



L'Uomo Comune: la strategia dello spionaggio russo

Pubblicato il 10/10/2026

Durante la Guerra Fredda, l'Europa divisa era il laboratorio privilegiato dello spionaggio clandestino. Nel lessico del controspionaggio si parlava comunemente di **agenti “dormienti”** o infiltrati sotto copertura (*Inoffizielle Mitarbeiter*), figure inserite con pazienza nel tessuto sociale con il compito di rimanere in attesa prima di **fornire supporto logistico, covi e informazioni riservate** alle reti operative del **GRU** sovietico e della **Stasi** est-tedesca.

Il luogo per eccellenza di questo scontro fu la **Germania Ovest**, dove la divisione del Paese forniva alla Repubblica Democratica Tedesca (DDR) condizioni ideali di infiltrazione. Il caso più celebre fu quello di **Günter Guillaume**: inviato nel 1956 in Occidente come sedicente rifugiato in fuga dal comunismo, Guillaume costruì per oltre quindici anni un'ineccepibile carriera politica nel Partito Socialdemocratico (SPD), fino a diventare **l'assistente personale del Cancelliere Willy Brandt**. La sua scoperta nel 1974 provocò uno dei più gravi shock politici della Guerra Fredda e le **dimissioni del Cancelliere**.

Accanto ai casi d'alto profilo politico, l'intelligence della DDR guidata da Markus Wolf perfezionò tattiche uniche come la rete dei cosiddetti **"Agenti Romeo"**: affascinanti operativi inviati a Bonn e nelle città dell'Ovest sotto falsa identità con lo specifico compito di **corteggiare e sedurre le segretarie dei ministeri e delle agenzie di sicurezza** della Germania Ovest, trasformandole inconsapevolmente in **preziose fonti di segreti di Stato**. Per approfondire questa tattica di seduzione e infiltrazione, il documentario [COLD WAR's Deadliest Trick: STASI's Romeo SPIES Are Back Online](#) analizza nel dettaglio l'evoluzione del "metodo Romeo" sviluppato dalla Stasi.

Oggi questo scenario si è ulteriormente evoluto. Con la drastica riduzione delle stazioni ufficiali presso le ambasciate, **Mosca ha riattivato e potenziato il programma degli "illegali"** (*Deep-cover operatives*), gestito dall'**SVR** (servizio d'intelligence esterna) e dal GRU, ereditando le tecniche di dissimulazione affinate proprio a Berlino Est nel secolo scorso.

Legali vs Illegali: La guerra delle coperture

Per comprendere l'impatto di questa minaccia, è necessario **distinguere le due figure operative** impiegate dai servizi russi:

Parametro Operativo	Agente "Legale"	Agente "Illegale"
Copertura	Diplomatica (Ambasciata, Consolato)	Fittizia (Imprenditore, Accademico, Gallerista)
Protezione Giuridica	Immunità diplomatica (Rischio espulsione)	Nessuna immunità (Rischio arresto e condanna)
Tracciabilità	Alta (Monitorato dal controspionaggio locale)	Pressoché nulla (Nessun legame con l'ambasciata)
Ruolo Strategico	Operato ordinario e rappresentanza	Snodo logistico e operatività in tempo di crisi

La scelta dell'illegale risponde a una logica di **invisibilità e continuità operativa**: un clandestino può **continuare ad agire anche quando le ambasciate vengono chiuse o svuotate**.

La “Fabbrica delle Leggende” e le coperture sudamericane

Il perno su cui ruota la vita dell'illegale è la “**leggenda**”, ovvero la **biografia fittizia costruita nei minimi dettagli**. Se in passato si usava la tecnica del *ghosting* (sostituzione dell'identità di neonati deceduti), oggi si prediligono i **passaporti dell'America Latina** (Argentina, Brasile, Perù).

I **registri anagrafici meno digitalizzati** consentono di ottenere documenti autentici, e l'origine sudamericana **giustifica con naturalezza l'accento straniero** e la mancanza di parenti in Europa. In questo schema, **la presenza di figli ignari** della reale identità dei genitori costituisce lo **scudo sociologico perfetto** per azzerare i sospetti del controspionaggio.

I casi emblematici in Europa e in Italia

La teoria trova riscontro in **recenti ed eclatanti operazioni di controspionaggio**:

- **Il caso Dultsev a Lubiana:** Una coppia con passaporti argentini — lui informatico, lei gallerista — gestiva un **hub logistico e finanziario nel cuore dell'Europa** prima dell'arresto e del successivo **scambio di prigionieri ad Ankara nel 2024**.
- **Il caso Maria Adela a Napoli:** Una finta designer di gioielli di origine peruviana (in realtà ufficiale del GRU) è riuscita a **infiltrarsi nella vita sociale della base NATO di Lago Patria**.
- **Infiltrazioni istituzionali:** Diversi operativi sono stati individuati mentre tentavano di inserirsi nella **Corte Penale Internazionale dell'Aja** o in **centri di ricerca universitari** in Nord Europa.

Prospettive e misure di difesa per la Sicurezza Nazionale

L'espulsione di centinaia di diplomatici russi dopo l'inizio del conflitto in Ucraina ha costretto Mosca ad affidarsi maggiormente alle **reti clandestine e ai collaboratori locali (proxies)**. L'Italia, per la presenza di **basi NATO, comandi alleati e industria della Difesa**, rappresenta un **obiettivo primario**.

Fronteggiare la "spia della porta accanto" non richiede paranoia verso i cittadini stranieri, ma un'efficace **strategia di prevenzione e sicurezza procedurale** basata su regole

fondamentali:

1. **Rafforzamento del Controspionaggio e Cooperazione:** Incrementare il tracciamento biometrico e documentale alle frontiere e intensificare lo **scambio informativo tempestivo tra i servizi alleati NATO ed europei**.
2. **Applicazione rigorosa del principio del *Need-to-Know*:** In ambito lavorativo, istituzionale e militare, l'accesso alle informazioni sensibili deve essere **strettamente limitato a chi ne ha effettiva e indispensabile necessità** per lo svolgimento delle proprie mansioni, evitando la condivisione cumulativa di dati.
3. **Cultura della Riservatezza Individuale:** Applicare una rigorosa **disciplina del silenzio (*Need-to-Share* limitato)** anche nelle cerchie personali e informali. Informazioni inerenti progetti della Difesa, spostamenti di personale, vulnerabilità tecnologiche o procedure operative **non devono essere discusse né condivise con familiari, amici o colleghi** privi della necessaria abilitazione di sicurezza.
4. **Resistenza all'Ingegneria Sociale e *Cyber Hygiene*:** Elevare la consapevolezza dei rischi legati all'**aggancio sociale (eventi benefici, circoli ricreativi, relazioni interpersonali)** e mantenere la massima attenzione nell'uso dei social network e dei canali di comunicazione privata.