

## NOTIZIE

# Esclusivo: all'interno dell'esercito segreto sotto copertura dell'esercito

DI WILLIAM M. ARKIN IL 17/05/21 ALLE 5:30 EDT

Pdf by:  
<https://www.pro-memoria.info>



NOTIZIE

PENTAGONO

STATI UNITI MILITARE

SPIE



Listen to this article now

Powered by **Trinity Audio**

10 10 1.0x

00:00

26:27



All'interno della più grande forza sotto copertura che il mondo abbia

mai conosciuto: quella creata dal Pentagono, con decine di migliaia di soldati, civili e appaltatori che operano sotto nomi falsi, sul terreno e nel cyberspazio.

TIMOTHY A. CLARY, AFP VIA GETTY IMAGES

Pdf by:  
<https://www.pro-memoria.info>

**L**a più grande forza sotto copertura che il mondo abbia mai conosciuto è quella creata dal [Pentagono](#) nell'ultimo decennio. Circa 60.000 persone ora appartengono a questo esercito segreto, molte delle persone che lavorano sotto identità mascherate e di basso profilo, tutte fanno parte di un ampio programma chiamato "riduzione della firma". La forza, più di dieci volte più grande degli elementi clandestini della [CIA](#), svolge incarichi nazionali e stranieri, sia in uniformi militari che sotto copertura civile, nella vita reale e online, a volte nascondendosi in imprese private e società di consulenza, alcune delle quali società di nomi familiari.

Il cambiamento senza precedenti ha posto un numero sempre maggiore di soldati, civili e appaltatori che lavorano sotto false identità, in parte come risultato naturale della crescita delle forze speciali segrete, ma anche come risposta intenzionale alle sfide di viaggiare e operare in un mondo sempre più trasparente. L'esplosione della guerra cyberneare del Pentagono, inoltre, ha portato a migliaia di spie che svolgono il loro lavoro quotidiano in vari personaggi incaiti, lo stesso tipo di operazioni nefaste che gli Stati Uniti denunciano quando le spie russe e cinesi fanno lo stesso.

## **ISCRIZIONE ALLA NEWSLETTER DI NEWSWEEK >**

Il rapporto esclusivo *di Newsweek* su questo mondo segreto è il risultato di un'indagine di due anni che coinvolge l'esame di oltre 600 curriculum e 1.000 annunci di lavoro, dozzine di richieste del Freedom of Information Act e decine di interviste con partecipanti e decisori della difesa. Ciò che emerge è una finestra non solo in un settore poco conosciuto dell'esercito americano, ma anche in una pratica completamente non regolamentata. Nessuno conosce le dimensioni totali del programma e l'esplosione della riduzione della firma non è mai stata esaminata per

il suo impatto sulle politiche e sulla cultura militare. [Il Congresso](#) non ha mai tenuto un'audizione sull'argomento. Eppure i militari che sviluppano questa gigantesca forza clandestina sfidano le leggi statunitensi, le Convenzioni di Ginevra, il codice di condotta militare e la responsabilità di base.

Lo sforzo di riduzione della firma coinvolge circa 130 aziende private per amministrare il nuovo mondo clandestino. Decine di organizzazioni governative poco conosciute e segrete sostengono il programma, enunciando contratti classificati e supervisionando operazioni pubblicamente non riconosciute. Complessivamente le aziende attirano oltre 900 milioni di dollari all'anno per servire la forza clandestina, facendo di tutto, dalla creazione di una falsa documentazione e il pagamento delle bollette (e delle tasse) delle persone che operano con nomi presunti, alla produzione di travestimenti e altri dispositivi per contrastare il rilevamento e l'identificazione, alla costruzione di dispositivi invisibili per fotografare e ascoltare l'attività negli

Le forze operative speciali costituiscono oltre la metà dell'intera forza di riduzione della firma, i guerrieri ombra che inseguono i terroristi nelle zone di guerra dal Pakistan all'Africa occidentale, ma lavorano anche sempre più in punti caldi non riconosciuti, anche dietro le linee nemiche in luoghi come la Corea del Nord e l'Iran. Gli specialisti dell'intelligence militare - collezionisti, agenti di controspionaggio, persino linguisti - compongono il secondo elemento più grande: migliaia di persone schierate in qualsiasi momento con un certo grado di "copertura" per proteggere le loro vere identità.

Il gruppo più nuovo e in più rapida crescita è l'esercito clandestino che non lascia mai le tastiere. Questi sono i combattenti informatici all'avanguardia e i collezionisti di intelligence che assumono falsi personaggi online, impiegando tecniche di "non attribuzione" e "errata attribuzione" per nascondere chi e dove della loro presenza online mentre cercano obiettivi di alto valore e raccolgono quelle che vengono chiamate "informazioni accessibili al pubblico" o addirittura si impegnano in campagne per influenzare e manipolare i social media. Centinaia lavorano in e per la [NSA](#), ma negli ultimi cinque anni, ogni unità di intelligence militare e operazioni

speciali ha sviluppato una sorta di cellula operativa "web" che raccoglie informazioni e tende alla sicurezza operativa delle sue stesse attività.

## **OFFERTE DI ABBONAMENTO NEWSWEEK >**

Nell'era elettronica, un importante compito di riduzione della firma è mantenere tutte le organizzazioni e le persone, anche le automobili e gli aerei coinvolti nelle operazioni clandestine, mascherati. Questo sforzo protettivo comporta tutto, dalla pulizia di Internet da segni rivelatori di vere identità a piantare false informazioni per proteggere missioni e persone. Poiché l'identificazione e la biometria indimenticabili sono diventate norme mondiali, l'industria della riduzione delle firme lavora anche per trovare modi per falsificare e sconfiggere tutto, dalle impronte digitali e il riconoscimento facciale ai valichi di frontiera, per garantire che gli agenti sotto copertura possano entrare e operare negli Stati Uniti, manipolando i registri ufficiali per garantire che le false identità corrispondano.

Proprio come la biometria e il "Real ID" sono i nemici del lavoro clandestino, così è anche il "scarichi digitali" della vita online. Una delle principali preoccupazioni del lavoro antiterrorismo nell'era dell'ISIS è che anche le famiglie militari sono vulnerabili, un'altra ragione, dicono i partecipanti, per operare sotto false identità. L'abbondanza di informazioni online sugli individui (insieme ad alcuni spettacolari hack stranieri) ha permesso ai servizi di intelligence stranieri di smascherare meglio le false identità delle spie americane. La riduzione della firma è quindi al centro non solo dell'antiterrorismo, ma fa parte dello spostamento del Pentagono verso la grande concorrenza di potenza con Russia e Cina: concorrenza, influenza e interruzione "al di sotto del livello del conflitto armato" o di ciò che i militari chiamano guerra nella "zona grigia", uno spazio "nel continuum pace-conflitto".

Un alto ufficiale recentemente in pensione responsabile della supervisione della riduzione della firma e dei "programmi di accesso speciale" super-segreti che li proteggono dal controllo e dal compromesso afferma che nessuno è pienamente consapevole della portata del programma, né è stata data molta considerazione alle implicazioni per l'istituzione militare. "Tutto, dallo status delle Convenzioni di



Ginevra - se un soldato operava sotto falsa identità per essere catturato da un nemico - alla supervisione del Congresso è problematico", dice. Teme che il desiderio di diventare più invisibile per il nemico non solo oscura ciò che gli Stati Uniti stanno facendo in tutto il mondo, ma rende anche più difficile porre fine ai conflitti. "La maggior parte delle persone non ha nemmeno sentito parlare del termine riduzione della firma, figuriamoci di ciò che crea", dice. L'ufficiale ha parlato a condizione di anonimato perché sta discutendo di questioni altamente classificate.



Operatori militari che svuotano la parte posteriore di un SUV dalla Siria per installare l'alimentazione e il cablaggio per trasformare il veicolo apparentemente normale in una piattaforma di intercettazione ravvicinata, in grado di intercettare i segnali di telefoni cellulari e walkie-talkie. (Foto fornita a William M. Arkin)

## La vita segreta di Jonathan Darby

Ogni mattina alle 10:00, Jonathan Darby si imbarca nei suoi giri settimanali di chiamata di posta. Darby non è il suo vero nome, ma non è nemmeno il nome falso sulla sua patente di guida del Missouri che usa per condurre il suo lavoro. E l'auto governativa che guida, una di una flotta di oltre 200.000 veicoli federali di proprietà della General Services Administration, non è registrata con il suo vero o il suo nome falso, e né le sue targhe statali del Maryland attaccate magneticamente sono davvero per la sua auto, né sono riconducibili a lui o alla sua organizzazione. Anche dove lavora Darby e i luoghi che visita sono classificati.

Darby si è ritirato dall'esercito e chiede che non si usino né il suo vero nome né il suo nome di copertina. Ha prestato servizio per 20 anni nel controspionaggio, tra cui due incarichi africani in cui ha operato di basso profilo in Etiopia e Sudan, mascherandosi da uomo d'affari espatriato. Ora lavora per un appaltatore di riduzione delle firme con sede nel Maryland che ha chiesto a *Newsweek* di non identificare.

Mentre Darby fa il suo giro in circa 40 uffici postali e negozi di cassette postali nell'area metropolitana di DC, raccoglie un baule pieno di lettere e pacchi, inviando un numero simile dagli indirizzi rurali. Tornato in ufficio, ordina la presa, consegnando le bollette alle persone finanziarie ed elaborando dozzine di lettere personali e aziendali spedite da decine di località all'estero. Ma il suo compito principale è registrare e inoltrare i "meccanismi" di riduzione della firma come vengono chiamati, passaporti e patenti di guida statali per persone che non esistono e altri documenti - fatture, documenti fiscali, carte associative dell'organizzazione - che costituiscono la base di identità false.

Per registrare e ricontrollare l'autenticità della sua ripresa quotidiana, Darby accede a due database, uno il database dei documenti di viaggio e di identità, il repository

della comunità di intelligence di esempi di 300.000 passaporti e visti stranieri autentici, contraffatti e alterati; e l'altro il Cover Acquisition Management System, un registro super-segreto di false identità in cui Per le false identità che viaggiano all'estero, Darby e i suoi colleghi devono anche modificare i database dell'immigrazione e delle dogane statunitensi per garantire che coloro che svolgono attività illecite possano tornare negli Stati Uniti indisturbati.

Per la verifica dell'identità, l'unità di Darby lavora con gli uffici segreti della Homeland Security e del Dipartimento di Stato, nonché con quasi tutti i 50 stati nell'iscrivere autentici "meccanismi" sotto nomi falsi. Un'immagine rara in questo mondo è arrivata nell'aprile 2013 quando un giornalista intraprendente della Northwest Public Broadcasting ha fatto una storia che suggerisce la portata di questo programma segreto. Il suo rapporto ha rivelato che solo lo stato di Washington aveva fornito centinaia di patenti di guida statali valide con nomi fittizi al governo federale. L'esistenza del "programma di patente di guida riservata", come veniva chiamato, era sconosciuta anche al governatore.

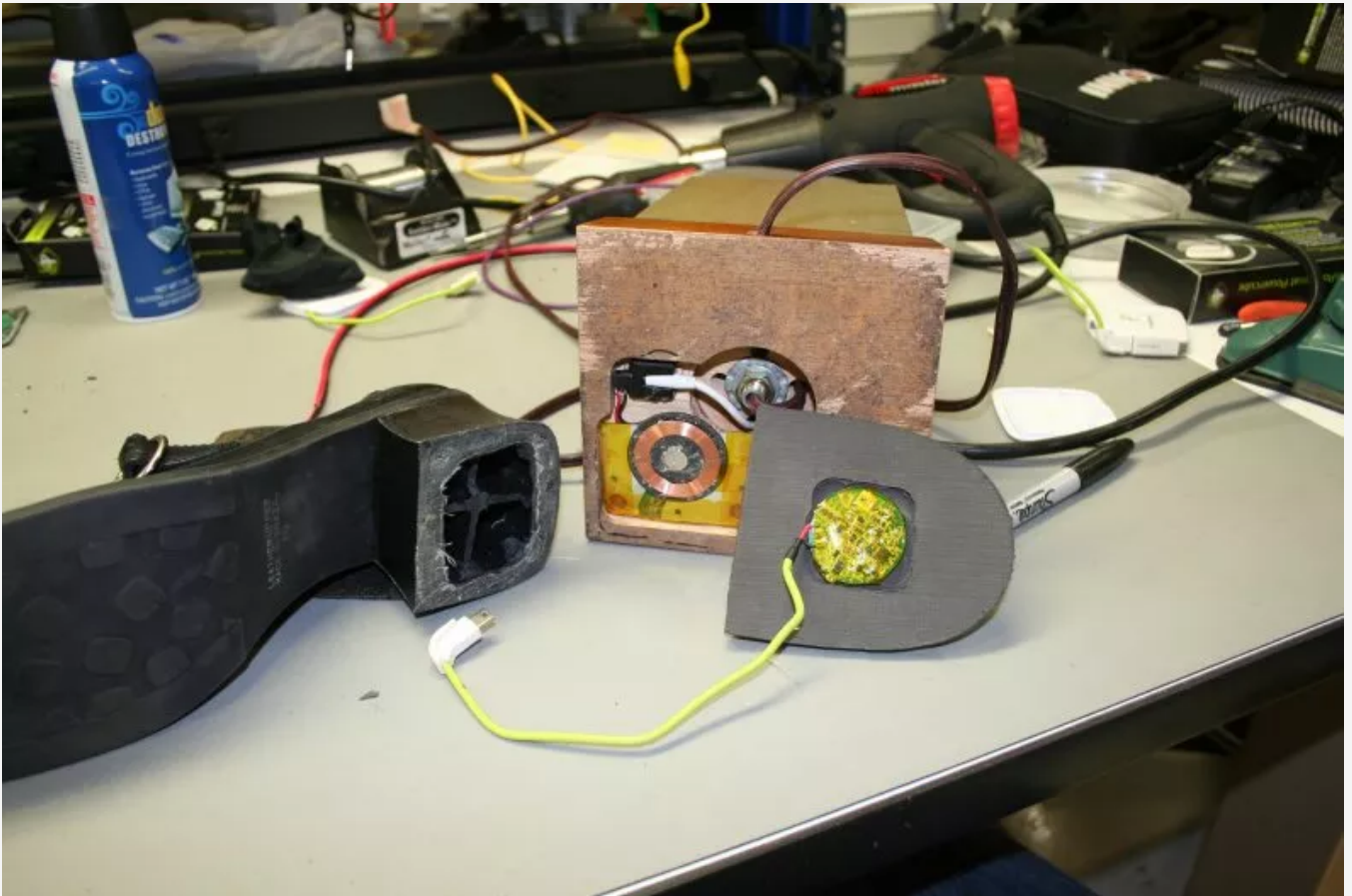
Prima di Internet, Darby dice - prima che un poliziotto locale o una guardia di frontiera fosse collegato ai database centrali in tempo reale - tutto ciò che un agente doveva essere "sotto copertura" era un documento d'identità con una foto autentica. In questi giorni, tuttavia, specialmente per coloro che operano sotto copertura profonda, la cosiddetta "leggenda" dietro un'identità deve corrispondere a qualcosa di più di un semplice nome inegno. Darby la chiama "due diligence": la creazione di questa scia di falsa esistenza. I luoghi di nascita e gli indirizzi di casa falsi devono essere attentamente studiati, devono essere create vite di e-mail false e account di social media. E quelle esistenze devono avere corrispondenti "amici". Quasi ogni singola unità che opera clandestinamente - operazioni speciali, raccolte di intelligence o cyber - ha una sezione di riduzione della firma, per lo più gestita da piccoli appaltatori, che conduce la due diligence. Lì aderiscono a quelli che Darby chiama i sei principi di riduzione della firma: credibilità, compatibilità, realismo, sostenibilità, verità e conformità.

La conformità è grande, dice Darby, soprattutto a causa del mondo creato dall'11

settembre, dove i punti di blocco sono comuni e l'attività nefasta è esaminata più da vicino. Mantenere qualcuno nascosto per davvero, e farlo per qualsiasi periodo di tempo, richiede una danza che richiede tempo che non solo deve prendersi cura dell'identità operativa di qualcuno, ma anche mantenere la sua vita reale a casa. Come spiega Darby, questo include il pagamento clandestino delle bollette, ma anche il lavoro con le banche e i dipartimenti di sicurezza delle carte di credito per guardare dall'altra parte mentre cercano frodi di identità o riciclaggio di denaro. E poi, i tecnici di riduzione della firma devono garantire che i punteggi di credito reali siano mantenuti - e che anche le tasse reali e i pagamenti di sicurezza sociale siano aggiornati - in modo che le persone possano tornare alla loro vita dormiente quando i loro incarichi di riduzione della firma cessano.

L'unità di Darby, originariamente chiamata Operational Planning and Travel Intelligence Center, è responsabile della supervisione di gran parte di questo (e per farlo gestisce il più grande ufficio finanziario militare del Pentagono), ma la documentazione, per quanto importante quanto importante, è solo un pezzo del puzzle. Altre organizzazioni sono responsabili della progettazione e della produzione dei travestimenti personalizzati e degli elementi di "sconfitte biometrica" per facilitare i viaggi. Darby dice che è qui che si trovano tutti i programmi di accesso speciale. Le SAP, la categoria più segreta di informazioni governative, proteggono i metodi utilizzati - e le capacità clandestine che esistono - per manipolare i sistemi stranieri per aggirare le salvaguardie apparentemente infallibili, tra cui il rilevamento delle impronte digitali e il riconoscimento facciale.





Dispositivo di tracciamento impiantato nel tallone di una scarpa. Sullo sfondo c'è la base di una lampada, anche con un dispositivo di ascolto impiantato. (Foto fornita a William M. Arkin)

W.M. ARKIN

## **"riduzione della firma" è un termine d'arte**

Numerosi SAP di riduzione delle firme, programmi con nomi come Hurricane Fan, Island Hopper e Peanut Chocolate, sono amministrati da un mondo oscuro di organizzazioni segrete che servono l'esercito clandestino: l'attività di supporto ai programmi di difesa, il Joint Field Support Center, il Field Support Center dell'esercito, l'Ufficio per lo sviluppo delle risorse del personale, l'Ufficio di supporto militare

A quanto sia segreto questo mondo, non esiste una definizione non classificata di riduzione della firma. La Defense Intelligence Agency, che gestisce il Defense

Clandestine Service e il Defense Cover Office, afferma che la riduzione della firma è un termine d'arte, che "gli individui potrebbero usare per ... descrivere misure di sicurezza operativa (OPSEC) per una varietà di attività e operazioni". In risposta alle domande di *Newsweek* che sottolineano che decine di persone hanno usato il termine per riferirsi a questo mondo, DIA suggerisce che forse il Pentagono può aiutare. Ma la persona responsabile lì, identificata come portavoce del Dipartimento della Dibattitura, dice solo che "per quanto riguarda le operazioni HUMINT", il che significa intelligenza umana, la riduzione della firma "non è un termine ufficiale" e che viene utilizzata per descrivere "misure adottate per proteggere le operazioni".

Un altro alto ex funzionario dell'intelligence, qualcuno che ha gestito un'intera agenzia e chiede di non essere nominato perché non è autorizzato a parlare di operazioni clandestine, afferma che la riduzione della firma esiste in un "twilight" tra segreto e sotto copertura. Il primo, definito dalla legge, è soggetto all'approvazione presidenziale e appartiene ufficialmente al National Clandestine Service della CIA. Quest'ultimo connota rigorosamente gli sforzi delle forze dell'ordine intrapresi da persone con un distintivo. E poi c'è il programma di protezione dei testimoni, amministrato dagli Stati Uniti. Marshals Service del Dipartimento di Giustizia, che si occupa delle false identità e vite delle persone che sono state reinsedate in cambio della loro cooperazione con i pubblici ministeri e le agenzie di intelligence.

L'esercito non conduce operazioni segrete, dice l'ex funzionario senior, e il personale militare non combatte sotto copertura. Cioè, tranne quando lo fanno, o perché gli individui sono assegnati - "pecore immerse" - alla CIA, o perché alcune organizzazioni militari, in particolare quelle del Joint Special Operations Command, operano come la CIA, spesso accanto a loro in status segreto, dove le persone che dipendono l'una dall'altra per la loro vita non conoscono i nomi reali dell'altro. Poi c'è un numero crescente di investigatori governativi - militari, **FBI**, sicurezza nazionale e persino funzionari statali - che non sono di per sé sotto copertura, ma che si avvalgono dello stato di riduzione della firma come documenti d'identità falsi e targhe false quando lavorano a livello nazionale, in particolare quando sono impegnati in un controllo estremo dei cittadini americani di origine araba, dell'Asia

meridionale

## "Diventa intelligente"?

Nel maggio 2013, in un incidente quasi comico che ricorda più "Get Smart" che abile spionaggio, Mosca ordinò a un "terzo segretario" dell'ambasciata degli Stati Uniti di nome Ryan Fogle di lasciare il paese, rilasciando foto di Fogle che indossava una parrucca bionda inaderente e portava una strana collezione di armamentario apparentemente dilettanti - quattro pai



THE  
**DEBATE**  
Newsweek

Il dibattito  
Israele contro i palestinesi

CONDIVIDI   ISCRIVITI   SCARICA   DESCRIZIONE

00:00 / 50:04

ART19

Informativa sulla privacy



Spionaggio sofisticato o "Get Smart"? Il 14 maggio 2013, uno schermo del computer a Mosca mostra una foto pubblicata dal sito web statale russo RT, che mostra alcuni degli effetti personali confiscati di Ryan C. Fogle, il terzo segretario della sezione politica dell'ambasciata di Washington a Mosca, è stato esistato al Federal Security Service dopo il suo arresto.

AFP/GETTY IMAGES

I media internazionali hanno avuto una giornata sul campo, molti pensionati della CIA che denunciavano il declino del commercio, la maggior parte dei commenti che opinavano su come eravamo passati dal vecchio mondo di parrucche e rocce finte, un riferimento alla Gran Bretagna che ammetteva solo un anno prima che in effetti era il proprietario di una roccia falsa e del suo dispositivo di comunicazione nascosto, un'altra scoperta dell

Sei anni dopo, un altro caso di spionaggio ha colpito la notizia, questa volta quando una giuria ha inviato l'ex ufficiale dell'intelligence militare americana Kevin Patrick Mallory a 20 anni di prigione per aver cospirato per vendere segreti alla Cina. Non c'era nulla di particolarmente unico nel caso Mallory, l'accusa ha fatto il suo spettacolo di presentare alla giuria una collezione di parrucche e baffi finti che assomigliano ai costumi di Halloween, il tutto sembra un altro episodio divertente di maldeto travestimento.

Eppure, dice Brenda Connolly (non il suo vero nome), si sarebbe ingenui a ridere troppo, perché entrambi i casi forniscono una sbirciatina nei nuovi trucchi del mestiere e nell'estrema segretezza che li nasconde. Connolly ha iniziato la sua carriera ingegneristica presso la Direzione della Scienza e della Tecnologia della CIA e ora lavora per un piccolo appaltatore della difesa che produce gli aggeggi - pensa a "Q" nei film di James Bond, dice - per le operazioni di riduzione della firma.

Quel "vecchio" telefono Nokia portato da Ryan Fogle, dice, non era niente del genere, gli esterni innocui che nascondevano quello che lei chiama un dispositivo di "comunicazioni occulte" all'interno. Allo stesso modo, inserito in evidenza nel caso

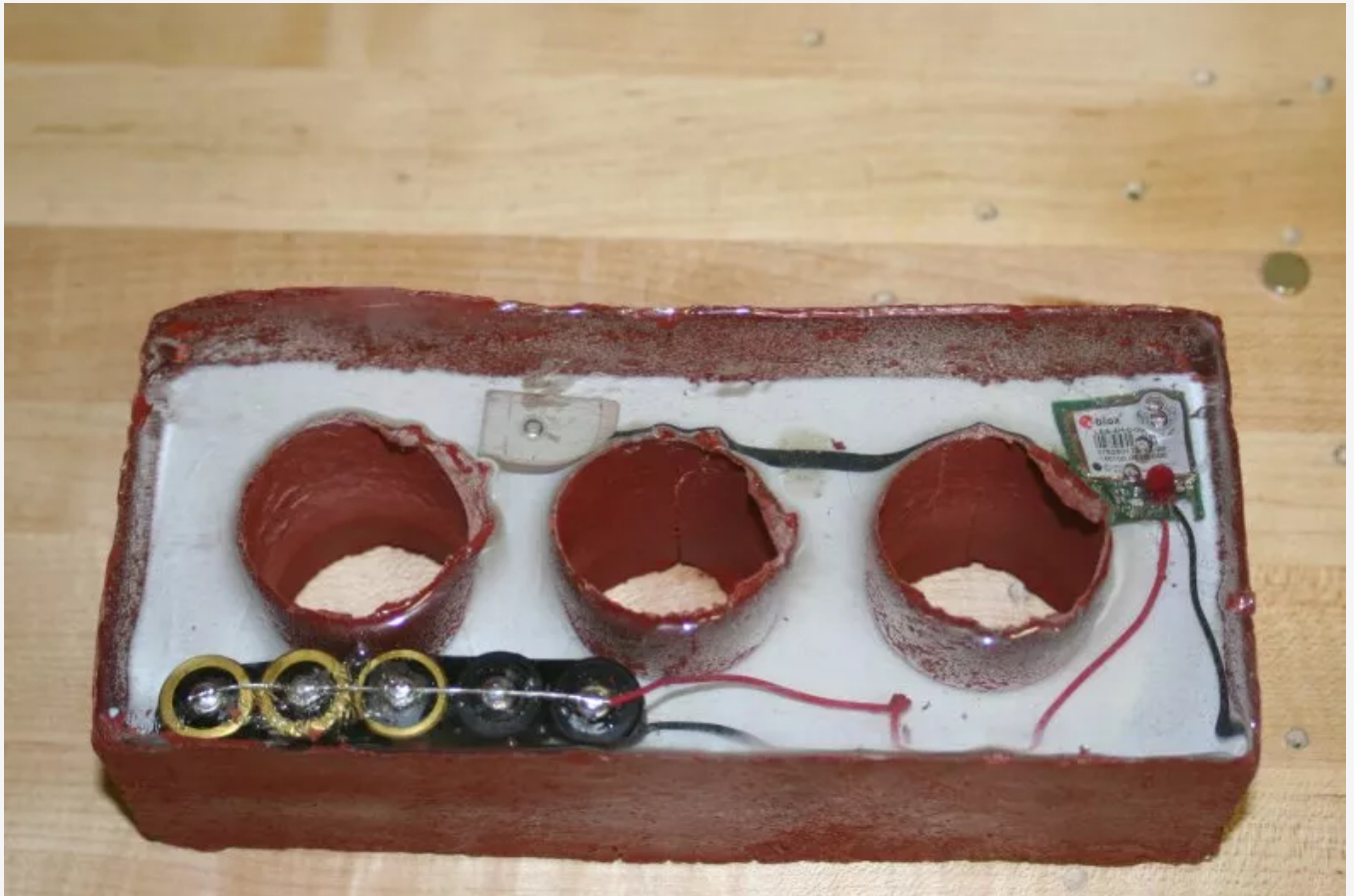
Mallory era un telefono Samsung datogli dall'intelligence cinese che era così sofisticato che anche quando l'FBI lo clonò elettronicamente, non riuscivano a trovare una partizione nascosta usata per conservare i segreti e una che Mallory alla fine ha dovuto rivelare loro.

Perso nel teatro spy-vs-spy di entrambi i casi c'erano altri indizi sulla moderna riduzione della firma, dice Connolly. Fogle portava anche uno scudo RFID, una custodia di blocco dell'identificazione a radiofrequenza destinata a impedire il tracciamento elettronico. E Mallory aveva fiale di sangue finto fornite dalla Cina; Connolly non avrebbe rivelato a cosa sarebbe stato usato.

Come molte persone in questo mondo, Connolly è un intenditore e curatore. Può parlare per ore delle trasmissioni che uscivano dall'Unione Sovietica, ma venivano anche trasmesse da Warrenton, Virginia, voci femminili che recitavano numeri casuali e passaggi da libri che gli agenti di tutto il mondo avrebbero raccolto sulle loro radio a onde corte e corrispondevano a codici prestabiliti.

Ma poi gli Internet caffè e le backdoor online sono diventati i canali clandestini di scelta per le comunicazioni segrete, sostituendo in gran parte le onde corte, fino a quando le tecnologie di sorveglianza (specialmente nei paesi autocratici) hanno raggiunto e le agenzie di intelligence hanno acquisito la capacità non solo di rilevare e intercettare l'attività di Internet, ma anche di intercettare ogni Questo ha inaugurato il mondo odierno delle comunicazioni segrete o COVCOMM, come lo chiamano gli addetti ai lavori. Questi sono dispositivi di crittografia molto speciali visti nei casi Fogle e Mallory, ma anche dozzine di diversi trasmettitori e ricevitori in "modalità scoppio" segreti in oggetti di uso quotidiano come rocce finte. Tutto ciò di cui un agente o operatore ha bisogno per attivare le comunicazioni con questi COVCOMM in alcuni casi è semplicemente passare da un ricevitore bersaglio (un edificio o una roccia falsa) e i messaggi clandestini vengono crittografati e trasmessi a centri di sorveglianza speciali.





Dispositivo di comunicazione segreta (COVCOMM). Mattone finto impiantato con dispositivo di ascolto alimentato a batteria, utilizzato nel lavoro di ricognizione "vicino" in Afghanistan. Foto fornita a William M. Arkin.

W.M. ARKIN

"E chi pensi che impianti quei dispositivi?" Connolly chiede retoricamente. " Ragazzi militari, ragazzi delle operazioni speciali che lavorano per sostenere operazioni ancora più segrete". Connolly parla di tessuti riscaldati che rendono i soldati invisibili al rilevamento termico, motociclette elettriche che possono operare silenziosamente nei terreni più accidentati, anche di come decine di piedi di fili vengono cuciti in abiti "nativi", lo shalwar kameez dell'Asia meridionale, i soldati stessi che diventano ricevitori ambulanti, in grado di intercettare le radio a bassa

### **Mani finte, facce finte**



Parrucche. Dispositivi di comunicazione coperti. Rocce finte. Nel nostro mondo di tutto elettronico, dove tutto diventa una questione di record, dove non puoi entrare in un parcheggio senza che la targa sia registrata, dove non puoi fare il check-in per un volo o un hotel senza un documento d'identità rilasciato dal governo, dove non puoi usare una carta di credito senza che la posizione venga catturata, come si può sconfiggere la biometria? Come può qualcuno superare i lettori di impronte digitali?

In 99 casi su 100, la risposta è: non c'è bisogno di. La maggior parte dei soldati di riduzione della firma viaggia con nomi reali, scambiandosi identità operative solo una volta sul terreno in cui operano. Oppure si infiltrano oltre i confini in luoghi come il Pakistan e lo Yemen, conducendo le missioni più pericolose. Queste missioni di riduzione della firma sono le più altamente sensibili e comportano la raccolta di informazioni "vicino" o l'uso di dispositivi di tracciamento nemico miniaturizzati, ognuno esistente nei propri programmi di accesso speciale, missioni che sono così sensibili che devono essere approvate personalmente dal Segretario della Difesa.

Per l'uno per cento, però, per coloro che devono superare il controllo dei passaporti sotto false identità, ci sono vari sistemi di sconfitta biometrici, alcuni fisici e altri elettronici. Uno di questi programmi è stato accennato in un dump di documenti un po' notato pubblicato da [Wikileaks](#) all'inizio del 2017 e chiamato "Vault 7": oltre 8.000 strumenti CIA classificati utilizzati nel mondo segreto dello spionaggio elettronico e dell'hacking. Si chiama ExpressLane, dove l'intelligence statunitense ha incorporato malware in sistemi biometrici e watchlist stranieri, consentendo alle spie informatiche americane di rubare dati stranieri.

Un mago IT che lavora per Wikileaks a Berlino dice che il codice con ExpressLane suggerisce che gli Stati Uniti possono manipolare questi database. "Immagina per un momento che qualcuno stia attraversando il controllo dei passaporti", dice, esitante a usare il suo vero nome a causa della paura dell'accusa negli Stati Uniti. "NSA o la CIA hanno il compito di corrompere - cambiare - i dati il giorno in cui passa la risorsa segreta. E poi riportalo indietro. Non è impossibile."



Una custodia in silicone fabbricata, usata per eludere le impronte digitali e creare identità false per i viaggiatori clandestini. (Foto fornita a William M. Arkin)

W. M. ARKIN

Un'altra fonte ha indicato una piccola azienda rurale della Carolina del Nord nel settore della riduzione delle firme, per lo più nel campo della raccolta clandestina e delle comunicazioni. Nella struttura di laboratorio e formazione dove insegnano agli operatori come fabbricare dispositivi di ascolto segreti in oggetti di uso quotidiano, sono all'avanguardia, o così dicono i loro materiali promozionali, un deposito per lo stampaggio e la fusione, la pittura speciale e sofisticate tecniche di invecchiamento.



Dietro la maschera: lo stampo di riduzione della firma per una maschera che invecchia, usato per alterare completamente l'aspetto di un operatore. (Foto fornita a William M. Arkin)

W. M. ARKIN

Questa compagnia tranquilla può trasformare qualsiasi oggetto, inclusa una persona, come fanno a Hollywood, un "apparecchio per il viso in silicone" scolpito per alterare perfettamente l'aspetto di qualcuno. Possono invecchiare, cambiare sesso e "aumentare la massa corporea", come dice un contratto classificato. E

possono cambiare le impronte digitali usando una custodia di silicio che si adatta così comodamente a una mano reale che non può essere rilevata, incorporando impronte digitali alterate e persino impregnata con gli oli che si trovano nella pelle reale. Alla domanda se l'apparecchio è efficace, una fonte, che ha attraversato la formazione, ride. "Se te lo dico, dovrò ucciderti".



**Newsweek** \*\*\*  
**90**

Non il suo viso: operazioni speciali sotto copertura operativo che indossa una maschera di invecchiamento di riduzione della firma per abbinare una falsa identificazione. (Foto fornita a William M. Arkin)

W.M. ARKIN

Nella vita reale, il furto di identità (per lo più a causa dell'intento di profitto dei criminali) rimane un'epidemia che colpisce tutti, ma per quelli nel mondo dell'intelligence e dell'antiterrorismo, il nemico è anche attivamente impegnato negli sforzi per compromettere le informazioni personali. Nel 2015, lo Stato islamico ha pubblicato i nomi, le foto e gli indirizzi di oltre 1.300 militari statunitensi, istruendo i sostenitori a

**ISCRIVITI PER 1 DOLLARA**

identificati. L'FBI ha affermato che il rilascio è stato seguito da sospetti hacker russi che si sono mascherati da membri dell'ISIS e hanno minacciato le famiglie militari attraverso Facebook. "Sappiamo tutto di te, di tuo marito e dei tuoi figli", ha detto un messaggio minaccioso.

I funzionari del controspionaggio e dell'OPSEC hanno iniziato uno sforzo su larga scala per informare le persone

colpite, ma anche per avvertire il personale militare e le loro famiglie di proteggere

meglio le loro informazioni personali sui social media. L'anno successivo, l'ISIS ha rilasciato 8.318 nomi target: la più grande versione di sempre fino a quando non è stata sormontata da 8.785 nomi nel 2017.

È stato rivelato che i militari che condividevano informazioni sulla posizione nei loro dispositivi di fitness stavano apparentemente rivelando le posizioni delle operazioni sensibili semplicemente facendo jogging e condividendo i loro dati. "Il rapido sviluppo di tecnologie dell'informazione nuove e innovative migliora la qualità della nostra vita, ma pone anche potenziali sfide alla sicurezza operativa e alla protezione delle forze", Stati Uniti Il Comando Centrale ha detto in una dichiarazione all'epoca al *Washington Post*.

Poi è arrivata la paura del DNA, quando l'Adm. John Richardson, allora capo delle operazioni navali, ha avvertito il personale militare e le loro famiglie di smettere di usare i kit di test del DNA di ascendenza a casa. "Fai attenzione a chi invii il tuo DNA", ha detto Richardson, avvertendo che i progressi scientifici sarebbero in grado di sfruttare le informazioni, creando sempre più armi biologiche mirate in futuro. E in effetti nel 2019, il Pentagono ha ufficialmente consigliato al personale militare di evitare i popolari servizi di DNA. "Esporre informazioni genetiche sensibili a parti esterne pone rischi personali e operativi per i membri del Servizio", ha detto la nota, riportata per la prima volta da Yahoo news.

"Siamo ancora agli inizi del nostro mondo trasparente", dice l'ufficiale di alto livello in pensione, mettendo in guardia dall'immaginare che ci sia un "divario di identità" simile al "divario dei bombardieri" della Guerra Fredda. "Stiamo vincendo questa guerra, anche sul lato informatico, anche se la segretezza su ciò che stiamo facendo fa sembrare di nuovo il ritratto mediatico dei russi come se fossero alti dieci piedi".

Ammette che l'elaborazione dei big data in futuro probabilmente avrà un ulteriore inganno sulle operazioni clandestine di tutti, ma dice che i benefici per la società, anche solo rendendo l'attività terroristica e i viaggi molto più difficili, superano le difficoltà create per la sicurezza operativa militare. L'ufficiale definisce la segretezza



legittima, ma dice che la leadership del Dipartimento della Difesa ha lasciato cadere la palla nel riconoscere il quadro generale. I servizi militari dovrebbero porre più domande sull'etica, la correttezza e persino la legalità dei soldati trasformati in spie e assassini, e su cosa significa per il futuro.

Tuttavia, il mondo della riduzione delle firme continua a crescere: prove, dice l'ufficiale in pensione, che la vita moderna non è così trasparente come la maggior parte di noi pensa.



L'attività di supporto dei programmi di difesa, nota anche come Operational Planning and Travel Intelligence Center, uno degli epicendi per l'amministrazione della riduzione della firma. (foto fornita a William M. Arkin)

W.M. ARKIN

Pdf by:  
<https://www.pro-memoria.info>