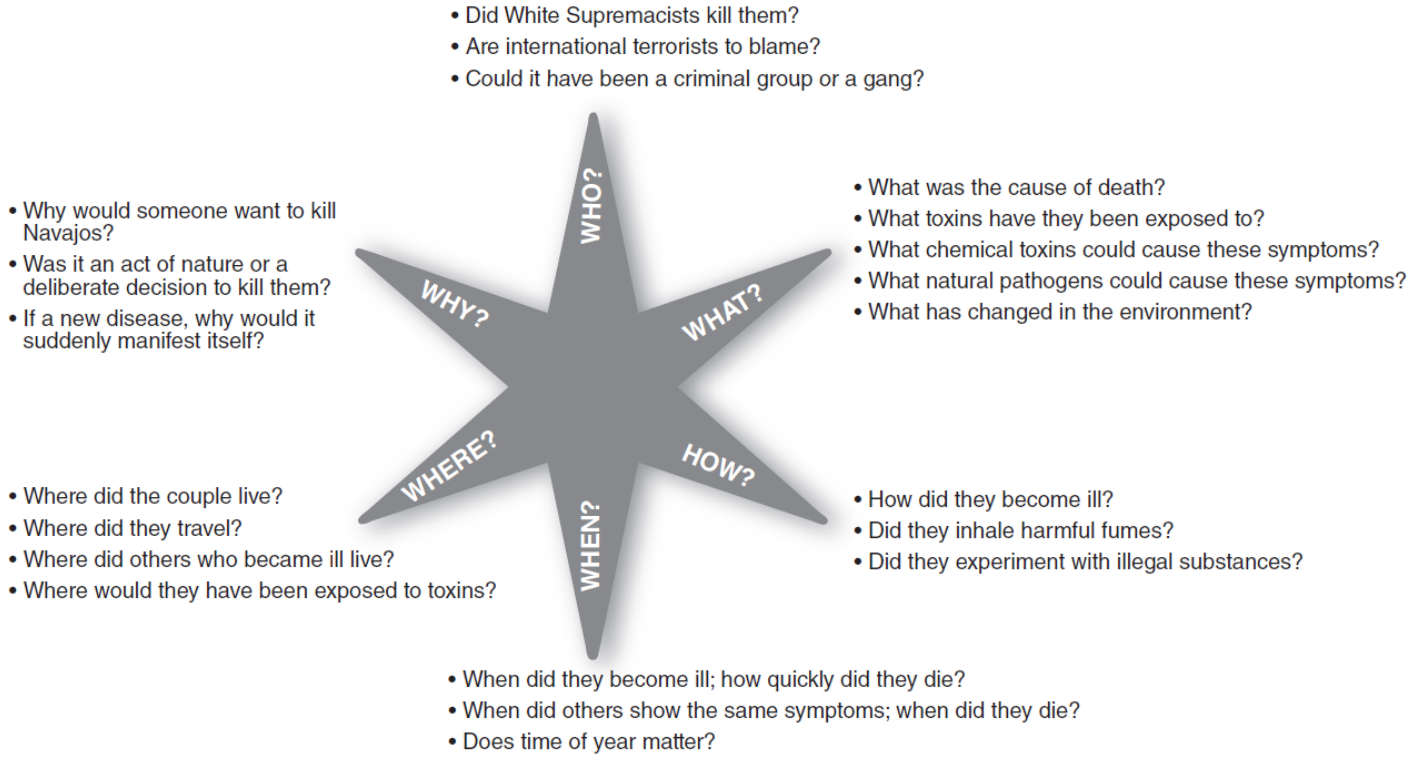
Gli **Step 1 e 2** di questa procedura consistono nel vagliare le assunzioni chiave e decomporle in *fatti* (noti e certi) ed altre componenti da esplorare

- In questo esercizio, si parte con la seguente assunzione: *A lone white male is conducting the shootings from a white van to extort money*
- In questa assunzione sono presenti dei fatti (e.g., è un fatto che ci sia una sparatoria) e altri termini da indagare (“lone”, “white”, “white van”, “extor money”)

Esempio: The DC Sniper

Lo **Step 3** consiste nel creare dimensioni che, tipicamente, (ma non sempre) sono su chi, cosa, quando, dove, perché e come.

- Tipiche prospettive dello Starbursting



Source: Cap. 11 del libro Cases in Intelligence Analysis

Esempio: The DC Sniper

Lo **Step 3** consiste nel creare dimensioni che, tipicamente, (ma non sempre) sono su chi, cosa, quando, dove, perché e come.

Table 11.11 ▶ DC Sniper Classic Quadrant Crunching™ Dimensions

Key Assumptions	Contrary Assumption	Contrary Dimensions	
A. Lone Attacker	Multiple Attackers	Team	Copycat Killers
B. White	Other Race	Black	Hispanic
C. White Van	Other Transportation Method	Sedan	On Foot
D. To Extort Money	Other Motivation	Seek Fame	Cause Terror

Source: Cap. 11 del libro Cases in Intelligence Analysis

Esempio: The DC Sniper

Assunzioni Chiave da esplorare

…nensioni che, tipicamente, (ma non sempre) sono su chi, cosa,

Table 11.11 ▶ DC Sniper Classic Quadrant Crunching™ Dimensions

Key Assumptions	Contrary Assumption	Contrary Dimensions	
A. Lone Attacker	Multiple Attackers	Team	Copycat Killers
B. White	Other Race	Black	Hispanic
C. White Van	Other Transportation Method	Sedan	On Foot
D. To Extort Money	Other Motivation	Seek Fame	Cause Terror

Source: Cap. 11 del libro Cases in Intelligence Analysis

Esempio: The DC Sniper

Assunzioni Chiave da esplorare

Assunzioni Contrarie per contrastare le assunzioni chiave

nensio mpre) sono su chi, cosa,

Table 11.11 ▶ DC Sniper Classic Quadrant Crunching™ Dimensions

Key Assumptions	Contrary Assumption	Contrary Dimensions	
A. Lone Attacker	Multiple Attackers	Team	Copycat Killers
B. White	Other Race	Black	Hispanic
C. White Van	Other Transportation Method	Sedan	On Foot
D. To Extort Money	Other Motivation	Seek Fame	Cause Terror

Source: Cap. 11 del libro Cases in Intelligence Analysis

Esempio: The DC Sniper

Dimensioni (contrarie) di analisi

Assunzioni Chiave da esplorare

Assunzioni Contrarie per contrastare le assunzioni chiave

nensio… …mpre) sono su chi, cosa,

Table 11.11 ▶ DC Sniper Classic Quadrant Crunching™ Dimensions

Key Assumptions	Contrary Assumption	Contrary Dimensions	
A. Lone Attacker	Multiple Attackers	Team	Copycat Killers
B. White	Other Race	Black	Hispanic
C. White Van	Other Transportation Method	Sedan	On Foot
D. To Extort Money	Other Motivation	Seek Fame	Cause Terror

Esempio: The DC Sniper

Lo **Step 4** consiste della creazione di combinazioni di array di queste ipotesi contrarie in un insieme di matrici 2 × 2

- Ad esempio, si crea un insieme di matrici a partire dalle dimensioni contrarie

Esempio: The DC Sniper

Source: Cap. 11 del libro Cases in Intelligence Analysis

Table 11.12 ▶ DC Sniper Classic Quadrant Crunching™: 2 × 2 Matrices

A/B	Multiple Attackers/Race			
1	Team Black		3	Team Hispanic
2	Copycat Killers Black		4	Copycat Killers Hispanic
A/C	Multiple Attackers/Transport			
1	Team Sedan		3	Team On Foot
2	Copycat Killers Sedan		4	Copycat Killers On Foot
A/D	Multiple Attackers/Motivation			
1	Team Seek Fame		3	Team Cause Terror
2	Copycat Killers Seek Fame		4	Copycat Killers Cause Terror
B/C	Race/Transport			
1	Black Sedan		3	Black On Foot
2	Hispanic Sedan		4	Hispanic On Foot
B/D	Race/Motivation			
1	Black Seek Fame		3	Black Cause Terror
2	Hispanic Seek Fame		4	Hispanic Cause Terror
C/D	Transport/Motivation			
1	Sedan Seek Fame		3	Sedan Cause Terror
2	On Foot Seek Fame		4	On Foot Cause Terror

6 matrici da quattro celle che si ottengono tramite le permutazioni delle dimensioni contrarie

Esempio: The DC Sniper

Source: Cap. 11 del libro Cases in Intelligence Analysis

Table 11.12 ▶ DC Sniper Classic Quadrant Crunching™: 2 × 2 Matrices

A/B	Multiple Attackers/Race			
1	Team Black		3	Team Hispanic
2	Copycat Killers Black		4	Copycat Killers Hispanic
A/C	Multiple Attackers/Transport			
1	Team Sedan		3	Team On Foot
2	Copycat Killers Sedan		4	Copycat Killers On Foot
A/D	Multiple Attackers/Motivation			
1	Team Seek Fame		3	Team Cause Terror
2	Copycat Killers Seek Fame		4	Copycat Killers Cause Terror
B/C	Race/Transport			
1	Black Sedan		3	Black On Foot
2	Hispanic Sedan		4	Hispanic On Foot
B/D	Race/Motivation			
1	Black Seek Fame		3	Black Cause Terror
2	Hispanic Seek Fame		4	Hispanic Cause Terror
C/D	Transport/Motivation			
1	Sedan Seek Fame		3	Sedan Cause Terror
2	On Foot Seek Fame		4	On Foot Cause Terror

La cella A/B-1 fa riferimento ad un ipotesi di attacco di un team di shooter neri

Esempio: The DC Sniper

Lo **Step 5** consiste della generazione di scenari possibili (da 1 a 3) per ogni cella della precedente matrice

- Esempio di scenario per la cella AB-1: "*Una squadra di cecchini neri sta conducendo attacchi in più località dell'area metropolitana di Washington, DC. I cecchini hanno formato una squadra nell'ultimo anno e hanno messo in moto il loro piano dopo diversi mesi di pianificazione e addestramento. I motivi alla base della creazione del loro e il numero esatto dei membri sono sconosciuti. Di conseguenza, se questa squadra è piuttosto piccola, potrebbero condurre gli attacchi uno alla volta. Se la squadra è più numerosa e dispersa, potrebbero condurre attacchi coordinati a orari prestabiliti*."

Esempio: The DC Sniper

Lo **Step 6** consiste nel rivedere gli scenari per escludere quelli meno pertinenti.

Si devono individuare dei criteri (es., fatti noti, precedent storici, etc.) per inclusione e esclusione degli scenari

- Ad esempio, nel nostro esercizio:
  - le celle con Copycat Killers si tendono ad escludere a causa delle evidenze balisitiche che affermano l'unicità dell'arma
  - le celle con On Foot si tendono ad escludere perchè sembra improbabile che che il tiratore, armato di fucile, possa passare inosservato sulla scena del delitto. Anche perché il tipo di fucile ipotizzato dalle prove balistiche non si disassembla facilmente.

Esempio: The DC Sniper

Table 11.12 ▶ DC Sniper Classic Quadrant Crunching™: 2 × 2 Matrices

A/B	Multiple Attackers/Race		
1	Team Black	3	Team Hispanic
2	Copycat Killers Black	4	Copycat Killers Hispanic
A/C	**Multiple Attackers/Transport**		
1	Team Sedan	3	Team On Foot
2	Copycat Killers Sedan	4	Copycat Killers On Foot
A/D	**Multiple Attackers/Motivation**		
1	Team Seek Fame	3	Team Cause Terror
2	Copycat Killers Seek Fame	4	Copycat Killers Cause Terror
B/C	**Race/Transport**		
1	Black Sedan	3	Black On Foot
2	Hispanic Sedan	4	Hispanic On Foot
B/D	**Race/Motivation**		
1	Black Seek Fame	3	Black Cause Terror
2	Hispanic Seek Fame	4	Hispanic Cause Terror
C/D	**Transport/Motivation**		
1	Sedan Seek Fame	3	Sedan Cause Terror
2	On Foot Seek Fame	4	On Foot Cause Terror

Esempio: The DC Sniper

Table 11.12 ▶ DC Sniper Classic Quadrant Crunching™: 2 × 2 Matrices

A/B	Multiple Attackers/Race			
1	Team Black		3	Team Hispanic
2	Copycat Killers Black		4	Copycat Killers Hispanic
A/C	Multiple Attackers/Transport			
1	Team Sedan		3	Team On Foot
2	Copycat Killers Sedan		4	Copycat Killers On Foot
A/D	Multiple Attackers/Motivation			
1	Team Seek Fame		3	Team Cause Terror
2	Copycat Killers Seek Fame		4	Copycat Killers Cause Terror
B/C	Race/Transport			
1	Black Sedan		3	Black On Foot
2	Hispanic Sedan		4	Hispanic On Foot
B/D	Race/Motivation			
1	Black Seek Fame		3	Black Cause Terror
2	Hispanic Seek Fame		4	Hispanic Cause Terror
C/D	Transport/Motivation			
1	Sedan Seek Fame		3	Sedan Cause Terror
2	On Foot Seek Fame		4	On Foot Cause Terror

Le celle con «Team» potrebbero spiegare come mai il cecchino scompare così velocemente. Una persona spara e l'altra funge da autista / vedetta.

Esempio: The DC Sniper

Table 11.12 ▶ DC Sniper Classic Quadrant Crunching™: 2 × 2 Matrices

A/B	Multiple Attackers/Race			
1	Team Black		3	Team Hispanic
2	Copycat Killers Black		4	Copycat Killers Hispanic
A/C	Multiple Attackers/Transport			
1	Team Sedan		3	Team On Foot
2	Copycat Killers Sedan		4	Copycat Killers On Foot
A/D	Multiple Attackers/Motivation			
1	Team Seek Fame		3	Team Cause Terror
2	Copycat Killers Seek Fame		4	Copycat Killers Cause Terror
B/C	Race/Transport			
1	Black Sedan		3	Black On Foot
2	Hispanic Sedan		4	Hispanic On Foot
B/D	Race/Motivation			
1	Black Seek Fame		3	Black Cause Terror
2	Hispanic Seek Fame		4	Hispanic Cause Terror
C/D	Transport/Motivation			
1	Sedan Seek Fame		3	Sedan Cause Terror
2	On Foot Seek Fame		4	On Foot Cause Terror

Le celle con «Team» potrebbero spiegare come mai il cecchino scompare così velocemente. Una persona spara e l'altra funge da autista / vedetta.

Le celle con entrambe le opzioni di razza sembrano ugualmente probabili e vale la pena considerare entrambe oltre all'ipotesi principale, (che è solitario razza bianca)

Esempio: The DC Sniper

Table 11.12 ▶ DC Sniper Classic Quadrant Crunching™: 2 × 2 Matrices

A/B	Multiple Attackers/Race			
1	Team Black		3	Team Hispanic
2	Copycat Killers Black		4	Copycat Killers Hispanic
A/C	Multiple Attackers/Transport			
1	Team Sedan		3	Team On Foot
2	Copycat Killers Sedan		4	Copycat Killers On Foot
A/D	Multiple Attackers/Motivation			
1	Team Seek Fame		3	Team Cause Terror
2	Copycat Killers Seek Fame		4	Copycat Killers Cause Terror
B/C	Race/Transport			
1	Black Sedan		3	Black On Foot
2	Hispanic Sedan		4	Hispanic On Foot
B/D	Race/Motivation			
1	Black Seek Fame		3	Black Cause Terror
2	Hispanic Seek Fame		4	Hispanic Cause Terror
C/D	Transport/Motivation			
1	Sedan Seek Fame		3	Sedan Cause Terror
2	On Foot Seek Fame		4	On Foot Cause Terror

Le celle con «Team» potrebbero spiegare come mai il cecchino scompare così velocemente. Una persona spara e l'altra funge da autista / vedetta.

Le celle con entrambe le opzioni di razza sembrano ugualmente probabili e vale la pena considerare entrambe oltre all'ipotesi principale, (che è solitario razza bianca)

Le cellule con "Causa terrore" sembrano realistiche poiché gli attacchi stavano causando una paura grave e diffusa.

Esempio: The DC Sniper

Lo **Step 7** si basa sullo sviluppo di indicatori per gli scenari selezionati

L'obiettivo dello sviluppo di indicatori per ogni scenario è aiutare gli investigatori a cercare ed essere consapevoli di un'ampia gamma di scenari e indicazioni che l'uno o l'altro scenario potrebbe emergere.

- Ad esempio, gli indicatori dello scenario B/C-1, un cecchino nero che usa una berlina, incoraggerebbe gli investigatori a non ignorare ulteriori segnalazioni di berline che lasciano l'area e a rivedere le precedenti segnalazioni e contattare i testimoni che in precedenza hanno segnalato la presenza di una berlina

Esempio: The DC Sniper

Conclusione del caso: *The snipers were John Allen Muhammad (age 41 at the time) and Lee Boyd Malvo (age 17 at the time), who traveled in a blue 1990 Chevrolet Caprice sedan* (source Wikipedia page of DC Sniper)

Il valore analitico di questa tecnica consiste nel rispondere alla domanda: Quali scenari alternativi avrebbero dovuto perseguire gli investigatori, e perché?

Esaminando criticamente ogni ipotesi e come potrebbe svolgersi un'ipotesi contraria, gli analisti possono valutare meglio il loro livello di fiducia nelle loro previsioni, la forza della loro ipotesi guida e la probabilità del loro scenario guida

Si nota, infatti, che le celle in grigio rappresentano ciò che stava effettivamente accadendo, in particolare A/B-1, A/C-1 e B/C-1.

Table 11.12 ▶ DC Sniper Classic Quadrant Crunching™: 2 × 2 Matrices

A/B	Multiple Attackers/Race			
1	Team Black		3	Team Hispanic
2	Copycat Killers Black		4	Copycat Killers Hispanic
A/C	Multiple Attackers/Transport			
1	Team Sedan		3	Team On Foot
2	Copycat Killers Sedan		4	Copycat Killers On Foot
A/D	Multiple Attackers/Motivation			
1	Team Seek Fame		3	Team Cause Terror
2	Copycat Killers Seek Fame		4	Copycat Killers Cause Terror
B/C	Race/Transport			
1	Black Sedan		3	Black On Foot
2	Hispanic Sedan		4	Hispanic On Foot
B/D	Race/Motivation			
1	Black Seek Fame		3	Black Cause Terror
2	Hispanic Seek Fame		4	Hispanic Cause Terror
C/D	Transport/Motivation			
1	Sedan Seek Fame		3	Sedan Cause Terror
2	On Foot Seek Fame		4	On Foot Cause Terror

Grazie per l’attenzione