

Contromisure tecniche alla sorveglianza nell'era digitale

— Il Metodo SPECTRA

Sommario

Abstract	3
1. Introduzione	4
2. Evoluzione della sorveglianza tecnica	8
3. Modelli operativi di sorveglianza	14
4. Il dispositivo mobile come vettore di sorveglianza	18
5. Limiti della bonifica ambientale tradizionale	22
6. La bonifica logica dei dispositivi	26
7. Limiti degli approcci basati solo su IOC	30
8. Approccio ibrido: IOC e analisi pattern-centrica	34
9. Principi della metodologia di analisi passiva	40
10. Limiti tecnici e ambiguità dell'analisi	44
11. Implicazioni per la bonifica moderna	48
Conclusioni	56
Bibliografia	58
L'autore	59

Sintesi del lavoro

Negli ultimi due decenni il punto di ascolto della sorveglianza tecnica si è spostato dall'ambiente fisico al dispositivo personale: non si intercetta più il segnale che esce dalla stanza, ma il contenuto alla sorgente. In questo scenario la bonifica non può più essere interpretata come semplice rilevazione radioelettrica, ma come un processo di analisi multidominio che integra spettro radio, traffico di rete, sistemi digitali e comportamento dei dispositi-

vi. Il white paper analizza l'evoluzione tecnica della sorveglianza, i limiti della bonifica ambientale tradizionale e i principi di un'analisi passiva, non attributiva e pattern-centrica. Introduce quindi il metodo SPECTRA, che formalizza un approccio integrato in cui la sicurezza non deriva dalla singola tecnica, ma dalla correlazione strutturata di più domini nel tempo.

PAROLE CHIAVE

TSCM

Captatori informatici

Sorveglianza tecnica

Bonifica multidominio

Analisi pattern-centrica

Metodo SPECTRA

Controsorveglianza

01

Dall'ambiente al dispositivo

Il punto di raccolta non è più la stanza, ma lo smartphone: dall'hardware occulto al software residente.

02

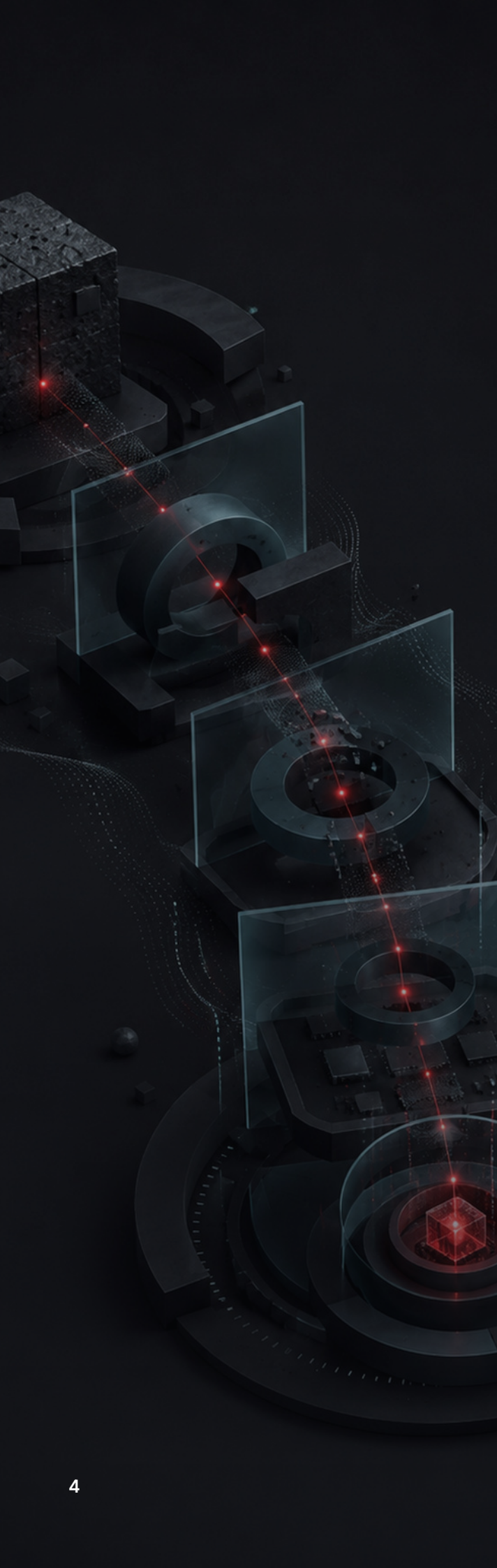
Bonifica multidominio

Spettro radio, traffico di rete, sistemi digitali e comportamento dei dispositivi, analizzati come un unico processo.

03

Correlazione nel tempo

Con SPECTRA la sicurezza non deriva dalla singola tecnica, ma dall'integrazione strutturata di più domini.



01

CAPITOLO 01

Introduzione

Negli ultimi due decenni il modo di condurre la sorveglianza tecnica è cambiato profondamente. Fino ai primi anni 2000 intercettare significava collocare un dispositivo fisico nell'ambiente: una microspia, un trasmettitore RF, un apparecchio GSM autonomo. Oggi il punto di ascolto si è spostato dentro il dispositivo della persona, lo smartphone o il computer, che diventa esso stesso lo strumento di intercettazione. Non è cambiata solo la tecnologia, ma il metodo stesso della sorveglianza, e questo ha conseguenze dirette anche per chi si occupa di contromisure: non basta più cercare un oggetto nascosto nella stanza.

In tale contesto, la bonifica tecnica non può più essere considerata esclusivamente come attività di rilevazione radioelettrica, ma deve essere interpretata come un processo di analisi multidominio che coinvolge lo spettro radio, il traffico di rete, i sistemi digitali e il comportamento dei dispositivi presenti nell'ambiente.

Il presente white paper ha tre obiettivi principali: chiarire cosa siano, dal punto di vista tecnico, i captatori informatici; descrivere come l'evoluzione tecnologica abbia modificato il concetto stesso di sorveglianza tecnica; introdurre la necessità di una metodologia di bonifica multidominio, integrata e strutturata. Con captatore informatico si intende qui un software di intercettazione installato direttamente sul dispositivo bersaglio (smartphone, tablet o computer), capace di acquisire dati e attivare i sensori da remoto; il termine spyware indica più in generale software di sorveglianza occulto, di cui il captatore informatico costituisce una specifica categoria d'uso investigativo o istituzionale. L'approccio adottato è esclusivamente tecnico-operativo. Non vengono affrontati profili giuridici o valutazioni di natura politica: l'analisi si concentra su architettura, funzionamento e implicazioni metodologiche.

1.1 Dal trasmettitore RF al software residente

Nel modello classico di sorveglianza ambientale, l'elemento centrale era il trasmettitore. Un dispositivo fisico veniva collocato in un ambiente e trasmetteva su una determinata frequenza radio un segnale audio o dati. La rilevazione si basava principalmente sull'analisi dello spettro elettromagnetico, sull'identificazione di portanti anomale, sullo studio della persistenza del segnale e sulla correlazione tra presenza del segnale e attività ambientale.

Accanto all'analisi dello spettro elettromagnetico, l'attività di bonifica ha sempre previsto anche un'ispezione manuale e strumentale dell'ambiente. L'analizzatore di spettro consente di individuare emissioni radio anomale, ma non può sostituire la verifica fisica degli spazi, degli oggetti e delle infrastrutture presenti nell'area oggetto di analisi. Per questo motivo, nelle attività TSCM l'analisi RF viene tradizionalmente affiancata da ispezioni visive, controlli strumentali e verifica diretta degli apparati, anche attraverso strumenti specifici come i rilevatori di giunzioni non lineari, finalizzati all'individuazione di dispositivi elettronici occultati pur in assenza di emissioni radio attive. In questo paradigma, l'oggetto principale della ricerca rimane comunque un'emissione RF riconducibile a un trasmettitore presente nell'ambiente.

Con l'introduzione dei captatori informatici, l'oggetto dell'intercettazione non è più esterno al bersaglio, ma interno. Il software si integra nel sistema operativo del dispositivo e acquisisce informazioni direttamente alla sorgente: microfono, fotocamera, tastiera, file system, memoria volatile, traffico dati. Il passaggio è concettualmente netto: non si intercetta più il segnale che esce dall'ambiente, ma il contenuto prima che venga cifrato o dopo che sia stato decifrato. Questo spostamento elimina completamente la necessità di una trasmissione radio dedicata. Il

traffico generato dal captatore utilizza la connettività legittima del dispositivo (rete cellulare o Wi-Fi), mimetizzandosi nel flusso dati ordinario.

Non si intercetta più il segnale che esce dall'ambiente, ma il contenuto prima che venga cifrato o dopo che sia stato decifrato.

1.2 Ridefinizione del concetto di bonifica

Le metodologie TSCM tradizionali restano valide nel loro ambito, ma non coprono la totalità dello scenario attuale. Un analizzatore di spettro non può rilevare codice eseguibile residente su un sistema operativo, così come un detector RF non può intercettare un flusso cifrato che viaggia su HTTPS verso un server remoto. Il problema non è l'obsolescenza degli strumenti, ma l'ampliamento del dominio di minaccia.

La bonifica moderna deve quindi estendersi dal dominio elettromagnetico al dominio logico e comportamentale. Ciò implica l'analisi del traffico dati con approccio pattern-based, lo studio delle connessioni persistenti e dei nodi dominanti, la verifica delle anomalie comportamentali del sistema, la correlazione temporale tra attività utente e attività di rete, nonché l'acquisizione e l'analisi di artefatti diagnostici (log, dump, sdiagnose, PCAP).

Non si tratta di cercare un file malevolo in senso tradizionale. Un captatore evoluto può operare con privilegi elevati, sfruttare vulnerabilità sconosciute o utilizzare tecniche di offuscamento tali da rendere inefficace una semplice scansione antivirus. L'analisi deve quindi spostarsi dai singoli indicatori di compromissione (IOC) ai pattern comportamentali.

1.3 Sorveglianza tecnica: continuità e discontinuità

È importante chiarire che la sorveglianza tradizionale non è scomparsa. Le microspie ambientali esistono ancora, così come i trasmettitori RF, i registratori stand-alone e altri dispositivi fisici. Ciò che è cambiato è il rapporto tra costo, efficacia e rischio operativo.

Un captatore informatico consente intercettazione continuativa, accesso remoto, acquisizione di dati strutturati (chat, file, credenziali) e attivazione selettiva dei sensori. Dal punto di vista tecnico, rappresenta un'evoluzione verso un modello di sorveglianza meno visibile sul piano fisico ma più invasivo sul piano informativo. Questo scenario produce una conseguenza diretta: la bonifica non può più essere concepita come esclusivamente ambientale.

1.4 Il messaggio centrale

La bonifica tecnica nel contesto attuale richiede un cambio di paradigma. L'analizzatore di spettro resta uno strumento imprescindibile e la ricerca di emissioni anomale rimane fondamentale, ma non è più sufficiente. La minaccia si è progressivamente estesa al livello software, alle infrastrutture di rete e al comportamento dei sistemi. Questo scenario richiede metodologie ibride, integrate e documentabili, capaci di correlare osservazioni provenienti da domini tecnici differenti.

È importante precisare che l'approccio multidominio descritto in questo lavoro non rappresenta l'introduzione di tecniche completamente nuove. In contesti operativi avanzati, attività che combinano analisi dello spettro radio, osservazione del traffico di rete e verifica tecnica dei dispositivi sono già adottate, spesso in modo non formalizzato. Ciò che manca è una formalizzazione metodologica esplicita che descriva queste attività come parte di un unico processo analitico strutturato.

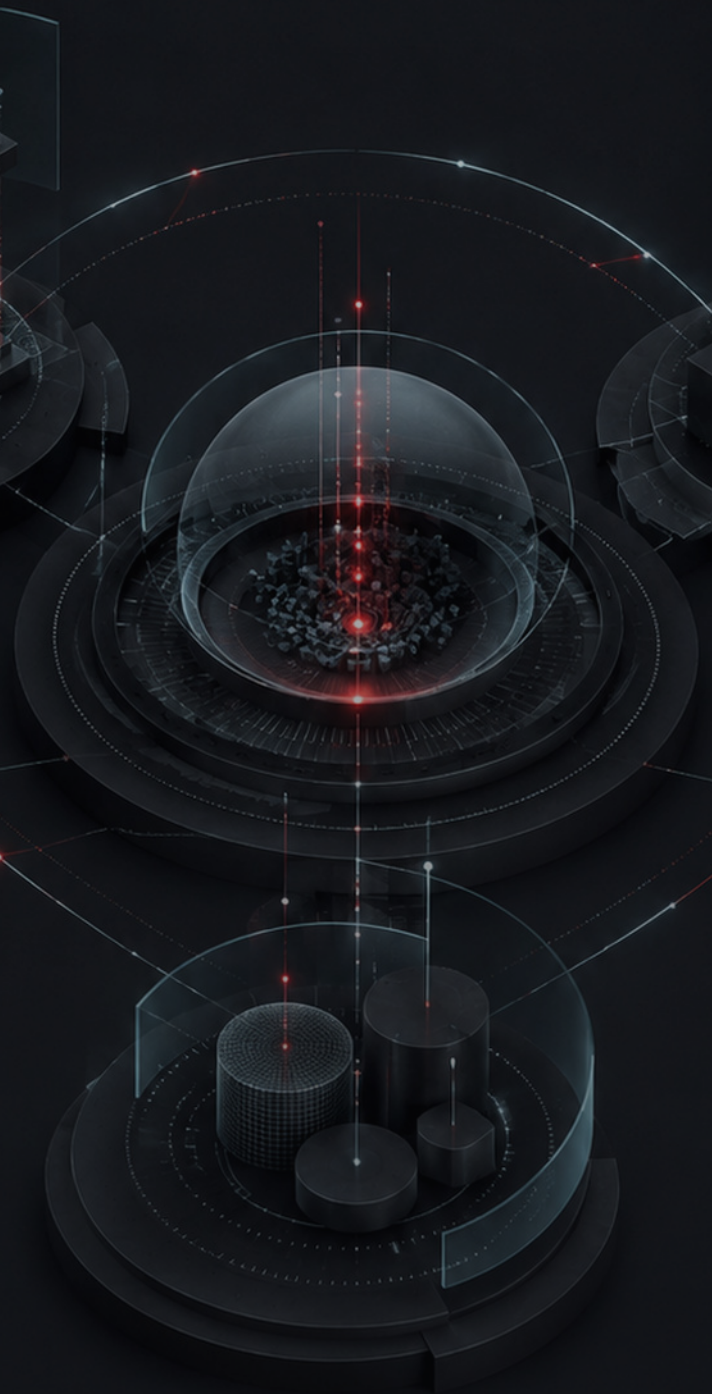
Il metodo SPECTRA (Security Pattern Environment Correlation Technical Reconnaissance & Analysis) nasce con l'obiettivo di colmare questa lacuna, sistematizzando e rendendo esplicito un approccio integrato basato su integrazione multidominio, correlazione di pattern tecnici e analisi nel tempo. Il contributo del metodo non consiste nell'introduzione di nuove tecnologie di rilevazione, ma nella formalizzazione di un processo analitico in cui la sicurezza è il risultato della combinazione strutturata delle tecniche e non della loro applicazione isolata.

02

CAPITOLO 02

Evoluzione della sorveglianza tecnica

Dalla trasmissione ambientale
alla compromissione del dispositi-
tivo



L'evoluzione della sorveglianza tecnica non è stata lineare ma progressiva, guidata da tre fattori principali: miniaturizzazione elettronica, digitalizzazione del segnale e integrazione con infrastrutture di rete. L'asse evolutivo mostra una traiettoria chiara: la raccolta informativa si è progressivamente spostata dall'ambiente fisico al dispositivo personale.

2.1 Microspie analogiche RF

Le prime soluzioni di intercettazione ambientale diffuse in ambito investigativo e commerciale erano basate su trasmettitori analogici in banda VHF/UHF con modulazione di frequenza (FM). Dal punto di vista tecnico, l'architettura era semplice: microfono, preamplificatore, oscillatore RF, modulazione FM, antenna. Nella configurazione più diffusa, il dispositivo trasmetteva in modo continuo un segnale audio modulato, con potenze generalmente comprese tra pochi milliwatt e alcune decine di milliwatt. La portata operativa dipendeva dal contesto ambientale e dalla sensibilità del ricevitore.

Questa tecnologia presentava caratteristiche precise: trasmissione generalmente continua (salvo dispositivi passivi o attivati esternamente), assenza di cifratura, spettro stabile e facilmente individuabile, spesso consumo energetico continuo.

Proprio in questo contesto tecnologico, durante la Guerra Fredda, si sviluppano negli Stati Uniti le prime attività sistematiche di ricerca di dispositivi di ascolto clandestini negli ambienti sensibili, in particolare nelle sedi diplomatiche e nelle installazioni governative. Alcuni episodi storici contribuirono a evidenziare la vulnerabilità degli ambienti alle tecniche di sorveglianza elettronica e a far nascere le moderne attività di contro sorveglianza tecnica. Nel 1952, il celebre dispositivo di ascolto nascosto nel Great Seal dell'ambasciata statunitense a Mosca venne scoperto dopo anni di intercettazioni clandestine, quando operatori radio intercettarono una trasmissione

anomala proveniente dall'edificio durante attività di monitoraggio delle frequenze. Il dispositivo, donato dai sovietici all'ambasciatore statunitense nel 1945 e rimasto attivo per circa sette anni, era stato progettato dall'ingegnere sovietico Lev Termen: un microfono passivo a risonanza privo di alimentazione interna, attivato da un segnale radio esterno e quindi particolarmente difficile da individuare, un caso tecnicamente distinto dalle successive microspie RF a trasmissione continua. Negli anni Settanta, durante la costruzione della nuova ambasciata USA a Mosca, furono individuati numerosi dispositivi di ascolto integrati direttamente nella struttura dell'edificio, a dimostrazione del livello di sofisticazione delle tecniche di sorveglianza impiegate in quel periodo.

In questo contesto operativo si afferma progressivamente il termine Technical Surveillance Countermeasures (TSCM), adottato negli ambienti militari e di intelligence statunitensi a partire dagli anni Sessanta per indicare l'insieme delle procedure tecniche finalizzate all'individuazione e neutralizzazione dei sistemi di sorveglianza elettronica. La metodologia di rilevazione è stata storicamente basata principalmente sull'analisi radioelettrica (sweep di banda, analisi spettrale, identificazione di portanti anomale e triangolazione delle sorgenti), affiancata dall'ispezione fisica dell'ambiente e dall'utilizzo di strumenti dedicati come i rilevatori di giunzioni non lineari. In questa fase storica, la sorveglianza era fisicamente localizzata nell'ambiente: il dispositivo nascosto rappresentava il punto di emissione e quindi il punto di vulnerabilità.

2.2 Trasmettitori digitali RF

Con l'introduzione della digitalizzazione del segnale, la microspia ambientale subisce una prima evoluzione significativa. Il segnale audio viene campionato, digitalizzato e trasmesso attraverso modulazioni più complesse, spesso in modalità burst o con tecniche spread spectrum. Questo comporta due conseguenze operative ri-

levanti: la riduzione del tempo di trasmissione attiva e una maggiore difficoltà di intercettazione con strumenti tradizionali. La possibilità di introdurre cifratura di base aumenta la resilienza del sistema, mentre la trasmissione intermittente rende meno evidente la presenza di una portante continua.

Dal punto di vista TSCM, diventa necessario affiancare allo sweep spettrale una componente di monitoraggio temporale e analisi comportamentale del segnale. Non è più sufficiente cercare una portante stabile: occorre osservare pattern, persistenza e correlazioni temporali. La sorveglianza resta nell'ambiente, ma diventa meno visibile.

2.3 Sistemi cellulari (2G, 3G, 4G)

L'integrazione di moduli GSM rappresenta una discontinuità tecnica sostanziale. Il dispositivo non trasmette più verso un ricevitore locale, ma utilizza l'infrastruttura cellulare pubblica. L'audio viene inviato attraverso la rete mobile, eliminando il vincolo geografico del raggio di azione. Le caratteristiche principali sono l'attivazione remota tramite chiamata o SMS, la gestione dinamica della potenza in uplink, l'integrazione con rete cellulare legittima e l'assenza di portanti RF anomale dedicate.

Il segnale emesso non è distinguibile, a livello macroscopico, da quello di un normale terminale mobile: la microspia diventa un utente cellulare silente. Per la bonifica, questo comporta uno spostamento metodologico verso l'analisi dell'uplink, lo studio della potenza indoor, il monitoraggio persistente nel tempo e la correlazione tra attività radio e contesto ambientale. In questa fase, la sorveglianza utilizza infrastruttura legittima e si mimetizza nel traffico ordinario.

2.4 Sorveglianza via rete dati

Con la diffusione di Wi-Fi e connettività broadband, la trasmissione radio dedicata diventa progressivamente secondaria. Il dispositivo ambientale può ora collegarsi a una rete Wi-Fi esistente, trasmettere flussi audio/video via IP, utilizzare protocolli cifrati (per esempio TLS) e comunicare verso server remoti o cloud. La componente RF non scompare, ma viene inglobata in un'infrastruttura dati ordinaria.

Dal punto di vista tecnico, l'attività di intercettazione diventa difficilmente distinguibile dal traffico legittimo, soprattutto in ambienti con elevata densità di dispositivi connessi. La bonifica richiede quindi analisi del traffico di rete, identificazione di endpoint sospetti, studio dei flussi persistenti e correlazione temporale tra traffico e attività ambientale. Il centro della sorveglianza si avvicina alla rete.

2.5 Captatori informatici su smartphone e PC

L'ultima fase evolutiva non consiste nell'occultare meglio un dispositivo ambientale, ma nell'eliminare il dispositivo esterno. Con l'introduzione di captatori informatici, spyware e Remote Access Trojan, la piattaforma di intercettazione coincide con il dispositivo della vittima. Il software può accedere direttamente a microfono, fotocamera, sensori, dati locali, comunicazioni cifrate e account cloud.

La trasmissione dei dati avviene attraverso canali di rete già attivi e pienamente legittimi (rete mobile o Wi-Fi): non esiste più una portante RF autonoma da rilevare, e il vettore è il traffico dati ordinario. La differenza strutturale è rilevante: la microspia ambientale è un oggetto fisico da individuare, mentre il captatore informatico è un software integrato nel dispositivo. La superficie di attacco si sposta definitivamente dal perimetro fisico al perimetro digitale.

2.5.1 Origine della bonifica dei dispositivi informatici

Con la progressiva digitalizzazione delle comunicazioni, tra la fine degli anni Novanta e i primi anni Duemila, le attività di intercettazione hanno iniziato a spostarsi dall'installazione di dispositivi fisici nell'ambiente alla compromissione diretta dei terminali informatici utilizzati dal soggetto monitorato. Parallelamente, anche le attività di contromisure tecniche hanno dovuto evolversi: accanto alla tradizionale bonifica radioelettrica si è progressivamente sviluppata la necessità di analizzare computer e dispositivi mobili alla ricerca di software intrusivi, spyware e strumenti di accesso remoto. Questa evoluzione ha portato alla nascita di una nuova dimensione della bonifica tecnica, orientata non più soltanto alla rilevazione di trasmettitori RF, ma anche all'analisi del comportamento software e del traffico generato dai dispositivi digitali presenti nell'ambiente.

2.5.2 Casi documentati di captatori informatici

L'impiego di captatori informatici non rappresenta un'ipotesi teorica, ma una pratica documentata in contesti giudiziari, investigativi e di intelligence. Alcuni casi emersi pubblicamente mostrano in modo concreto il passaggio dalla sorveglianza ambientale basata su dispositivi esterni alla compromissione del terminale personale.

Un caso noto in ambito giudiziario italiano è quello che ha coinvolto Luca Palamara nel 2019. Nell'ambito dell'indagine della Procura di Perugia, l'utilizzo di un captatore informatico sul dispositivo mobile dell'indagato consentì la registrazione di conversazioni ambientali tramite il microfono dello smartphone. Il caso rese evidente, anche nel dibattito pubblico, come il telefono cellulare possa essere trasformato in un sensore ambientale remoto senza necessità di installare apparati fisici nei luoghi frequentati dal soggetto monitorato.

Un secondo caso di rilievo internazionale riguarda Pegasus, spyware sviluppato dalla società israeliana NSO Group. Analisi tecniche, attività di ricerca indipendente e inchieste giornalistiche hanno documentato la capacità di tale software di compromettere dispositivi mobili e acquisire comunicazioni, dati locali, posizione geografica e attivazioni dei sensori, confermando il livello di maturità raggiunto dai moderni strumenti di sorveglianza software.

Nel contesto italiano va inoltre ricordato il caso Exodus, spyware sviluppato dalla società eSurv e utilizzato in attività investigative tra il 2016 e il 2019. La sua esposizione pubblica, anche a seguito dell'individuazione di alcune componenti all'interno del Google Play Store, ha evidenziato criticità operative e di controllo nella gestione di tecnologie intrusive destinate all'intercettazione.

A questi episodi si aggiunge il caso della società Hacking Team, azienda italiana con sede a Milano specializzata nello sviluppo di sistemi di intrusione remota destinati a contesti governativi e investigativi. Nel luglio 2015 la società fu coinvolta in un'importante violazione informatica che portò alla pubblicazione online di documentazione interna, codice sorgente ed elenchi di clienti, contribuendo ad ampliare il dibattito internazionale sull'impiego dei captatori informatici e degli strumenti di sorveglianza offensiva. Anche questo caso ha mostrato come la sorveglianza tecnica contemporanea si sia progressivamente spostata dall'hardware occulto al software residente.

Questi casi, pur differenti per contesto, finalità e livello di sofisticazione, convergono su un punto tecnico essenziale: il dispositivo personale dell'utente può diventare esso stesso il vettore primario di acquisizione ambientale e informativa.

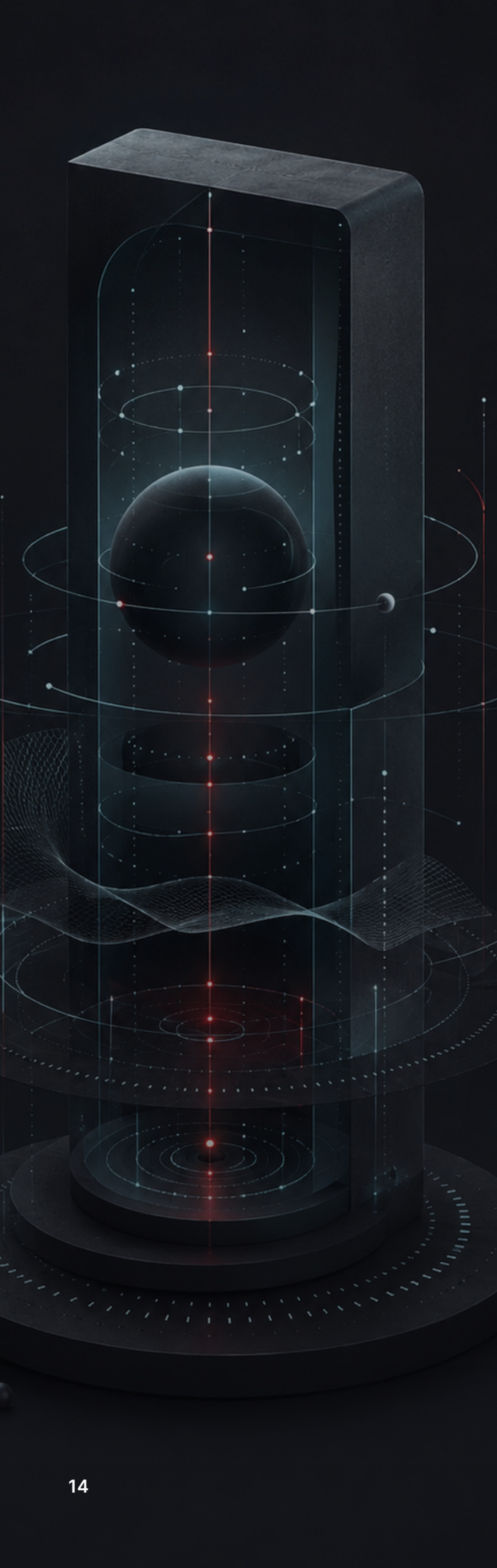
CONCLUSIONE

L'analisi storica evidenzia una trasformazione coerente, articolata in cinque fasi: trasmissione RF diretta; digitalizzazione e mimetizzazione radio; integrazione con rete cellulare; trasmissione IP; compromissione software del dispositivo. Il punto di raccolta informativa non è più la stanza, ma lo smartphone; non è più l'oggetto nascosto, ma il sistema operativo. La sorveglianza tecnica si è progressivamente spostata dall'ambiente fisico al dispositivo personale. Questo passaggio non è solo tecnologico, ma metodologico: la bonifica moderna non può più limitarsi alla ricerca radioelettrica o all'ispezione manuale, ma deve integrare analisi di rete, analisi comportamentale e verifica del dispositivo digitale.



**Non esiste una sola microspia:
esistono modelli operativi
differenti.**

— IL METODO SPECTRA · CAPITOLO 03



03

CAPITOLO 03

Modelli operativi di sorveglianza

La sorveglianza tecnica non è un oggetto, ma un modello. Nel linguaggio comune si parla di microspia come se si trattasse di un dispositivo isolato, identificabile e definito. Dal punto di vista tecnico-operativo, questa rappresentazione è fuorviante. Nella realtà esistono modelli operativi di sorveglianza, cioè architetture strutturate che combinano vettori, infrastrutture, logiche di gestione e obiettivi informativi. La differenza non è nel singolo strumento, ma nel modo in cui viene integrato in un sistema.

In questo capitolo vengono classificati tre macro-modelli: sorveglianza statale, sorveglianza privata/professionale e scenari amatoriali. La classificazione non riguarda il giudizio etico, ma la struttura tecnica e organizzativa.

3.1 Sorveglianza statale

La sorveglianza statale si distingue per l'approccio metodologico e per l'integrazione multidominio. Non si tratta di un'azione impulsiva o improvvisata: è preceduta da uno studio di fattibilità che include l'analisi del profilo tecnico del target, la mappatura dell'ecosistema digitale e ambientale, la valutazione dei vettori disponibili e la stima del rischio di rilevazione. La selezione del vettore non è casuale, ma orientata al miglior rapporto tra efficacia informativa, sostenibilità operativa e probabilità di successo.

Elemento distintivo è l'uso combinato di tecniche. La sorveglianza statale tende a non affidarsi a un singolo canale, ma a costruire ridondanza tra dominio radio, dominio rete, dominio fisico e dominio umano. L'architettura risultante è un sistema coordinato, spesso con infrastruttura proprietaria o dedicata, gestione centralizzata dei dati e capacità di integrazione tra diverse fonti

informative. In questo modello non esiste la microspia isolata: esiste una catena informativa integrata.

3.2 Sorveglianza privata / professionale

La sorveglianza privata o professionale presenta caratteristiche intermedie. Può essere strutturata e persistente, ma generalmente opera con strumenti commerciali, soluzioni customizzate su base esistente e infrastrutture esterne (server, piattaforme, servizi cloud). A differenza del modello statale, la disponibilità di risorse e di integrazione inter-dominio è più limitata; tuttavia può comunque essere tecnicamente sofisticata.

L'elemento chiave è la logica di monitoraggio remoto. Ogni sistema professionale implica una catena composta da acquisizione del dato, trasmissione, archiviazione e accesso controllato. La vera differenza non è nel dispositivo terminale, ma nell'infrastruttura che consente la gestione continuativa delle informazioni. La persistenza è spesso il fattore critico: non tanto la capacità di attivare un vettore, quanto la capacità di mantenerlo nel tempo senza generare anomalie evidenti.

3.3 Scenari amatoriali (accenno)

Gli scenari amatoriali sono qualitativamente diversi. Non si basano su architetture strutturate, ma su accessi non autorizzati, utilizzo improprio di applicazioni di controllo, configurazioni di rete non sicure ed errori di gestione delle credenziali. In questi casi manca uno studio di fattibilità formale: l'azione è opportunistica, spesso relazionale o situazionale. La vulnerabilità sfruttata non è tecnologicamente avanzata, ma deriva da superficialità, scarsa consapevolezza e configurazioni improprie. Qui il rischio non nasce dalla sofisticazione tecnica, ma dall'asimmetria di competenze.

Tre architetture di sorveglianza a confronto

Statale

Integrazione multidominio, studio di fattibilità, ridondanza tra dominio radio, rete, fisico e umano. Catena informativa coordinata con infrastruttura dedicata.

Privata / professionale

Strumenti commerciali e infrastrutture esterne (server, cloud). Fattore critico: la persistenza del monitoraggio remoto nel tempo.

Amatoriale

Accessi non autorizzati, app di controllo improprie, errori di configurazione. Rischio derivato dall'asimmetria di competenze, non dalla sofisticazione.

La classificazione non riguarda il giudizio etico, ma la struttura tecnica e organizzativa.

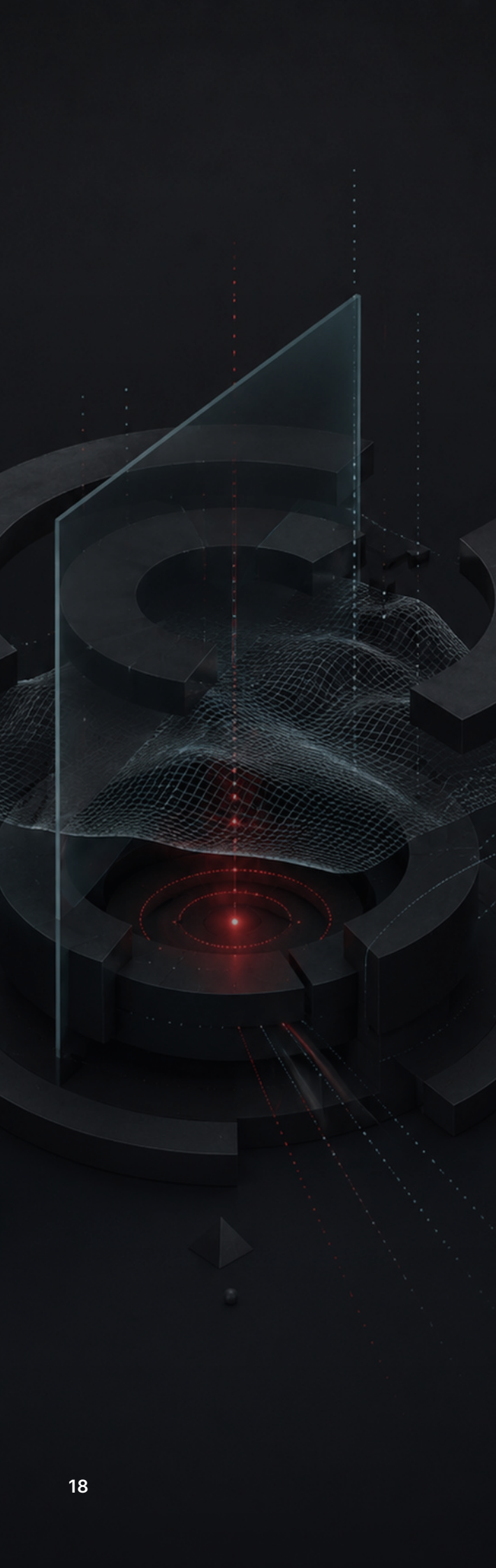
CONCLUSIONE

I tre modelli differiscono per livello di pianificazione, integrazione tra domini, infrastruttura di gestione, persistenza nel tempo e capacità di ridondanza. La classificazione non riguarda il tipo di dispositivo, ma la struttura operativa. Non esiste una sola microspia: esistono modelli operativi differenti, che possono includere dispositivi fisici, strumenti radio, software, infrastrutture di rete ed errori configurativi. Ridurre il fenomeno a un oggetto significa ignorare la dimensione sistemica della sorveglianza tecnica. Comprendere il modello operativo è il primo passo per impostare una corretta metodologia di rilevazione e analisi.



**Non si introduce più la microspia
nell'ambiente, si sfrutta il
dispositivo già ammesso
volontariamente.**

— IL METODO SPECTRA · CAPITOLO 04



04

CAPITOLO 04

Il dispositivo mobile come vettore di sorveglianza

Il dispositivo mobile moderno non è semplicemente uno strumento di comunicazione. È un nodo sensoriale permanente, costantemente connesso, dotato di capacità di acquisizione, elaborazione e trasmissione dati superiori a quelle di molti sistemi di sorveglianza dedicati di dieci anni fa. Nel contesto della sicurezza e delle attività di bonifica tecnica, lo smartphone rappresenta oggi uno dei principali vettori di sorveglianza potenziale.

4.1 Architettura sensoriale dello smartphone

Uno smartphone contemporaneo integra una molteplicità di sensori progettati per migliorare l'esperienza utente ma che, in presenza di compromissione logica, possono essere riconfigurati come strumenti di raccolta informativa.

Il microfono è un sensore MEMS (Micro-Electro-Mechanical System) ad alta sensibilità, progettato per comunicazioni vocali, comandi vocali, assistenti digitali e registrazioni ambientali. In caso di compromissione del sistema operativo o tramite malware con privilegi adeguati può attivarsi in background, registrare audio ambientale, trasmettere flussi audio in tempo reale o salvare registrazioni per esfiltrazione differita. Dal punto di vista TSCM, ciò implica che un dispositivo apparentemente inattivo possa funzionare come microspia ambientale software.

Le fotocamere (anteriore e posteriore) integrano sensori CMOS ad alta risoluzione e possono essere sfruttate per acquisizione immagini, cattura video ambientale, scansione documenti e rico-

noscimento facciale. In contesto di sorveglianza, un attore ostile può attivare la fotocamera in background, scattare immagini periodiche, registrare video o acquisire documentazione cartacea presente nell'ambiente. L'assenza di indicatori hardware dedicati (LED fisicamente collegati al sensore) rende la rilevazione non banale in caso di compromissione avanzata.

Il sistema GNSS (GPS, Galileo, GLONASS, Bei-Dou) consente geolocalizzazione precisa, tracciamento storico degli spostamenti e correlazione spazio-temporale degli eventi. In aggiunta al GPS, lo smartphone utilizza triangolazione celle LTE/5G, Wi-Fi positioning e Bluetooth beaconing, permettendo una profilazione estremamente accurata dei movimenti anche in ambienti indoor. Dal punto di vista investigativo, la cronologia posizione è uno dei dataset più sensibili in assoluto. Questa caratteristica apre anche alla possibilità di forme di osservazione opportunistica basate sull'analisi passiva dei segnali emessi dai dispositivi, che possono consentire la correlazione della presenza o degli spostamenti di determinati terminali anche senza una loro compromissione diretta.

Il dispositivo mobile è infine costantemente connesso tramite rete cellulare (2G-5G), Wi-Fi, Bluetooth e NFC. La presenza di una connessione dati attiva consente controllo remoto, aggiornamenti silenti, comando e controllo (C2) ed esfiltrazione immediata dei dati raccolti. A differenza di una microspia RF tradizionale, lo smartphone utilizza infrastrutture legittime di rete, rendendo la rilevazione radio molto più complessa.

Architettura sensoriale dello smartphone

	Funzione legittima	Impiego in sorveglianza
Microfono (MEMS)	Voce, comandi, assistenti	Registrazione audio ambientale in background
Fotocamere (CMOS)	Foto, video, scansione	Acquisizione immagini e video senza indicatori
GNSS / posizionamento	Navigazione, servizi di rete	Tracciamento storico e correlazione spazio-tempo
Connettività (2G-5G, Wi-Fi)	Dati, chiamate, sincronizzazione	Comando e controllo ed esfiltrazione immediata

Gli stessi sensori progettati per l'esperienza utente, in caso di compromissione, diventano strumenti di raccolta informativa.

4.2 Presenza costante del dispositivo

Lo smartphone è sempre acceso, sempre con l'utente, raramente spento e spesso presente in riunioni riservate. Questa caratteristica lo rende un vettore ideale di sorveglianza opportunistica: non è necessario installare un dispositivo esterno, perché il sensore è già nella stanza. Dal punto di vista della sicurezza fisica, il paradigma si è invertito: non si introduce più la microspia nell'ambiente, si sfrutta il dispositivo già ammesso volontariamente.

Non si introduce più la microspia nell'ambiente, si sfrutta il dispositivo già ammesso volontariamente.

4.3 Accesso remoto ai dati

Uno smartphone moderno contiene messaggi, email, documenti, fotografie, credenziali salvate, cronologia di navigazione, token di autenticazione e dati biometrici. In caso di compromissione logica (malware, exploit zero-click, trojan commerciali) è possibile accedere ai file system, intercettare comunicazioni cifrate prima della cifratura, estrarre database applicativi, acquisire backup locali e attivare sensori on-demand. L'accesso remoto può avvenire tramite server

C2 esterni, relay cloud o infrastrutture CDN legittime, rendendo la detection puramente basata su IOC spesso insufficiente.

4.4 Perché lo smartphone è oggi il vettore principale

Rispetto a una microspia RF tradizionale, uno smartphone compromesso presenta caratteristiche strutturalmente più favorevoli alla sorveglianza: non richiede installazione fisica, perché è già presente nell'ambiente; utilizza reti legittime invece di una banda dedicata facilmente identificabile; dispone di alimentazione e ricarica costante; integra in un solo dispositivo funzioni audio, video, localizzazione e accesso ai dati; richiede un'analisi logica e comportamentale, non soltanto radioelettrica.

4.5 Implicazioni per la metodologia TSCM moderna

L'analisi tecnica non può più limitarsi alla ricerca di trasmissioni RF anomale, dispositivi nascosti e segnali burst in banda non autorizzata. È necessario integrare analisi logica del dispositivo, analisi del traffico di rete, analisi dei pattern comportamentali, correlazione temporale tra uplink e dati, verifica della persistenza e individuazione

di consumi energetici anomali. Il paradigma di bonifica deve quindi diventare ibrido: RF, logico, comportamentale e infrastrutturale.

4.6 Gestione dei dispositivi non verificabili

In contesti operativi può verificarsi la presenza di dispositivi mobili introdotti da soggetti esterni all'organizzazione, come ospiti, consulenti o partner commerciali. Tali dispositivi non possono essere sottoposti a verifica tecnica preventiva e introducono quindi un potenziale vettore di captazione ambientale, dal momento che gli smartphone moderni dispongono di microfoni ad alta sensibilità, capacità di registrazione locale e connettività permanente.

In queste condizioni, la sicurezza dell'ambiente non può essere garantita esclusivamente tramite attività di bonifica tecnica, ma richiede anche misure di mitigazione del rischio associate alla presenza di dispositivi non verificabili. Tra le pratiche operative adottate in contesti sensibili rientrano tecniche di neutralizzazione acustica dei terminali mobili, basate sulla saturazione dei sensori audio mediante emissioni sonore controllate. Tali approcci non eliminano la presenza fisica del dispositivo, ma riducono la possibilità di acquisizione di audio utile durante attività sensibili.

CONCLUSIONE

Lo smartphone non è semplicemente un potenziale bersaglio. È un sistema sensoriale avanzato, costantemente connesso, già accettato all'interno degli ambienti sensibili. Per questo motivo rappresenta oggi uno dei principali vettori di sorveglianza nel panorama contemporaneo: non per natura intrinsecamente ostile, ma per concentrazione funzionale di sensori, connettività e dati.



05

CAPITOLO 05

Limiti della bonifica ambientale tradizionale

Nella pratica operativa delle bonifiche tecniche non è raro riscontrare ambienti radio privi di anomalie significative, nei quali successive verifiche sui dispositivi presenti evidenziano invece comportamenti di rete incompatibili con un uso fisiologico. La bonifica ambientale tradizionale rimane uno strumento fondamentale nel contrasto alle microspie e ai dispositivi di intercettazione ambientale, ma l'integrazione tra comunicazioni radio, reti IP e dispositivi mobili impone una revisione critica del suo perimetro operativo. Non si mette in discussione l'efficacia della bonifica classica: se ne analizzano i limiti strutturali in uno scenario tecnologico ibrido.

5.1 Componenti e capacità della bonifica tradizionale

Una bonifica TSCM tradizionale si articola in tre attività complementari. La prima è l'analisi radioelettrica, che comprende l'analisi dello spettro radio (tipicamente da 9 kHz a 6/8 GHz, estendibile oltre), la ricerca di trasmissioni attive (analogiche, digitali, burst, FHSS) e la verifica di segnali persistenti o anomali rispetto alla baseline ambientale, con strumentazione tipica come spectrum analyzer, antenne direzionali e omnidirezionali, near-field probe e tecniche di sweep dinamico. Il principio operativo è semplice: se un dispositivo trasmette in radiofrequenza, la sua emissione può essere rilevata e analizzata.

La seconda è l'ispezione fisica tecnica dell'ambiente: verifica di arredi, oggetti e infrastrutture, controllo di cablaggi e alimentazioni, identificazione di elementi non coerenti con l'ambiente, eventualmente supportata da endoscopi, telecamere termiche e altre tecnologie di imaging. Questa attività rimane uno dei pilastri della bonifica TSCM, poiché molti dispositivi di intercettazione sono progettati per mimetizzarsi in oggetti di uso comune. La terza è la rilevazione di elettronica nascosta tramite strumenti come il rilevatore di giunzioni non lineari (NLJD, Non Linear Junction Detector), che individua dispositivi elet-

tronici occultati grazie alle giunzioni semiconduttive tipiche dei circuiti integrati, anche in assenza di trasmissioni radio attive.

Se correttamente eseguite e integrate, queste tecniche possono individuare microspie RF analogiche, trasmettitori digitali UHF/VHF, dispositivi GSM/UMTS/LTE attivi, microspie Wi-Fi o Bluetooth in fase di trasmissione, beacon RF persistenti, dispositivi elettronici occultati e circuiti elettronici nascosti anche in assenza di emissioni RF. In sintesi, il modello TSCM tradizionale è progettato per individuare dispositivi hardware dedicati all'intercettazione, collocati fisicamente nell'ambiente.

5.2 Il limite strutturale del modello tradizionale

Il limite emerge quando la minaccia non consiste in un dispositivo esterno, ma in una compromissione dei dispositivi legittimi presenti nell'ambiente. In questi scenari le tecniche classiche possono risultare inefficaci, perché non esiste alcun nuovo hardware da individuare. In particolare, esse non possono individuare:

- software di intercettazione installato su dispositivi mobili, come spyware o captatori informatici presenti su smartphone o tablet;
- compromissioni di sistemi informatici, come PC, workstation o server aziendali accessibili da remoto;
- esfiltrazione di dati attraverso traffico di rete cifrato apparentemente legittimo (HTTPS, VPN o altri canali normalmente utilizzati dalle applicazioni);
- l'utilizzo dei microfoni o dei sensori già presenti nei dispositivi dell'ambiente (smartphone, smart TV, assistenti vocali o altri dispositivi con capacità di acquisizione audio);
- compromissioni software di dispositivi di rete, come router, access point o altri apparati

utilizzabili come punto di accesso o di raccolta dati.

La criticità non riguarda una singola tecnica di rilevazione, ma il paradigma stesso della bonifica tradizionale, concepito per individuare dispositivi hardware dedicati.

5.3 Il cambio di paradigma: la minaccia nel dispositivo

Nel contesto tecnologico attuale, la minaccia può non essere esterna all'ambiente, ma interna ai dispositivi legittimi: smartphone compromesso tramite spyware, PC con Remote Access Trojan, tablet con applicazioni di monitoraggio occulto, dispositivi IoT compromessi, smart TV con accesso remoto, router con firmware alterato. In questi scenari non esiste un nuovo dispositivo da cercare, l'hardware è legittimo, la trasmissione avviene su canali perfettamente normali (HTTPS, VPN, DNS, QUIC), il traffico è cifrato e l'emissione RF non è distinguibile da quella ordinaria. Dal punto di vista TSCM tradizionale, l'ambiente può risultare formalmente pulito; dal punto di vista della sicurezza reale, può essere completamente compromesso.

Lo scenario tipico è quello di un ufficio dirigenziale sottoposto a bonifica tecnica completa (RF, ispezione fisica, NLJD) senza alcuna anomalia rilevata, nel quale emerge successivamente uno smartphone con spyware commerciale che esfiltra dati tramite traffico HTTPS e attiva da remoto il microfono. Per la bonifica ambientale tradizionale non risultano né trasmettitori occulti né dispositivi elettronici nascosti; per la sicurezza reale, l'intercettazione è completa e realizzata tramite un dispositivo legittimo. Il punto è metodologico, non strumentale: la bonifica classica controlla lo spettro radio, verifica la presenza di elettronica nascosta e ispeziona fisicamente l'ambiente, ma non analizza il comportamento logico dei dispositivi digitali, e quindi non può eseguire analisi forense dei terminali, individuare malware o spyware, rilevare pattern di esfiltrazione né identificare compromissioni software.

Da qui un rischio operativo significativo: la certificazione di un ambiente pulito basata esclusivamente sull'assenza di dispositivi di intercettazione hardware.

CONCLUSIONE

La bonifica ambientale tradizionale resta necessaria, fondamentale e imprescindibile, ma non è più sufficiente da sola. L'evoluzione delle minacce ha spostato il baricentro dai trasmettitori hardware dedicati ai dispositivi legittimi compromessi, e dai segnali evidenti al traffico cifrato indistinguibile. Una bonifica tradizionale può dichiarare con elevata affidabilità l'assenza di dispositivi di intercettazione hardware attivi o occultati, ma non può escludere la presenza di intercettazioni realizzate tramite dispositivi legittimi compromessi. La differenza tra queste due affermazioni rappresenta il vero punto di rottura concettuale, e richiede un approccio integrato che affianchi alle tecniche TSCM tradizionali l'analisi dei dispositivi digitali, la verifica logica dei terminali e lo studio dei pattern di comunicazione, oggetto del capitolo seguente.



**La bonifica logica non cerca
necessariamente malware noto:
cerca incoerenze strutturali.**

— IL METODO SPECTRA · CAPITOLO 06

06

CAPITOLO 06

La bonifica logica dei dispositivi

La bonifica logica rappresenta l'estensione naturale della bonifica ambientale nel dominio digitale. Se la TSCM tradizionale si occupa di intercettazioni radio e microspie fisiche, la bonifica logica si concentra su dispositivi informatici e mobili che possono fungere da vettori di raccolta e trasmissione occulta di informazioni. Smartphone e computer non sono solo strumenti di comunicazione, ma veri e propri nodi sensoriali permanenti: microfono, fotocamera, GPS, accelerometri e connettività multi-radio (Wi-Fi, Bluetooth, LTE/5G) li rendono potenziali piattaforme di intercettazione sofisticata. Smartphone apparentemente inattivi possono mantenere comunicazioni periodiche verso endpoint remoti, difficilmente distinguibili dal traffico applicativo ordinario senza un'analisi strutturata dei pattern di rete.

La bonifica logica non coincide con la digital forensics né con il penetration testing offensivo. È un'attività difensiva, osservativa e metodologica, orientata alla rilevazione di anomalie compatibili con scenari di sorveglianza remota, e può essere interpretata come un processo strutturato che prevede acquisizione dei dati tecnici, analisi dei pattern di comunicazione e correlazione tra domini tecnologici diversi.

6.1 Analisi di smartphone e PC

L'analisi logica di un dispositivo si fonda su un principio essenziale: osservare senza alterare. L'obiettivo non è forzare il sistema o installare strumenti invasivi, ma analizzare configurazioni di sistema, profili di gestione, servizi attivi, processi in esecuzione, connessioni di rete e pattern temporali di attività. Nei dispositivi mobili (Android e iOS) si osservano in particolare configurazioni MDM o profili enterprise, permessi anomali concessi ad applicazioni, persistenza di servizi in background e attivazioni radio non coerenti con l'uso dichiarato. Nei sistemi desktop (Windows, macOS) si osservano servizi persistenti, attività pianificate, connessioni outbound ripetitive e nodi di comunicazione domi-

nanti. L'analisi è pattern-centrica: non si fonda esclusivamente su IOC (Indicator of Compromise), ma sulla ricerca di comportamenti ricorrenti, dominanti o incompatibili con l'uso fisiologico del dispositivo.

6.2 Acquisizione e osservazione del traffico

La bonifica logica si fonda su una verità tecnica: un dispositivo compromesso deve comunicare. L'acquisizione dei dati di rete, quando consentita dal contesto operativo, avviene in modalità passiva, privilegiando catture di traffico (PCAP/PCAPNG), log di sistema, log radio (Wi-Fi e cellulare) e metadati di connessione. L'attenzione non è rivolta al contenuto delle comunicazioni, ma alla struttura del traffico: frequenza delle connessioni, persistenza temporale, distribuzione IP sorgente/destinazione e concentrazione verso specifici nodi. L'analisi quantitativa (conteggi, flussi, ricorrenze) consente di individuare flussi dominanti, comunicazioni periodiche, nodi di aggregazione e pattern di beaconing. Senza effettuare ispezione profonda del payload è quindi possibile individuare anomalie statistiche compatibili con attività di esfiltrazione o controllo remoto.

L'osservazione del traffico non è un'attività di intercettazione, ma di analisi comportamentale. Si valutano variazioni improvvise del volume dati, attività in orari non coerenti con l'utilizzo, traffico in assenza di interazione utente e correlazioni tra eventi radio e attività di rete. Un principio chiave è la distinzione tra traffico infrastrutturale fisiologico, traffico applicativo legittimo e traffico anomalo per persistenza, frequenza o direzionalità. La bonifica logica non attribuisce automaticamente natura malevola a un flusso sconosciuto: produce invece una classificazione (compatibile con uso normale, da approfondire, incompatibile con scenario fisiologico).

6.3 Approccio non invasivo e differenza rispetto ad altre discipline

Elemento distintivo della bonifica logica è l'approccio passivo, non distruttivo e non alterante. Non si effettuano rooting o jailbreak, installazioni di agenti permanenti né modifiche strutturali al sistema. Questo garantisce l'integrità del dispositivo, la preservazione di eventuale valore probatorio e la neutralità metodologica. La disciplina si colloca così in una zona intermedia tra audit tecnico, analisi di sicurezza e osservazione comportamentale.

La bonifica logica non cerca necessariamente malware noto: cerca incoerenze strutturali.

CONCLUSIONE

In un contesto TSCM moderno la bonifica logica diventa imprescindibile, perché la microspia può essere software, l'esfiltrazione può avvenire su banda legittima e il vettore può essere il dispositivo stesso della vittima. La chiave non è lo strumento, ma la metodologia: separazione tra dato e interpretazione, analisi quantitativa prima di quella qualitativa, esclusione delle spiegazioni fisiologiche prima di formulare ipotesi. La bonifica tecnica moderna non consiste esclusivamente nella ricerca di dispositivi di intercettazione, ma nell'analisi strutturata dell'ecosistema tecnologico presente nell'ambiente osservato. In questo ecosistema, il dispositivo personale è il primo punto di osservazione e, potenzialmente, il primo punto di compromissione.



**Un sistema basato su firme
riconosce solo ciò che già
conosce.**

— IL METODO SPECTRA · CAPITOLO 07



07

CAPITOLO 07

Limiti degli approcci basati solo su IOC

Nella bonifica logica moderna, soprattutto in ambito smartphone e PC, uno degli errori metodologici più frequenti è affidarsi esclusivamente agli Indicatori di Compromissione (IOC). Gli IOC sono uno strumento fondamentale nell'analisi forense e nella risposta agli incidenti, ma diventano pericolosi quando utilizzati come unico criterio decisionale.

7.1 Cosa sono gli IOC e il limite delle signature

Gli IOC sono elementi osservabili che indicano una possibile compromissione: hash di file malevoli, domini o IP associati a infrastrutture C2, nomi di processi noti, certificati digitali specifici, stringhe di firma binaria, pattern di traffico già classificati. Sono, di fatto, tracce riconosciute di minacce già identificate, e il loro funzionamento si basa su una logica semplice: se compare qualcosa già noto come malevolo, si segnala la compromissione. È il paradigma alla base di anti-virus tradizionali, EDR basati su firme, database di spyware noti, blacklist DNS/IP e scanner mobile commerciali.

I sistemi basati su signature funzionano per confronto tra il campione osservato e un database di firme conosciute. Se il campione non è presente nel database, non viene rilevato e tende a essere classificato come pulito. Da qui un limite strutturale: un sistema basato su firme riconosce solo ciò che già conosce. In ambito TSCM logico questo è critico, perché uno spyware custom non sarà presente nei database pubblici, un'operazione mirata può usare infrastrutture dedicate e non tracciate, un captatore istituzionale non compare nelle blacklist commerciali e un malware evoluto può mutare hash a ogni build.

7.2 Database incompleti e minacce evolute

I database pubblici contengono indicatori relativi a spyware commerciali diffusi, trojan Android/iOS noti, famiglie malware catalogate e infra-

strutture già smantellate, ma presentano limiti evidenti: lag temporale (l'indicatore viene pubblicato solo dopo analisi e disclosure), visibilità parziale (non tutte le operazioni vengono rese pubbliche), bias commerciale (i tool mostrano ciò che possono rilevare, non ciò che esiste) e cecità verso le operazioni mirate (una campagna altamente selettiva può non lasciare tracce pubbliche).

Il problema diventa evidente con minacce zero-day, malware polimorfico, captatori custom, infrastrutture temporanee, C2 su CDN legittime e uso di servizi cloud comuni. In questi casi l'IP può sembrare legittimo, il dominio neutro, il traffico cifrato HTTPS e il processo dotato di un nome innocuo. Dal punto di vista IOC puro non esiste alcun indicatore classificato come malevolo; dal punto di vista comportamentale possono invece emergere persistenza anomala, flussi dati costanti in orari atipici, connessioni ripetitive verso ASN non coerenti con l'uso dell'utente e pattern di esfiltrazione compatibili con sorveglianza remota.

7.3 L'illusione del “nessun risultato”

Uno dei rischi operativi maggiori è l'inferenza “non abbiamo trovato IOC, quindi il dispositivo è pulito”. L'affermazione è metodologicamente scorretta: l'assenza di IOC equivale solo a “non sono stati trovati indicatori già noti”, non ad “assenza di compromissione”. In ambito TSCM logico questo errore può portare a falsi negativi critici. Un approccio esclusivamente IOC-based è infatti reattivo, dipendente da intelligence esterna, non autonomo e non investigativo: non analizza il comportamento, non studia i pattern, non costruisce una baseline e non misura le anomalie relative al contesto. Si limita a confrontare.

CONCLUSIONE

Nonostante i limiti, gli IOC restano preziosi: utili per identificare minacce note, fondamentali in ambito incident response, indispensabili per la correlazione OSINT e validi come primo filtro rapido. Il problema non è l'uso degli IOC, ma il loro uso esclusivo. In un contesto caratterizzato da spyware custom, captatori evoluti, infrastrutture dinamiche, cifratura end-to-end e servizi cloud legittimi, un'analisi basata solo su IOC è insufficiente. La vera differenza metodologica risiede nella capacità di analizzare ciò che non è ancora classificato, e richiede l'integrazione tra analisi degli indicatori noti e analisi dei pattern comportamentali, oggetto del capitolo seguente.



**Un modello solo IOC è
insufficiente; un modello solo
comportamentale rischia
un'eccessiva interpretazione.**

08

CAPITOLO 08

Approccio ibrido: IOC e analisi pattern- centrica

Nell'analisi del traffico acquisito durante attività di bonifica è frequente osservare dispositivi che mantengono connessioni periodiche verso un numero ristretto di endpoint dominanti. La distinzione tra servizi legittimi e possibili architetture di controllo remoto richiede quindi un'analisi quantitativa dei flussi nel tempo. Questo capitolo rappresenta il cuore metodologico della bonifica logica moderna.

In uno scenario caratterizzato da minacce evolute, infrastrutture distribuite e strumenti di sorveglianza sempre più modulari, nessun singolo approccio analitico è sufficiente. La metodologia efficace si fonda su un modello ibrido che integra analisi basata su IOC (Indicator of Compromise) e analisi pattern-centrica comportamentale. L'integrazione di queste due prospettive consente di ridurre i falsi negativi, aumentare la capacità di individuare minacce non catalogate e mantenere un impianto metodologico tecnicamente difendibile.

8.1 Analisi basata su IOC

L'analisi IOC individua indicatori noti, già associati a campagne di sorveglianza o malware documentati: indirizzi IP noti per attività C2, domini associati a infrastrutture di sorveglianza, hash di file malevoli, certificati digitali anomali, pattern di User-Agent riconducibili a tool specifici, processi o servizi riconosciuti come spyware commerciali. I vantaggi sono la rapidità di identificazione delle minacce già catalogate, l'alta affidabilità quando l'indicatore è verificato e la facilità di documentazione tecnica. I limiti strutturali sono altrettanto netti: funziona solo su minacce note, è inefficace contro infrastrutture custom o dedicate ed è eludibile tramite rotazione IP, domini dinamici, CDN e tunneling. Nel contesto della sorveglianza professionale o statale, l'infrastruttura può essere dedicata, temporanea, non riutilizza-

ta e priva di indicatori pubblici: in tali scenari l'analisi IOC può risultare formalmente corretta ma operativamente cieca.

8.2 Analisi basata su pattern

L'approccio pattern-centrico non cerca etichette, ma comportamenti. Non si domanda "questo IP è noto?", ma "questo comportamento è coerente con un uso legittimo del dispositivo?". L'osservazione comportamentale studia i flussi in termini di frequenza, durata, periodicità, volume e direzionalità, con l'obiettivo di individuare regolarità anomale: connessioni periodiche a intervalli costanti, trasmissioni notturne ripetitive, sincronizzazioni non giustificate dall'uso dell'utente.

In assenza di Deep Packet Inspection (DPI), l'analisi si basa su conteggi, distribuzioni e correlazioni temporali. Un flusso persistente è una comunicazione che si ripete nel tempo, mantiene endpoint stabili e mostra comportamento strutturato; la persistenza è un parametro chiave nella valutazione di compatibilità con scenari di monitoraggio remoto. Un nodo dominante è un endpoint che concentra una percentuale significativa dei flussi, mantiene relazioni multiple e mostra comportamento di aggregazione: in un contesto di sorveglianza può rappresentare un server di raccolta, un relay o un punto di orchestrazione, ma la sua identificazione resta strutturale, non attributiva. L'analisi temporale è spesso decisiva: attività in assenza di interazione utente, picchi in orari specifici, variazioni cicliche e incrementi improvvisi di uplink. Nel contesto TSCM logico, l'uplink anomalo persistente è uno degli elementi più significativi, in quanto compatibile con scenari di esfiltrazione.

Analisi IOC e analisi pattern-centrica

	Analisi IOC	Analisi pattern-centrica
Domanda guida	"Questo indicatore è già noto?"	"Questo comportamento è coerente con l'uso del dispositivo?"
Oggetto	Hash, IP/domini C2, signature, processi catalogati	Frequenza, persistenza, periodicità, nodi dominanti, direzionalità
Punto di forza	Rapidità e alta affidabilità su minacce note	Individua ciò che non è ancora classificato
Limite	Cieco su infrastrutture custom e zero-day	Rischio di sovra-interpretazione senza correlazione

La robustezza metodologica nasce dal confronto fra dato noto e comportamento osservato.

8.3 Integrazione operativa

L'approccio ibrido non è una semplice somma di tecniche, ma una sequenza logica: ricerca IOC per l'esclusione rapida di minacce note; analisi strutturale dei flussi; studio della persistenza; identificazione dei nodi dominanti; valutazione temporale; separazione tra traffico infrastrutturale normale e pattern compatibili con monitoraggio. L'analisi non produce certezze assolute, ma gradi di compatibilità, scenari probabilistici e valutazioni tecnicamente argomentabili.

8.3.1 Esempio illustrativo

Lo scenario seguente ha finalità esclusivamente didattiche. Non descrive un caso reale, ma serve a mostrare l'applicazione della separazione tra dato, analisi e ipotesi.

Si supponga di acquisire passivamente, per un periodo di osservazione di sette giorni, il traffico di rete di uno smartphone presente in un ambiente sensibile.

Il dato è l'insieme degli elementi osservabili e verificabili: lo smartphone stabilisce connessioni verso un medesimo endpoint a intervalli regolari di circa quindici minuti, anche nelle ore notturne

e in assenza di interazione utente; il volume in uplink verso tale endpoint è costante e superiore al downlink; il flusso si mantiene su HTTPS e l'endpoint non compare in alcuna blacklist pubblica.

L'analisi interpreta questi elementi in relazione tra loro: la regolarità dell'intervallo è compatibile con un meccanismo di beaconing; la prevalenza dell'uplink in assenza di attività dell'utente è coerente con un trasferimento di dati verso l'esterno; la persistenza notturna esclude una correlazione con l'uso applicativo dichiarato. Il confronto con la baseline degli altri dispositivi dell'ambiente mostra che nessuno presenta un profilo analogo. Allo stesso tempo, l'analisi registra le spiegazioni alternative legittime: notifiche push, sincronizzazione cloud, telemetria di sistema o keep-alive di un'applicazione di messaggistica possono produrre pattern simili.

L'ipotesi, esplicitamente condizionale, è che il comportamento osservato risulti tecnicamente compatibile con uno scenario di esfiltrazione remota persistente, qualora le spiegazioni alternative vengano escluse attraverso la correlazione con il dispositivo e la verifica delle applicazioni installate. L'output corretto non è quindi "il di-

spositivo è intercettato", ma una valutazione di compatibilità tecnica, argomentata e subordinata all'esclusione delle ipotesi fisiologiche.

DISCIPLINA METODOLOGICA

Dato, analisi, ipotesi: tre livelli separati

Dato 01	Analisi 02	Ipotesi 03
Elemento osservabile, numerico, verificabile e riproducibile. Connessioni a intervalli regolari, uplink costante superiore al downlink, flusso su HTTPS.	Interpretazione tecnica e correlazione fra elementi. Regolarità compatibile con beaconing; persistenza notturna che esclude l'uso applicativo.	Scenario possibile, sempre condizionale. Compatibilità tecnica con esfiltrazione remota persistente, subordinata all'esclusione delle spiegazioni fisiologiche.

La separazione evita che il sospetto diventi conclusione e che l'interpretazione si trasformi in narrativa.

8.4 Perché l'approccio combinato è necessario

Un modello solo IOC è insufficiente; un modello solo comportamentale rischia un'eccessiva interpretazione. La robustezza metodologica deriva dal confronto tra dato noto e comportamento osservato e dalla distinzione netta tra dato oggettivo, pattern e ipotesi. La bonifica logica moderna richiede analisi passiva, assenza di attribuzione prematura e separazione tra evidenza tecnica e narrativa.

8.5 L'intelligenza artificiale come supporto analitico

Nel contesto della bonifica logica moderna, l'analisi di traffico di rete, log di sistema, metadati di comunicazione e osservazioni provenienti da domini differenti può generare una quantità elevata di dati tecnici eterogenei. In tali scenari, strumenti basati su intelligenza artificiale possono rappresentare un supporto utile all'attività dell'analista, soprattutto nelle fasi di normalizzazione, correlazione e prioritizzazione delle anomalie.

L'intelligenza artificiale non deve tuttavia essere intesa come sostituzione dell'operatore, né come meccanismo decisionale autonomo. Nel metodo SPECTRA, il suo ruolo è quello di intelligenza aumentata: un sistema di supporto capace di assistere l'analista nell'individuazione di pattern ricorrenti, nella comparazione tra eventi tecnici e nell'evidenziazione di comportamenti che meritano approfondimento.

In ambito TSCM logico, l'intelligenza artificiale può essere utile in particolare per aggregare grandi volumi di dati provenienti da PCAP, log di sistema, eventi RF, traffico Wi-Fi, traffico cellulare e metadati di rete; per individuare ricorrenze temporali non immediatamente evidenti all'osservazione manuale; per evidenziare nodi dominanti, flussi persistenti e comunicazioni ripetitive; per correlare eventi appartenenti a domini diversi (ad esempio attività RF, uplink cellulare e traffico dati); per supportare la costruzione di baseline ambientali o dispositive; e per assegnare priorità agli elementi da verificare, riducendo il carico cognitivo dell'analista.

Sul piano delle tecniche, questo supporto si traduce in famiglie di metodi già consolidate nell'analisi del traffico e dei log. Algoritmi di

anomaly detection (per esempio Isolation Forest o autoencoder) possono segnalare flussi che si discostano da una baseline appresa, evidenziando uplink anomali o connessioni in fasce orarie atipiche. Tecniche di clustering non supervisionato (per esempio DBSCAN o k-means su feature di flusso quali frequenza, volume, durata e periodicità) consentono di raggruppare comunicazioni con comportamento simile e di isolare i flussi che non rientrano in alcun raggruppamento atteso. Modelli linguistici di grandi dimensioni (LLM) possono assistere nella normalizzazione e nella correlazione di log eterogenei, nella sintesi di sequenze di eventi e nella generazione di ipotesi da sottoporre a verifica. In tutti i casi si tratta di strumenti di supporto alla lettura del dato, non di moduli decisionali autonomi.

Il valore dell'intelligenza artificiale non risiede quindi nella capacità di decidere se un dispositivo sia compromesso, ma nella capacità di rendere più leggibili strutture complesse di dati. Un sistema di analisi può, ad esempio, segnalare che un determinato endpoint compare con frequenza anomala, che un flusso si ripete in assenza di interazione utente, oppure che un'attività di rete coincide temporalmente con eventi radio osservati nello stesso ambiente. Questi output non costituiscono prove autonome: rappresentano indicatori analitici che devono essere interpretati all'interno del contesto operativo.

Per essere realmente utile, l'intelligenza artificiale deve essere integrata in una metodologia strutturata. Un utilizzo generico, non contestualizzato o basato su prompt isolati rischia di produrre risultati apparentemente convincenti ma metodologicamente deboli. In particolare, nel dominio della bonifica tecnica, l'intelligenza artificiale deve operare su dati normalizzati, criteri espliciti e categorie analitiche coerenti con il modello di riferimento: dato, pattern, ipotesi e valutazione.

Il rischio principale è l'automazione dell'interpretazione. Un'anomalia statistica non equivale a una compromissione; un flusso persistente non

equivale automaticamente a un canale di esfiltrazione; un endpoint dominante non è necessariamente un server di comando e controllo. L'intelligenza artificiale può evidenziare correlazioni, ma non può sostituire la valutazione tecnica dell'analista, che deve distinguere tra comportamento fisiologico, anomalia contestuale e scenario compatibile con sorveglianza remota.

Nel metodo SPECTRA l'intelligenza artificiale assume quindi una funzione di supporto su tre livelli. Sul piano descrittivo, organizza i dati osservati, li sintetizza e li rende consultabili in modo più rapido. Sul piano correlativo, evidenzia relazioni temporali o strutturali tra eventi appartenenti a domini differenti. Sul piano prioritario, aiuta l'analista a individuare quali elementi meritano verifica ulteriore. Non assume invece funzione attributiva o conclusiva: non stabilisce l'autore di un'attività, non identifica con certezza una compromissione e non sostituisce la validazione umana.

In questa prospettiva, l'intelligenza artificiale può diventare uno strumento rilevante per la bonifica moderna, ma solo se subordinata a una metodologia rigorosa. Il suo impiego deve rafforzare la separazione tra dato, analisi e ipotesi, non indebolirla. Il processo decisionale resta responsabilità dell'analista umano, che deve valutare gli output alla luce del contesto, delle spiegazioni alternative e dei limiti tecnici dell'osservazione passiva. L'intelligenza artificiale non trasforma la bonifica tecnica in un processo automatico: la rende più scalabile, più ordinata e più efficiente, ma non elimina la necessità di competenza tecnica, interpretazione critica e validazione metodologica.

CONCLUSIONE

La bonifica logica non può basarsi esclusivamente su liste di indicatori, né su intuizioni comportamentali isolate. Richiede un approccio combinato, strutturato e tecnicamente difendibile. L'analisi IOC individua ciò che è già conosciuto; l'analisi pattern-centrica individua ciò che si comporta in modo anomalo. Solo l'integrazione delle due consente una valutazione coerente nel contesto della sorveglianza contemporanea.

09

CAPITOLO 09

Principi della metodologia di analisi passiva

Questo capitolo definisce l'impianto metodologico alla base dell'analisi tecnica applicata alla bonifica logica dei dispositivi e delle comunicazioni. Non si tratta di una procedura operativa, ma di un modello concettuale strutturato che consente di interpretare correttamente i fenomeni osservabili senza alterare il contesto tecnico analizzato. L'obiettivo non è trovare uno spyware, ma stabilire se il comportamento tecnico di un sistema sia compatibile o incompatibile con scenari di sorveglianza remota.

9.1 Analisi passiva del traffico

Il primo principio è la passività assoluta dell'osservazione. L'analisi si fonda sull'acquisizione e l'esame di traffico di rete già generato, metadati di comunicazione, distribuzione protocollare, persistenza dei flussi, frequenza e periodicità delle connessioni. Non viene generato traffico di test, non vengono effettuate interrogazioni forzate, non si inducono risposte dal dispositivo. Questo approccio garantisce integrità forense del contesto, assenza di alterazioni comportamentali e riduzione dei falsi positivi dovuti a stimolazione artificiale. In altre parole, si osserva il sistema mentre si comporta naturalmente.

9.2 Nessuna interazione attiva con il dispositivo

L'analisi non prevede installazione di software di scansione invasivi, esecuzione di exploit di verifica, test di penetrazione sul dispositivo oggetto di analisi né interrogazioni dirette verso endpoint sospetti. L'interazione attiva può modificare i log, attivare meccanismi di autodifesa, alterare i pattern di comunicazione e compromettere la validità dell'analisi. Il dispositivo viene trattato come una sorgente di dati, non come un bersaglio da stimolare.

9.3 Approccio non attributivo

Un principio fondamentale è la non attribuzione. L'analisi non identifica un autore, non attribuisce responsabilità, non formula accuse e non costruisce narrative investigative. Si limita a rispondere a una domanda tecnica: il comportamento osservato è compatibile con un'architettura di sorveglianza remota? Qualsiasi riferimento a soggetti, organizzazioni o presunti attori rimane fuori dall'ambito metodologico, riducendo bias interpretativi, derive speculative e sovrainterpretazioni.

9.4 Priorità ai pattern comportamentali

Il fulcro metodologico è l'analisi dei pattern. Non si parte da un indicatore di compromissione predefinito, ma dall'osservazione di nodi dominanti, flussi persistenti, distribuzione anomala dei protocolli, ricorrenza temporale e volumi incoerenti rispetto all'uso dichiarato. L'analisi è orientata a frequenza, durata, periodicità e topologia delle comunicazioni. Un singolo evento isolato non ha valore diagnostico; un comportamento ripetitivo, strutturato e coerente nel tempo può invece assumere significato tecnico. L'attenzione si concentra sulla coerenza del sistema, non sull'eccezione.

9.5 Separazione tra dato, analisi e ipotesi

Il metodo impone una distinzione netta tra tre livelli. Il dato è un elemento osservabile, numerico, verificabile e riproducibile. L'analisi è l'interpretazione tecnica del dato, la correlazione tra più elementi e l'identificazione di pattern. L'ipotesi è un possibile scenario compatibile, sempre condizionale e mai affermato come certezza. Questa separazione evita che l'ipotesi influenzi la lettura del dato, che il sospetto diventi conclu-

sione e che l'interpretazione si trasformi in narrativa. Il dato resta autonomo, l'analisi è dichiarata, l'ipotesi è esplicitamente condizionale.

9.6 Coerenza con il paradigma contemporaneo

La sorveglianza moderna non si manifesta necessariamente con segnali evidenti o comportamenti plateali. Può essere silente, intermittente, a basso volume e distribuita su più endpoint. Per questo motivo l'approccio metodologico non è orientato alla firma, ma alla struttura comportamentale del sistema. La domanda centrale non è "c'è uno spyware noto?", ma "il comportamento complessivo del dispositivo è compatibile con un modello di controllo remoto?".

CONCLUSIONE

La metodologia di analisi passiva si fonda su cinque principi cardine: osservazione non intrusiva, assenza di stimolazione attiva, neutralità attributiva, centralità dei pattern e separazione rigorosa tra dato e ipotesi. È un modello che privilegia la solidità tecnica rispetto alla spettacolarizzazione del risultato. In un contesto in cui la sorveglianza si è spostata dal perimetro fisico al dispositivo, la qualità dell'analisi dipende dalla disciplina metodologica: non dalla ricerca dell'effetto, ma dalla coerenza del metodo.



L'errore metodologico più grave è interpretare un'anomalia come prova.

— IL METODO SPECTRA · CAPITOLO 10

10

CAPITOLO 10

Limiti tecnici e ambiguità dell'analisi

Ogni analisi tecnica, sia essa RF, logica o di traffico di rete, opera entro limiti strutturali che devono essere esplicitati con chiarezza. L'obiettivo di una bonifica moderna non è produrre certezze assolute, ma valutare la compatibilità tecnica dei pattern osservati con scenari di sorveglianza.

10.1 Traffico cifrato

L'evoluzione delle comunicazioni digitali ha portato a un uso quasi totale della cifratura end-to-end: TLS 1.3, HTTPS obbligatorio, DNS over HTTPS e DNS over TLS, VPN commerciali, protocolli proprietari cifrati. Dal punto di vista forense passivo (PCAP, log di rete, metadata), il contenuto del traffico non è analizzabile, il payload non è interpretabile e l'ispezione profonda (DPI) è spesso inefficace o tecnicamente inappropriata. L'analisi si concentra quindi su pattern di persistenza, frequenza delle connessioni, distribuzione temporale, nodi dominanti e anomalie rispetto alla baseline. Un flusso cifrato verso un endpoint remoto non è di per sé indicativo di attività malevola: è un dato compatibile con molteplici scenari, inclusi quelli pienamente legittimi.

10.2 Servizi cloud legittimi

Le infrastrutture cloud moderne (CDN, storage distribuito, push notification, telemetria) rendono complessa l'attribuzione tecnica. Un dispositivo può comunicare costantemente con infrastrutture di aggiornamento sistema, servizi di sincronizzazione, backup automatici, piattaforme di messaggistica e servizi di analytics. Molti captatori informatici, commerciali o statali, utilizzano infrastrutture cloud per mascherare il traffico, ma lo stesso vale per applicazioni legittime. Ne consegue che la presenza di traffico verso IP di grandi provider non è di per sé indicativa, la reputazione dell'IP non è elemento decisivo e

l'assenza di blacklist non equivale a innocuità. L'analisi deve quindi basarsi sulla coerenza comportamentale, non sulla mera destinazione.

10.3 Falsi positivi

Ogni metodologia orientata ai pattern comporta il rischio di falsi positivi: applicazioni che mantengono socket persistenti per notifiche push, sistemi di backup che generano upload periodici, servizi VoIP con keep-alive frequenti, sincronizzazioni in background dopo inattività. Un pattern di traffico persistente, notturno o ricorrente può essere compatibile sia con un captatore sia con un servizio cloud legittimo. La distinzione richiede correlazione temporale, analisi del contesto operativo, confronto con baseline e validazione su più fonti di dato (rete, sistema, comportamento utente). L'errore metodologico più grave è interpretare un'anomalia come prova.

L'errore metodologico più grave è interpretare un'anomalia come prova.

10.4 Impossibilità di certezza assoluta

In ambito tecnico-forense passivo non si dispone sempre del controllo dell'infrastruttura, delle chiavi di cifratura, dell'accesso ai server remoti né dei log lato controparte. L'analisi può quindi stabilire la compatibilità tecnica con uno scenario di sorveglianza, l'incompatibilità tecnica con determinate ipotesi e la probabilità relativa di determinati comportamenti, ma non può, nella maggior parte dei casi, stabilire con certezza assoluta l'identità dell'operatore remoto, la finalità esatta della comunicazione o la presenza di un captatore specifico in assenza di artefatti diretti.

L'analisi tecnica moderna non produce verità assolute, ma valutazioni strutturate, classificazione dei pattern, analisi di coerenza e scenari compatibili. L'output corretto non è "il dispositivo è intercettato", ma "i pattern osservati risultano tecnicamente compatibili con uno scenario di esfil-

trazione remota persistente, in assenza di spiegazioni alternative coerenti". Questa distinzione non è debolezza metodologica: è rigore scientifico.

CONCLUSIONE

La bonifica logica e l'analisi di traffico devono essere presentate per ciò che sono: strumenti probabilistici ad alta competenza tecnica, non strumenti di certezza assoluta. La credibilità di un'analisi non deriva dall'enfasi conclusiva, ma dalla chiarezza con cui vengono dichiarati i suoi limiti. L'analisi individua compatibilità tecniche, non prove definitive.



Il pattern rappresenta l'unità minima di significato analitico nel metodo.

11

CAPITOLO 11

Implicazioni per la bonifica moderna

Il percorso tecnico sviluppato nei capitoli precedenti conduce a una conclusione chiara: la bonifica moderna non può più essere intesa come una semplice attività di scansione radio o ispezione manuale, ma come un processo analitico integrato, multidimensionale e continuativo. Le tecniche di rilevazione radio rimangono fondamentali, così come l'ispezione manuale dell'ambiente e la verifica fisica delle infrastrutture; tuttavia, l'evoluzione delle tecnologie di sorveglianza ha progressivamente ampliato il dominio della minaccia, che oggi può manifestarsi anche a livello software, di rete o di comportamento dei dispositivi. La bonifica tecnica moderna richiede quindi un approccio metodologico capace di integrare analisi provenienti da domini differenti: spettro radio, infrastrutture di rete e sistemi digitali.

11.1 Integrazione tra analisi RF e analisi logica

La bonifica RF tradizionale rimane uno strumento fondamentale. L'analisi dello spettro consente di individuare trasmettitori attivi in ambiente, rilevare segnali anomali per potenza, persistenza o modulazione, identificare uplink sospetti su bande note e analizzare comportamenti radio incompatibili con la semplice ricezione passiva. Accanto all'analisi RF deve essere sempre affiancata l'ispezione manuale dell'ambiente: la verifica fisica degli spazi, degli oggetti e delle infrastrutture rimane una componente essenziale delle attività TSCM, consentendo di individuare dispositivi elettronici occultati anche in assenza di emissioni radio attive.

L'evoluzione delle minacce ha però spostato una parte significativa del rischio dal dominio ambientale al dominio digitale. Oggi la sorveglianza può manifestarsi attraverso dispositivi mobili compromessi, software di controllo remoto, configurazioni improprie di rete, flussi dati anomali ma apparentemente legittimi e pattern di comunicazione compatibili con esfiltrazione silente. Di conseguenza, la bonifica moderna deve integra-

re analisi RF ambientale, analisi di rete locale, analisi logica dei dispositivi e correlazione tra livelli fisico e digitale. La separazione netta tra bonifica ambientale e bonifica informatica non è più coerente con lo scenario operativo attuale.

11.2 Evoluzione delle minacce: dall'emissione alla mimetizzazione

Le microspie analogiche classiche erano relativamente semplici da individuare: trasmissione continua, modulazione riconoscibile, comportamento stabile. Le minacce moderne si caratterizzano invece per trasmissioni intermittenti, uso di infrastrutture esistenti (rete cellulare, Wi-Fi), cifratura dei contenuti, attivazione condizionata (trigger remoto) e integrazione in dispositivi apparentemente legittimi. Il paradigma non è più semplicemente cercare una frequenza, ma interpretare un comportamento.

Un segnale su una banda nota non è automaticamente innocuo, così come un flusso dati cifrato non è automaticamente malevolo. La distinzione avviene attraverso l'analisi del contesto: potenza rispetto all'ambiente, persistenza nel tempo, coerenza con l'uso dichiarato dello spazio, correlazione con eventi o presenze, distribuzione temporale delle attività. La minaccia moderna tende alla mimetizzazione, e la bonifica deve quindi evolversi verso l'interpretazione dei comportamenti tecnici.

11.3 Il ruolo dell'analisi comportamentale

Il passaggio concettuale più rilevante riguarda l'introduzione dell'analisi comportamentale. Non si tratta di attribuire intenzioni, ma di osservare pattern oggettivi: flussi dati ricorrenti in determinate fasce orarie, attivazioni RF non coerenti con l'uso dell'ambiente, uplink persistenti senza traffico visibile, dispositivi che mantengono comunicazioni costanti anche in stato di apparente inattività. L'analisi comportamentale non sostituisce la tecnica, ma la completa, e richiede raccol-

ta strutturata dei dati, comparazione temporale, definizione di baseline ambientali e capacità di distinguere traffico infrastrutturale da trasmissione locale. In questo modello la bonifica diventa un processo ciclico: acquisizione, classificazione, correlazione, interpretazione, validazione. Il risultato non è un semplice "assenza di segnali", ma una valutazione tecnica argomentata del rischio.

11.4 Il metodo SPECTRA: formalizzazione della metodologia multidominio

Posizionamento rispetto allo stato dell'arte

Le attività di Technical Surveillance Countermeasures (TSCM) sono da tempo descritte in letteratura tecnica e in ambito istituzionale attraverso linee guida operative consolidate. Documenti riconducibili a contesti governativi, come quelli sviluppati in ambito National Security Agency e Dipartimento della Difesa statunitense, definiscono in modo strutturato le procedure di bonifica ambientale, con particolare enfasi sull'analisi radioelettrica, sull'ispezione fisica e sulla rilevazione di dispositivi elettronici. Parallelamente, negli ultimi anni si sono sviluppate metodologie tecniche avanzate orientate all'analisi dei dispositivi e dei captatori informatici: in questo ambito, i lavori di Amnesty International Security Lab e Citizen Lab hanno introdotto approcci forensi e di network analysis basati su indicatori tecnici, analisi dei log e correlazione delle infrastrutture di comunicazione, contribuendo in modo significativo alla comprensione delle moderne tecnologie di sorveglianza software.

Nonostante l'elevato livello tecnico, questi approcci risultano generalmente strutturati per dominio: le metodologie TSCM tradizionali operano prevalentemente sul piano fisico e radio, mentre le metodologie forensi moderne si concentrano sul dispositivo e sul traffico di rete. Il metodo SPECTRA si inserisce in questo contesto come formalizzazione di un approccio integrato. Non introduce nuove tecniche di rilevazione, ma organizza in modo esplicito un modello analitico multidominio in cui analisi ambientale e radioelettrica, ispezione fisica, analisi dei dispositivi e osservazione del traffico di rete vengono trattate come componenti interdipendenti di un unico processo. L'elemento distintivo del metodo non è quindi lo strumento utilizzato, ma la logica di integrazione: il valore analitico non è attribuito alla singola evidenza, ma alla correlazione tra evidenze eterogenee osservate nel tempo.

La differenza metodologica è netta. Nei framework tradizionali il dato viene analizzato principalmente all'interno del proprio dominio di origine; nel metodo SPECTRA il dato assume significato solo attraverso la relazione con altri domini e la sua evoluzione temporale. Questo comporta due elementi metodologici espliciti: il pattern multidominio come unità minima di analisi e la correlazione temporale come criterio interpretativo. In questo senso, SPECTRA non rappresenta un rebranding di pratiche esistenti, ma la formalizzazione di un modello analitico che integra in modo strutturato domini tecnici tradizionalmente trattati separatamente.

Il confronto sintetico con i principali riferimenti dello stato dell'arte chiarisce il contributo specifico del metodo.

STATO DELL'ARTE

Posizionamento del metodo SPECTRA

	TSCM tradizionale	Metodologie forensi	SPECTRA
Dominio principale	Fisico e radioelettrico	Dispositivo e traffico di rete	Integrazione multidominio
Unità di analisi	Emissione / dispositivo	Indicatore tecnico / artefatto	Pattern multidominio
Correlazione temporale	Limitata	Per caso analizzato	Criterio interpretativo centrale
Contributo	Bonifica ambientale	Analisi forense del captatore	Formalizzazione del processo

Riferimenti: linee guida TSCM istituzionali (NSA, DoD) e metodologie forensi (Amnesty International Security Lab, Citizen Lab).

Va inoltre osservato che la stessa metodologia forense di Amnesty riconosce esplicitamente un principio coerente con l'impianto di questo lavoro: la mancata corrispondenza con indicatori pubblici noti non conferma l'assenza di compromissione, ma indica soltanto che non sono stati trovati riscontri con indicatori già catalogati. È la stessa logica che, al capitolo 7, motiva il superamento di un approccio basato esclusivamente su IOC.

11.4.1 Definizione estesa

SPECTRA (Security Pattern Environment Correlation Technical Reconnaissance & Analysis) è una metodologia multidominio per attività di Technical Surveillance Countermeasures (TSCM) basata sull'integrazione coordinata di tecniche eterogenee e sulla correlazione di pattern tecnici nel tempo. Il metodo non introduce una singola tecnica, ma formalizza un sistema integrato di analisi in cui ogni componente contribuisce alla riduzione del rischio di sorveglianza tecnica.

Le sei componenti operative di SPECTRA



Figura 1. Schema concettuale del metodo SPECTRA: domini tecnici differenti integrati in un unico processo di correlazione finalizzato alla valutazione del rischio di sorveglianza.

11.4.2 Principio cardine

Nessuna tecnica, isolatamente, è sufficiente a garantire una bonifica efficace. La sicurezza deriva esclusivamente da integrazione, correlazione e continuità temporale. La mancanza di uno di questi elementi introduce inevitabilmente zone cieche analitiche.

11.4.3 Architettura del metodo

SPECTRA è composto da sei componenti operative, da applicare congiuntamente.

Analisi ambientale fisica: ispezione strutturale, verifica di accessi e punti sensibili, individuazione di modifiche o anomalie.

Analisi spettro RF: scansione wideband e mirata, identificazione di segnali persistenti e burst, valutazione della potenza rispetto al contesto.

Rilevazione elettronica (giunzioni non lineari): individuazione di circuiti attivi/passivi, rilevamento di dispositivi spenti o non trasmettenti, attività conforme alle tecniche TSCM tradizionali.

Analisi dispositivi autorizzati: smartphone, PC, IoT; verifica logica e comportamentale; analisi del traffico dati e delle attività anomale; individuazione di compatibilità con captatori informatici.

Gestione dispositivi non bonificabili: dispositivi esterni (ospiti, fornitori, terzi) per i quali è impossibile una verifica tecnica diretta; misure di isolamento controllato, esclusione dall'ambiente sensibile e messa in sicurezza attiva (per esempio saturazione acustica dei microfoni).

Monitoraggio temporale: osservazione a breve, medio e lungo termine; correlazione degli eventi nel tempo; identificazione di pattern ricorrenti.

Figura 1. Schema concettuale del metodo SPECTRA. Il metodo integra domini tecnici differenti (ambiente fisico, spettro RF, rilevazione elettronica, dispositivi, gestione del rischio residuo e osservazione temporale) all'interno di un processo di correlazione multidominio e analisi pattern-centrica finalizzato alla valutazione tecnica del rischio di sorveglianza.

11.4.4 Logica unificante

Il metodo si basa su un principio operativo preciso: il valore analitico non è nella singola rilevazione, ma nella correlazione tra domini e nel tempo. Per esempio: RF più traffico dati indica una possibile attività di esfiltrazione; dispositivo più comportamento anomalo indica una possibile compromissione; segnale più persistenza indica una possibile sorgente locale.

11.4.5 Approccio pattern-centrico

SPECTRA introduce un cambio di paradigma. Non si cerca il singolo dispositivo, la singola frequenza o l'indicatore statico, ma si analizzano pattern tecnici, coerenza con il contesto e anomalie multidominio. Il pattern rappresenta l'unità minima di significato analitico nel metodo.

11.4.6 Dimensione temporale

Il metodo opera su tre scale: breve termine (rilevazioni immediate), medio termine (comportamento nel tempo) e lungo termine (persistenza e ricorrenza).

11.4.7 Gestione del rischio residuo

Elemento fondamentale del metodo: ciò che non è verificabile deve essere controllato. Questo riguarda in particolare i dispositivi non autorizzati, i dispositivi non analizzabili e gli ambienti non completamente isolabili. La soluzione è il contenimento del rischio, la riduzione della capacità di acquisizione (audio/dati) e il controllo delle condizioni operative. L'assenza di rilevazioni non equivale all'assenza di capacità di acquisizione.

11.4.8 Distinzione metodologica rispetto alla TSCM tradizionale

SPECTRA non sostituisce la TSCM: la include, la estende e la integra. Supera il limite di una visione orientata solo all'RF, solo al piano fisico o

solo al dispositivo, introducendo correlazione strutturata, analisi comportamentale e integrazione multidominio.

11.4.9 Limite delle tecniche isolate

Il metodo formalizza un punto chiave: la bonifica RF da sola è insufficiente, così come lo sono l'analisi dei dispositivi da sola, l'isolamento dei dispositivi da solo e il monitoraggio RF continuativo da solo. La sicurezza emerge solo dalla combinazione delle tecniche. La sicurezza non è funzione della tecnica utilizzata, ma del grado di integrazione tra tecniche.

La sicurezza non è funzione della tecnica utilizzata, ma del grado di integrazione tra tecniche.

11.4.10 Output del metodo

SPECTRA non produce certezza assoluta, ma una valutazione tecnica strutturata basata su anomalie rilevate, pattern identificati e coerenza con il contesto. Il risultato è sempre espresso in termini probabilistici e contestuali, non deterministici.

11.4.11 Formalizzazione dell'acronimo

S, Security: finalità di protezione dalla sorveglianza tecnica.

P, Pattern: analisi basata su pattern tecnici, non su eventi isolati.

E, Environment: ambiente fisico come dominio operativo.

C, Correlation: correlazione multidominio e temporale.

T, Technical: approccio tecnico, non teorico.

R, Reconnaissance: ricognizione sistematica dell'ambiente.

A, Analysis: analisi strutturata dei dati raccolti.

11.4.12 Definizione conclusiva

SPECTRA è una metodologia multidominio che integra tecniche di analisi ambientale, RF, elettronica, dispositiva e comportamentale, basata sulla correlazione di pattern nel tempo, finalizzata all'identificazione di anomalie tecniche compatibili con attività di sorveglianza o acquisizione non autorizzata di informazioni.

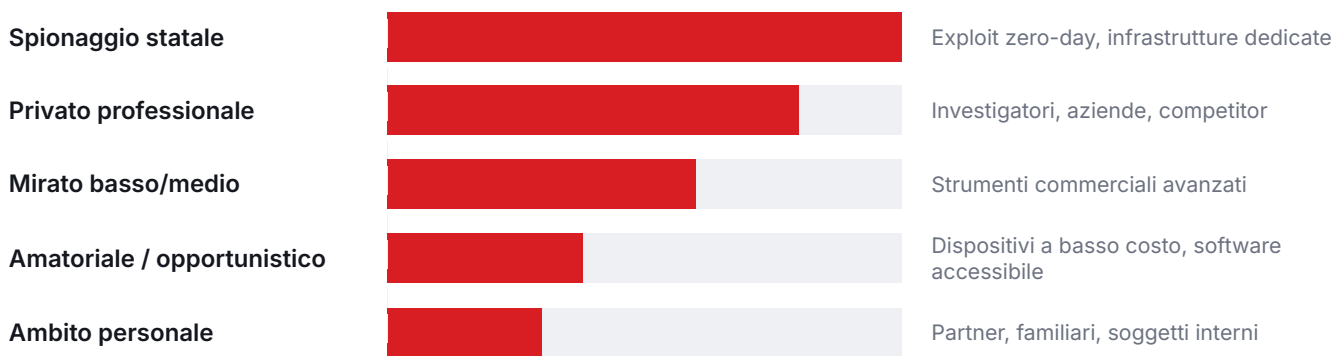
11.4.13 Contesto operativo e livelli di minaccia

Le attività di sorveglianza tecnica possono manifestarsi su livelli profondamente differenti in termini di capacità, risorse e obiettivi. In via gene-

rale è possibile distinguere lo spionaggio statale (elevata capacità tecnica, accesso a risorse avanzate come exploit zero-day e infrastrutture dedicate), lo spionaggio privato professionale (investigatori, aziende, competitor), lo spionaggio mirato a basso/medio livello (strumenti commerciali avanzati), lo spionaggio amatoriale/opportunistico (dispositivi a basso costo, software facilmente accessibile) e la sorveglianza in ambito personale (partner, familiari, soggetti interni). Il fattore discriminante tra questi scenari è rappresentato principalmente da budget operativo, livello tecnico dell'attore e obiettivi della sorveglianza.

CONTESTO OPERATIVO

Livelli di minaccia per capacità e risorse



Il contesto orienta la valutazione del rischio e l'interpretazione delle anomalie, ma non giustifica mai una riduzione del perimetro della bonifica.

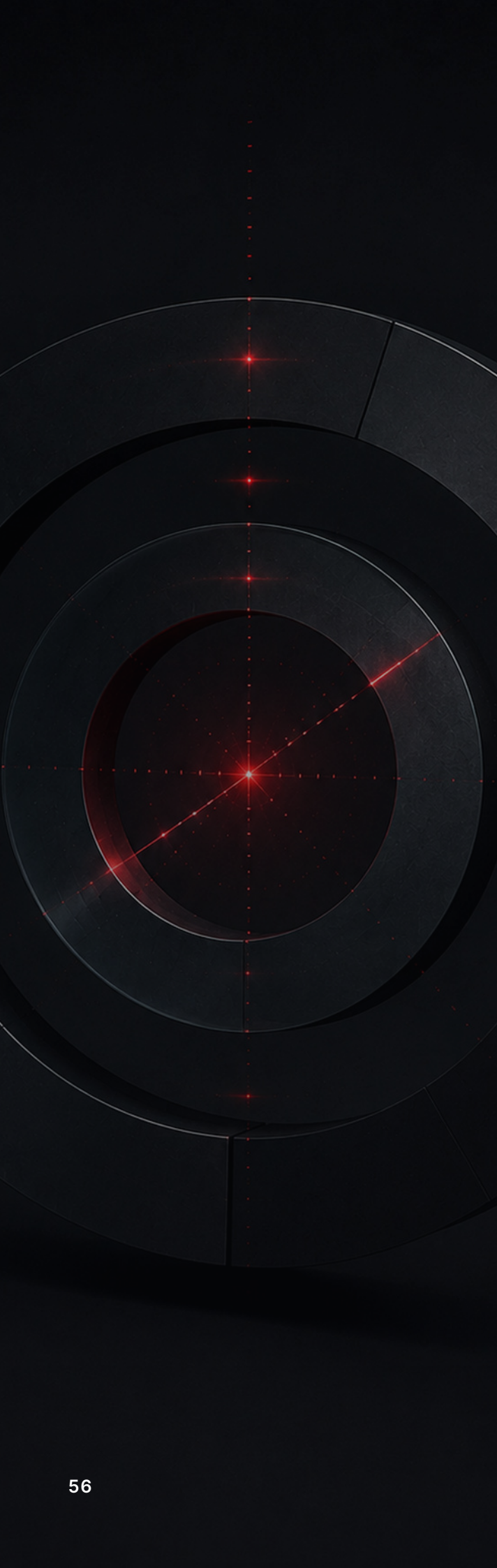
Nel contesto operativo TSCM/SPECTRA, tali differenze non modificano il principio metodologico fondamentale. L'analisi del contesto orienta la valutazione del rischio, ma non riduce il perimetro della bonifica. Durante la fase preliminare vengono raccolte informazioni sul contesto, stimato lo scenario di minaccia e definito il livello di rischio; in fase operativa, però, la bonifica deve comunque essere completa e multidominio. Una microspia da 50 euro e un sistema avanzato condividono lo stesso spazio operativo, un captatore software e un trasmettitore RF possono coesistere, e una minaccia apparentemente semplice può produrre effetti critici. Di conse-

guenza, il metodo SPECTRA prescinde dal livello dell'attaccante nella fase di verifica tecnica: il contesto serve a interpretare i risultati, a pesare le anomalie e a formulare ipotesi, ma non giustifica mai una riduzione dell'analisi.



La sicurezza non è il risultato di una tecnica, ma dell'integrazione strutturata di più domini analitici.

— IL METODO SPECTRA · CONCLUSIONI



CONCLUSIONI

Conclusioni



L'evoluzione della sorveglianza tecnica ha determinato uno spostamento strutturale del punto di acquisizione delle informazioni: dall'ambiente fisico al dispositivo personale, e dall'hardware dedicato al software residente. Questo cambiamento non è esclusivamente tecnologico, ma profondamente metodologico. Le tecniche di bonifica tradizionali, basate su analisi radioelettrica, ispezione fisica e rilevazione elettronica, rimangono strumenti fondamentali, ma non sono più sufficienti a descrivere l'intero dominio della minaccia.

Nel contesto contemporaneo la sorveglianza può manifestarsi attraverso dispositivi legittimi compromessi, traffico di rete cifrato, pattern comportamentali distribuiti nel tempo e infrastrutture apparentemente indistinguibili da quelle ordinarie. Di conseguenza, la bonifica tecnica non può più essere intesa come una singola attività, ma come un processo analitico multidominio. Il metodo SPECTRA si inserisce in questo contesto come formalizzazione di tale approccio, integrando analisi ambientale, analisi RF, rilevazione elettronica, analisi dei dispositivi, osservazione del traffico e correlazione comportamentale all'interno di un unico modello metodologico coerente.

Il contributo principale del metodo non consiste nell'introduzione di nuove tecnologie, ma nella definizione di un principio operativo chiaro: la sicurezza non è il risultato di una tecnica, ma dell'integrazione strutturata di più domini analitici. In questo paradigma il dato isolato perde significato, il pattern diventa unità analitica, il tempo diventa variabile critica e la certezza lascia spazio alla valutazione probabilistica. La bonifica tecnica moderna non consiste quindi nel trovare una microspia, ma nel determinare se un sistema tecnico, nel suo complesso, presenti comportamenti compatibili con scenari di sorveglianza. Questo passaggio rappresenta il vero

punto di discontinuità rispetto ai modelli tradizionali e definisce il perimetro operativo della contro-sorveglianza tecnica contemporanea.

Il dato isolato perde significato, il pattern diventa unità analitica, il tempo diventa variabile critica.

Il presente lavoro si basa principalmente su esperienza tecnica operativa e sull'analisi di casi documentati nella letteratura tecnica e giornalistica internazionale relativi all'utilizzo di captatori informatici e spyware commerciali.

Bibliografia

1. **Citizen Lab, University of Toronto.** Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries.
<https://citizenlab.ca/research/hide-and-peek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>
2. **Citizen Lab, University of Toronto.** Pegasus Spyware Research Reports and Investigations.
<https://citizenlab.ca/tag/pegasus/>
3. **Amnesty International Security Lab.** Forensic Methodology Report: How to Catch NSO Group's Pegasus.
<https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/>
4. **U.S. Department of Defense.** DoD Instruction 5240.05, Technical Surveillance Countermeasures (TSCM) Program.
<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/524005p.pdf>
5. **National Security Agency, Technical Surveillance Countermeasures (TSCM) Policy (documento ospitato dalla Federation of American Scientists, Government Secrecy Project).**
<https://sgp.fas.org/spb/tscmpol.html>
6. **SecurityWeek.** Exodus Android Spyware With Possible Links to Italian Government Analyzed.
<https://www.securityweek.com/exodus-android-spyware-possible-links-italian-government-analyzed/>
7. **European Parliament Research Service.** The Pegasus Spyware Scandal and Its Implications for Surveillance in Europe.
[https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU\(2022\)729397_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf)
8. **European Parliament, PEGA Committee.** Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware.
<https://www.europarl.europa.eu/committees/en/archives/9/pega>
9. **European Parliament.** Resolution of 15 June 2023 on the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware.
https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.pdf
10. **Access Now.** Spyware and Targeted Surveillance Resources.
<https://www.accessnow.org/tag/spyware/>
11. **Sistema Penale.** Cassazione n. 50972/2019, inutilizzabilità delle intercettazioni tramite trojan fuori dai luoghi consentiti.
<https://www.sistemapenale.it/it/sentenza/cassazione-50972-2019-inutilizzabilita-intercettazioni-trojan-fuori-luoghi-consentiti>
12. **Giurisprudenza Penale.** Il Tribunale di Perugia in tema di utilizzabilità delle intercettazioni nel c.d. caso Palamara.
<https://www.giurisprudenzapenale.com/2023/01/27/il-tribunale-di-perugia-in-tema-di-utilizzabilita-delle-intercettazioni-nel-c-d-caso-palamara/>
13. **Cammino Diritto.** Il captatore informatico (trojan horse) come strumento investigativo.
https://rivista.camminodiritto.it/public/pdfarticoli/9711_8-2023.pdf

Chi ha scritto questo paper



Stefano Cangiano

Specialista in Sicurezza Informatica & TSCM Analyst

Stefano Cangiano è un ricercatore indipendente e specialista in sicurezza informatica con esperienza nella controsorveglianza tecnica (TSCM) e nell'analisi dei segnali RF. Dal 2019 al 2025 è stato fondatore e CEO di ISK Security S.r.l., operando in contesti bancari, energetici, industriali e nelle telecomunicazioni, con attività di bonifica ambientale, analisi del traffico dati e valutazione delle vulnerabilità tecnologiche. Dal 2025 prosegue la propria attività come ricercatore indipendente, con focus su TSCM, analisi tecnica dei dispositivi e delle comunicazioni e valutazioni di sicurezza in ambienti sensibili.

È autore di pubblicazioni su ICT Security Magazine, tra cui lavori sulla sicurezza delle reti 5G e sull'impiego dei jammer in contesti critici. La sua attività di ricerca è oggi focalizzata sull'analisi multidominio della sorveglianza tecnica, con particolare attenzione all'integrazione tra spettro radio, infrastrutture di rete e dispositivi digitali.

Forum ICT Security

24^a Edizione

Auditorium della Tecnica, Roma

Novembre

18 e 19 NOVEMBRE 2026

**08 am -
04 pm**

Iscriviti sul sito web:

ictsecuritymagazine.com