# Capitolo 3 – Architetture di missione: i "codici"

Come avrete letto, tutte le missioni sono rapportate a specifici codici operativi che vengono inviati all'occorrenza sui dispositivi "beeper" tattici degli operatori: lettere e numeri utilizzati sono interpretabili grazie a uno specifico algoritmo di cifratura a 512 bit che convertono luoghi, obiettivi e priorità in otto caratteri alfanumerici, quattro lettere e quattro numeri. Ciò al fine di garantire la sicurezza delle comunicazioni qualora i codici fossero intercettati. Ricevuto il codice, gli operatori avrebbero dovuto applicare la chiave di decriptazione per ottenere le informazioni complete, ma già visualizzando la sequenza alfanumerica e conoscendo il sistema usato dall'algoritmo, le info di base sarebbero state già chiare. Questo perché il codice avrebbe potuto essere ricevuto in qualsiasi momento e non necessariamente mentre si era in base SOC o in licenza: magari si era già dislocati in teatro operativo e la ricezione del codice avrebbe significato ricevere ordini precisi di esecuzione. Il tutto avviene sfruttando una portante radio in modulazione di frequenza alla quale sono integrati pacchetti digitali compressi, al fine di garantirne la ricezione sostanzialmente ovunque nel globo, facendo rimbalzare il segnale dai satelliti, dagli AWACS[21] o dalle antenne radio base militari e di diffusione radio civili.

La ricezione del codice operativo dà inizio alla pianificazione della missione in ogni suo aspetto o all'esecuzione di quanto precedentemente pianificato: ogni team deve operare in autonomia per tutte le esigenze, iniziando dal reperire le ulteriori informazioni necessarie fino alla progettazione completa degli aspetti tattici e l'organizzazione degli assets di supporto. Una volta fuori dal SOC e dal paese, il team diviene a tutti gli effetti un "ghost", fino a scomparire completamente anche dai sistemi di comunicazione e rilevazione, arrivato nella zona obiettivo. Primario non lasciare tracce che possano ricondurre al blocco o alla nazione di provenienza, anche a costo di non essere evacuati con mezzi convenzionali se qualcosa dovesse andare storto: i governi negherebbero qualsiasi coinvolgimento e il team diverrebbe a tutti gli effetti una semplice cellula terroristica in paese ostile, con tutte le conseguenze del caso. È quindi sempre demandato ai componenti del CODE il compito di creare false identità ben documentate e

[21] AWACS: Airborne Early Warning Control System

tracciabili almeno fino alla maggiore età, perché i servizi segreti stranieri avrebbero sicuramente indagato e scandagliato a fondo chiunque fosse attenzionato, per qualsiasi motivo che fosse anche il solo entrare nel loro paese. Ora comprenderete l'importanza di Nerd all'interno del "J". L'architettura di missione potrebbe durare anche mesi, al variare dell'importanza del target e della pericolosità del territorio: i CODES hanno compiuto operazioni praticamente ovunque, tranne che in Corea del Nord, Iran e nel paese più pericoloso e organizzato in assoluto tra i blocchi rivali: la Cina. Non mi riferisco alle classiche incursioni hacker o con droni a pilotaggio remoto, ma al "boots on the ground", ossia infiltrare operatori sul territorio. Nessuno ha mai osato. Finora almeno. La costruzione delle missioni ha inizio con l'acquisizione delle informazioni di base, fornite usualmente dall'intelligence, dalle quali occorre generare tutte le opzioni possibili per acquisire il jackpot, l'obiettivo primario. Si potrebbe rendere necessario infiltrarsi nel paese, nelle organizzazioni, nelle industrie di riferimento o negli stabilimenti produttivi, nei palazzi amministrativi, al fine di stilare i piani operativi conseguenti. Poi viene la parte preparatoria atta a prevenire eventuali controlli di identità, creando appunto delle storie individuali credibili, documenti, passaporti, social networks e quanto riconducibile a una persona affidabile. Questo se la missione rende possibile l'infiltrazione preventiva pianificando anche la via di uscita sicura. Ma non sempre è possibile e allora il lavoro più difficile si rivela essere la sorveglianza elettronica: droni, satelliti, clonazione di celle telefoniche, videocamere… fino ad ottenere una proiezione tridimensionale del punto di attacco, spesso ricreandolo in scala reale nelle aree di addestramento predisposte nei SOC. Immensi spazi attrezzabili atti ad alloggiare le riproduzioni fedeli di ambienti, corridoi, strade e a consentire l'addestramento degli operatori che avrebbero poi applicato le tecniche e le modalità previste direttamente sull'area bersaglio, in modo da verificarne l'effettiva fattibilità. Si cerca, per quanto possibile, di prevedere tutte le incognite, ma non sempre la ciambella riesce col buco. Anzi, quasi mai. Viene messa in conto la possibile perdita del team impegnato e questo significherebbe un enorme buco nelle capacità operative dei centri segreti di comando, visto che addestrare e rendere operativo un CODE team richiede circa un anno e a volte anche di più. Per contro, ad ogni team viene data ampia scelta su tutto quanto fosse necessario all'architettura di missione, inclusa una disponibilità di fondi sostanzialmente illimitata. Siamo chiaramente pagati molto bene, certo, anche

se difficilmente si riesce a spendere quanto guadagnato rischiando la vita ad ogni codice ricevuto: chissà, forse una volta raggiunto il termine del periodo operativo, sempre che il mondo esista ancora per come lo conosciamo.

Ricevere un codice operativo potrebbe significare anche la necessità di intercettazione di operatori stranieri proprio sul nostro territorio, e questo accade non di rado. Oltre ad operare sul campo, che già risulta abbastanza complicato, occorre evitare contatti indesiderati con le forze dell'ordine perché una sovrapposizione sarebbe estremamente controproducente e potrebbe generare un risalto mediatico indesiderato: la popolazione non deve venire a conoscenza dei rischi che si corrono a livello mondiale o sarebbe una catastrofe. Al momento della nostra entrata in servizio come team CODE, ci era stata fornita una lista criptata dei codici di missione già prefissati come obiettivi del SOC, sulla cui pianificazione operativa si lavora sostanzialmente tutti i giorni, in attesa che fosse assegnato ad un team specifico o a gruppi di team, i quali avrebbero poi interagito ognuno con la sua linea di condotta tattica sul campo, anche separatamente e contemporaneamente. Il codice più temuto, quello con il più alto valore strategico ma anche con la più alta percentuale di rischio è considerato la "madre di tutte le missioni": XATS-7132. Ricevere questo codice avrebbe significato rendere operativa l'architettura di missione del team convocato e prepararsi ad operare in Cina sull'obiettivo prefissato. Gli analisti monitorano continuamente le varie pianificazioni sottoposte, creando algoritmi che hanno lo scopo di valutare le percentuali di riuscita, le quali finora non hanno mai superato il 20%. Sostanzialmente un suicidio. Tenete presente che queste pianificazioni non sono limitate al nostro ISOC e ai suoi CODES, ma sono eseguite dai SOC di tutto il blocco occidentale, quindi vi renderete conto di quanto la percentuale di riuscita ottenuta finora dalle simulazioni risulti estremamente esigua e totalmente insufficiente per pensare di operare un qualsiasi tentativo. Tutti noi teniamo nota delle nostre idee e proposte che registriamo sui dispositivi portatili in dotazione e che periodicamente sottoponiamo allo Stargate, il quale puntualmente ce le smonta pezzo per pezzo. Collaboriamo molto con i nostri omologhi del CODE K, tra i quali Moon è la più prolifera come idee e ipotesi, di cui solitamente discute con Nerd: il problema è che spesso anche Cicalone propone azioni impossibili, degne di un fumetto dei supereroi Marvel. Ma non è colpa sua, lo disegnano così, e lo apprezziamo tutti per il gran cuore che manifesta sempre, nei confronti di tutti.

Oltre ovviamente alle innegabili capacità tattiche, non fosse altro per la spiccata prerogativa di far bollire i timpani del nemico con il suo cicalare continuo: un'arma impropria! Non a caso ogni volta che capita di incontrarlo, anche solo per mangiare insieme a mensa, Bear porta sempre con sé le cuffie tattiche che puntualmente indossa dopo esserglisi seduto accanto. Al contrario di lui, il loro team leader, Starfive, parla pochissimo e tutti noi continuiamo a chiederci il perché del suo nickname: nessuno vuole spiegarcelo e quindi fioccano le ipotesi più fantasiose.

Al primo giorno di assegnazione ad ISOC i famigerati codici operativi ci vengono spiegati, e ci viene prospettato a grandi linee il parametro fondamentale dell'algoritmo di codifica. L'algoritmo si basa su otto alfabeti trasposti che utilizzano i 26 caratteri internazionali e i relativi numeri da zero a nove: il testo del codice operativo viene cifrato utilizzando in sequenza gli otto alfabeti, trasposti in modo diverso per ogni chiave di cifratura. In sostanza a ciascuna lettera o numero del testo in chiaro, corrisponde in sequenza una lettera o un numero degli alfabeti trasposti, generando del testo illeggibile se non si è in possesso della chiave crittografica specifica, e di quella generata in rolling-code e quindi volatile, tramite un dispositivo OTM in dotazione ai team, per poterla leggere. Non basterebbe entrare in possesso del dispositivo, perché sarebbe necessario anche conoscere la chiave crittografica di base per lo specifico codice ricevuto. Durante la spiegazione di questa metodologia, a parecchi è venuto il mal di testa, come ad esempio a Bear e a Weasel, ai quali Nerd ha dovuto dare ripetizioni e penare non poco per farlo entrare nella loro testa in maniera comprensibile. Resta poi la leggenda metropolitana su Cicalone, che avrebbe compreso talmente a fondo il sistema di decodifica, da aver fatto arrivare il team K dentro un centro commerciale della Papuasia… Ma vi garantisco che Cicalone sa il fatto suo in merito, qualsiasi sfottò venga messo in giro.

Quanto descritto nella metodologia è il motivo per il quale alcuni dei codici operativi più pericolosi siano già conosciuti ai CODES, ancor prima che vengano effettivamente inviati: ad ognuno è assegnata una operazione, pianificata o in pianificazione, che potrebbe essere inviato per renderla operativa e attuale in qualsiasi momento sia ritenuto necessario. Ma quali sono le percentuali accettabili da ottenere nelle simulazioni dello Stargate per questo tipo di operazioni? Chiaramente all'aumentare delle difficoltà e della

pericolosità o importanza dell'obiettivo, tali percentuali scendono, ma in media il valore richiesto per approvare un'architettura di missione non deve risultare inferiore al 75%. Si scende al massimo al 65% per le cosiddette missioni impossibili, come quella relativa al codice XATS-7132, percentuale comunque ancora ben lontana anche dall'essere intravista. Ma funzionano veramente le valutazioni ottenute su queste simulazioni? In linea di massima devo ammettere che funzionano, almeno due volte su tre i parametri immessi rispecchiano ciò che poi realmente si verifica, ma sarebbe un enorme errore affidarsi unicamente all'intelligenza artificiale per guidare la riuscita di una missione: il fattore umano deve essere sempre in primo piano, a prescindere dalle fredde valutazioni matematiche o statistiche, e tutti noi ne siamo consapevoli, il Generale prima di tutti. La nota positiva resta quella per cui, se la percentuale risulti troppo bassa, la missione non viene passata agli operativi, per salvaguardarne l'incolumità a svantaggio di possibili eclatanti successi costruiti sulla pelle di chi rischia la vita sul campo. Con qualche eccezione da parte di comandanti con meno scrupoli di Rimbaudo. Mi capita spesso di parlare con Martina, la mia compagna, di questa metodologia di valutazione, per tranquillizzarla in modo effimero sui rischi che corriamo, ma non sono mai riuscito a convincerla più di tanto… Pur utilizzando la tecnologia come tutti ormai, non ne è mai stata una sostenitrice, affermando che le uniche macchine perfette sono il cervello, l'istinto e il cuore di ogni essere umano. Come darle torto, in un mondo dove sembrano avere più importanza i followers su Instagram che le effettive capacità personali e di correlazione interpersonale con i simili? Mi sono sempre posto una domanda: cosa accadrebbe se lo Stargate ci sottoponesse una missione della quale non siamo convinti, a prescindere dalle percentuali di valutazione? Eseguiremmo gli ordini?