



The Common Man: The Strategy of Russian Espionage

Published on 10/10/2026

During the Cold War, divided Europe was the premier testing ground for clandestine espionage. In counterintelligence terminology, the term **“sleeper” agents** or undercover infiltrators (*Inoffizielle Mitarbeiter*) was commonly used, referring to individuals patiently embedded in the social fabric and tasked with lying in wait before **providing logistical support, safe houses, and classified information** to the operational networks of the Soviet **GRU** and East German **Stasi**.

The epicenter of this confrontation was **West Germany**, where the country's division gave the German Democratic Republic (GDR) ideal conditions for infiltration. The most famous case was that of **Günter Guillaume**: sent to the West in 1956 as a purported refugee fleeing communism, Guillaume built an impeccable political career in the Social Democratic Party (SPD) over more than fifteen years, eventually becoming **Chancellor Willy Brandt's personal assistant**. His exposure in 1974 triggered one of the Cold War's most serious political shocks and the **Chancellor's resignation**.

Alongside high-profile political cases, the GDR's intelligence service, led by Markus Wolf, refined unique tactics such as the network of so-called **"Romeo Agents"**: charming operatives sent to Bonn and Western cities under false identities with the specific task of **courting and seducing secretaries at West German ministries and security agencies**, unwittingly turning them into **valuable sources of state secrets**. For a closer look at this tactic of seduction and infiltration, the documentary [COLD WAR's Deadliest Trick: STASI's Romeo SPIES Are Back Online](#) examines in detail the evolution of the Stasi-developed "Romeo method."

Today, this landscape has evolved further. With the drastic reduction in official embassy postings, **Moscow has reactivated and strengthened its “illegals” program** (*Deep-cover operatives*), run by the **SVR** (foreign intelligence service) and the GRU, drawing on the concealment techniques honed in East Berlin during the last century.

Legals vs. Illegals: The War of Covers

To understand the impact of this threat, it is necessary to **distinguish between the two types of operatives** employed by Russian intelligence services:

Operational Parameter	“Legal” Agent	“Illegal” Agent
Cover	Diplomatic (Embassy, Consulate)	Fictitious (Businessperson, Academic, Gallery Owner)
Legal Protection	Diplomatic immunity (Risk of expulsion)	No immunity (Risk of arrest and conviction)
Traceability	High (Monitored by local counterintelligence)	Virtually none (No ties to the embassy)
Strategic Role	Routine operations and representation	Logistical hub and operational capability in times of crisis

The choice of an illegal follows a logic of **invisibility and operational continuity**: a deep-cover operative can **continue operating even when embassies are closed or emptied**.

The “Factory of Legends” and South American covers

The cornerstone of an illegal's life is the **“legend,”** meaning a **fictitious biography constructed down to the smallest detail**. While the *ghosting* technique (assuming the identities of deceased infants) was used in the past, today **Latin American passports** (Argentina, Brazil, Peru) are preferred.

Less digitized civil registries make it possible to obtain genuine documents, while a South American background **naturally explains a foreign accent** and the absence of relatives in Europe. Under this model, **the presence of children unaware** of their parents' true identities provides the **perfect sociological shield** to dispel counterintelligence suspicions.

Emblematic cases in Europe and Italy

The theory is borne out by **recent high-profile counterintelligence operations**:

- **The Dultsev case in Ljubljana:** A couple holding Argentine passports — he a computer specialist, she a gallery owner — ran a **logistics and financial hub at the heart of Europe** before their arrest and subsequent **prisoner exchange in Ankara in 2024**.
- **The Maria Adela case in Naples:** A fake Peruvian-born jewelry designer (actually a GRU officer) managed to **infiltrate the social life of the NATO base at Lago Patria**.
- **Institutional infiltration:** Several operatives were identified while attempting to gain positions at the **International Criminal Court in The Hague** or at **university research centers** in Northern Europe.

Outlook and defense measures for National Security

The expulsion of hundreds of Russian diplomats following the start of the conflict in Ukraine has forced Moscow to rely more heavily on **clandestine networks and local collaborators (proxies)**. Italy, due to the presence of **NATO bases, Allied commands, and the defense industry**, represents a **primary target**.

Countering the “spy next door” does not require paranoia toward foreign nationals, but an effective **prevention and procedural security strategy** based on fundamental rules:

1. **Strengthening Counterintelligence and Cooperation:** Increase biometric and document screening at borders and intensify the **timely exchange of intelligence**

among NATO and European Allied services.

2. **Strict application of the *Need-to-Know* principle:** In workplace, institutional, and military settings, access to sensitive information must be **strictly limited to those with an actual and essential need** to perform their duties, avoiding the cumulative sharing of data.
3. **Culture of Individual Confidentiality:** Apply strict **information discipline (*Need-to-Share limited*)** even within personal and informal circles. Information concerning defense projects, personnel movements, technological vulnerabilities, or operational procedures **must not be discussed or shared with family members, friends, or colleagues** who do not hold the required security clearance.
4. **Resistance to Social Engineering and *Cyber Hygiene*:** Increase awareness of the risks associated with **social engagement (charity events, recreational clubs, interpersonal relationships)** and maintain the utmost caution when using social media and private communication channels.