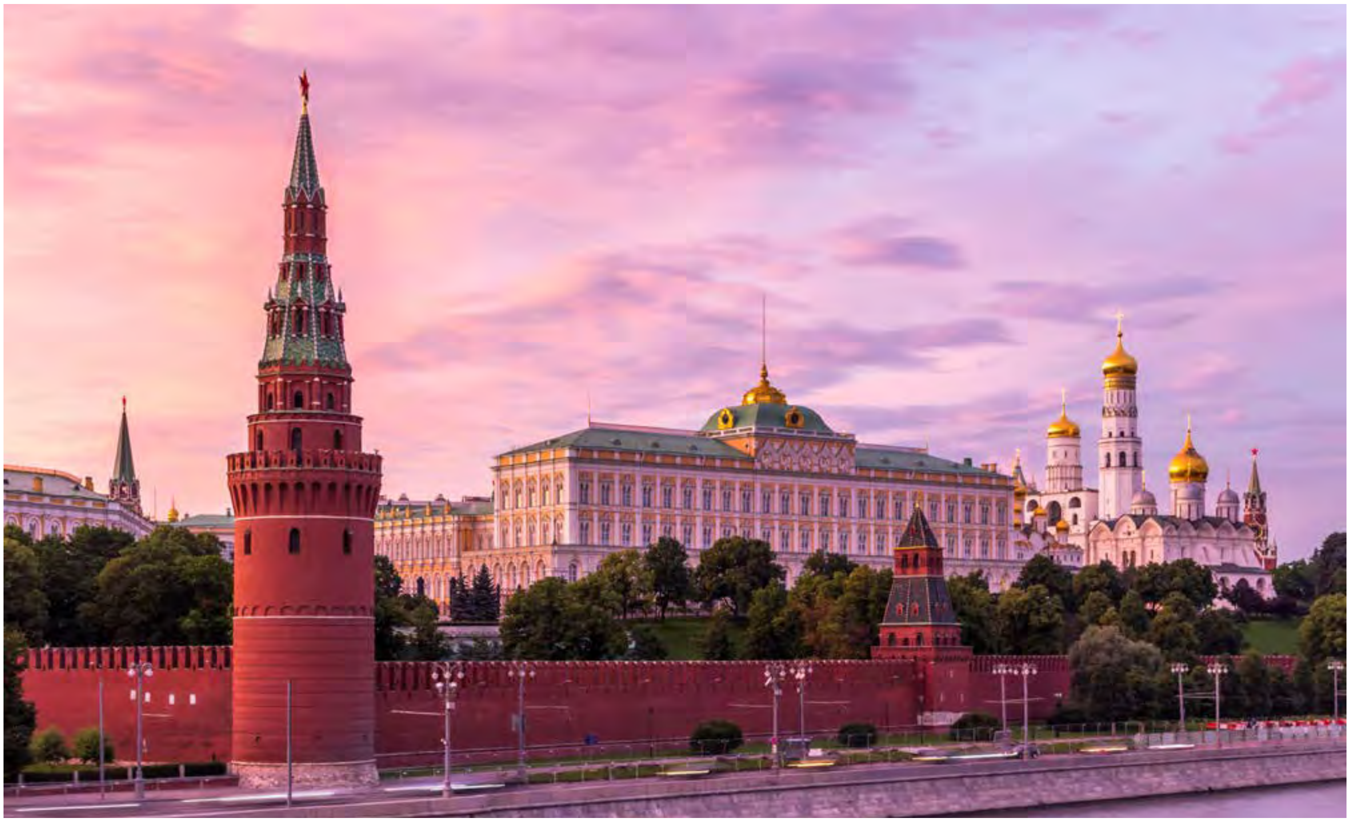

A view of the Kremlin in summer calls to mind fictional spymaster George Smiley's quip, "It would be beautiful in another context."

# "Beautiful in Another Context": A Counterintelligence Assessment of GTPROLOGUE

**Alexander Orleans**

Alexander Orleans is a cyber threat intelligence analyst and former US government contractor.

In the 1980s, the Soviet Union's Committee for State Security (KGB) launched a concentrated disinformation campaign as part of an effort to safeguard the identity of their CIA penetration agent, Aldrich Ames. Part of that campaign involved Aleksandr Vasilyevich "Sasha" Zhomov, dispatched as a dangle-type double agent by the KGB in May 1987 targeting CIA's Moscow Station and its Soviet and Eastern European (SE) Division. CIA assigned Zhomov the cryptonym GTPROLOGUE and accepted him as a source; he subsequently became a key disinformation and deception channel for the KGB. In a broader historical context, GTPROLOGUE exemplifies CIA's troubled experience with hostile double agents during the 1980s, when a few select services—particularly the Soviets, East Germans, and Cubans—badly burned the agency.

The views, opinions, and findings of the author expressed in this article should not be construed as asserting or implying US government endorsement of its factual statements and interpretations or representing the official positions of any component of the United States government.

Both the KGB's dispatch of Zhomov and CIA's handling of him as GTPROLOGUE are instructive. The former provides insight into the crafting of offensive counterintelligence operations, particularly underscoring how proper tailoring of a controlled source operation can manipulate a targeted service's attempts at asset validation and thus extend the lifespans of operations. The latter is a cautionary tale of counterintelligence flags that, when methodically inspected, could improve the likelihood of successfully unmasking future provocations.

This assessment is based entirely on publicly available material. To the author's knowledge, the primary source documents associated with this case remain classified, as do illuminating details they might contain. Also, the publicly available facts of the GTPROLOGUE case are rather disparate and occasionally contradictory. In attempting to reconcile such instances of contradiction, the author has preferred to use information that is supported by a preponderance of available research. With both of these qualifications in mind, what follows is an endeavor to present the first public, comprehensive, and contextual accounting of the case as well as its implications for running double-agent operations and conducting asset validation.

## Contemporaneous KGB Perspective

On June 13, 1985, Aldrich Ames used his position as a counterintelligence officer in CIA's elite Soviet and Eastern European (SE) Division to sell the identities of more than a dozen Soviet agents—including military and intelligence officers—secretly working for the United States to the KGB for $2 million in an escrow account.[1] The losses resulting from Ames's betrayal played out over the rest of 1985 and 1986. CIA learned of them in sporadic bursts during that two-year period, finding itself by 1987 operating at a marked disadvantage. The '85–86 losses, as they became colloquially known within CIA, also signaled the need for a major KGB undertaking to deceive CIA as to the real reason for these losses. A multichannel KGB disinformation campaign, which operated from at least 1986, was launched to convince SE Division that its losses were the result of anything but a penetration.[2]

Two narratives were included in this campaign. The first was that the KGB had managed to secure a technical penetration of CIA's Moscow Station in the US Embassy. The second, which this author terms the "SCD [Second Chief Directorate] omniscience narrative," was that the operational brilliance and ingenuity of the KGB's SCD, abetted by poor CIA tradecraft, had exposed CIA sources in Moscow that in reality had been betrayed by Ames.

To make this campaign as effective as possible, the KGB relied on its traditional approach to counterintelligence operations. A guiding principle was a certain aggressiveness that emphasized seizing the initiative from the enemy and staying on the offensive.[3] For the Soviet Union, counterintelligence—both foreign and domestic—was the principal raison d'etre of its intelligence efforts both as a revolutionary movement prior to October 1917 and later as a government. Harry Rositzke, the first chief of CIA's original Soviet Division, summarized this legacy:

> *… there is an intangible quality of Soviet intelligence that is perhaps its greatest strength. It is the natural product of the origins and character of Soviet society, what I choose to call the clandestine mentality, the psychological tendency and ability to think and act in secret.… The clandestine mentality is rooted in a conspiratorial view of the world: the world is an unsafe place, for someone out there is plotting against me.… Since the world is a threatening place, only secret counter-action can guarantee survival.*[4]

The emphasis on counterintelligence, and an offensive conception of it, was deeply ingrained in the institutional and operational culture of the KGB. According to the official KGB dictionaries of intelligence and counterintelligence terminologies, the three guiding principles of KGB operational culture were "clandestinity," "vigilance," and "aggressiveness."[5] Of the three, it was aggressiveness that was meant to suffuse the KGB officer's attitude toward operational action:

> [The style] *of counter-intelligence (intelligence) activity which is proactive and full of initiative, ensuring maximum success in the struggle against the enemy. It is a guiding principle which the intelligence and counter-intelligence agencies seek to follow in their work. In accordance with this, the side which takes the offensive will, all things being equal, achieve the best results.*[6]

The same terminologies defined "counter-intelligence" as:

> [The] *fight against the subversive activity of capitalist intelligence services, the organizations and individuals which they use and hostile elements within the country.… It is characterized by active measures designed to take the offensive against the enemy and to obtain information about his secret plans, intentions, and aspirations. This makes it possible to take steps in advance to forestall enemy subversive actions.*[7]

In attempting to forestall such adversary activity, the KGB "reflexively" favored the use of controlled source operations and mounted many dangle operations.[8] As the Cold War progressed, the KGB became known for extensively using double agents and dangles, most often for tactical counterintelligence (as opposed to strategic deception) purposes.[9] The use of dangles and double agents was considered to be valuable not only as a way to gain windows into an adversary services' motives and methods, but also to plant disinformation and tie down adversary personnel and resources in useless activity. This reflected a long-held preference to use disinformation to conceal real sources.[10]

By the 1980s, that norm of aggressiveness was tempered by two fears: potential punishment for over-disclosure of information during double-agent operations, and the risk that certain dangles would jump ship if given information significant enough to warrant substantial rewards from Western services. It was apparently "strict KGB doctrine that certain types of people and certain types of information would never be shared with CIA in double-agent operations."[11]

Within the KGB, the Soviet preoccupation with secrecy fostered an institutional bias against release of the sort of valid feed typically required to establish the credibility of a deception channel.[12] Stoking this bias among KGB officers running double-agent operations was the fear that someone higher up in the chain of command could decide later that passed information was in fact too sensitive to have been used as bait and then punish the officers involved. Ames himself said after his arrest:

> *Even if a document were of no real value, no one in the Soviet military was willing to sign off on releasing it, knowing that it was going to be passed to the West. They were afraid that a few months later, they would be called before some Stalinlike tribunal and be shot for treason.*[13]

As the pool of information available for use as valid feed was limited, so was the pool of available candidates for its delivery. The KGB feared using staff officers, who, given their rank and position, would have access to detailed knowledge of the KGB's internal workings—and should they defect would be worth their weight in gold to a Western counterintelligence service. Therefore, provocations dispatched by the KGB who actually worked inside the KGB typically presented themselves as having "peripheral or infrequent access" to information of particular interest to target services.[14] The KGB was still operating under both of these constraining policies when the decision was made to mount a disinformation campaign to conceal Ames's treachery. However, opportunities for innovation were provided by Ames himself.

Ames's initial betrayal to the KGB had been the identities of several sources whom CIA had accurately identified as KGB dangles but had chosen to run in order to monitor their production in an effort to ascertain KGB goals. Ames had chosen to expose these sources specifically because he convinced himself it was a moral way to make a quick buck, given that CIA was only receiving false information from them and that the KGB would not punish agents it truly controlled.[15] Yet, by revealing to the KGB which sources CIA knew to be dangles, he also was offering it vital details on how to craft future dangles in a way that would avoid detection.

At some point later in his career as a Soviet spy, Ames eventually provided explicit coaching to his KGB handlers on how to improve their dangle techniques and may have done so well that least a few subsequent dangles were taken by CIA as genuine.[16] This coaching likely included revealing the prevailing theories in the SE Division about how the Soviets ran double agents (discussed below).[17] It is possible that the nontraditional risks taken during the Zhomov case described below were, at least in part, a result of Ames explicitly providing such guidance. Similar guidance also may have been available to SCD via Edward Lee Howard, the former CIA officer who had previously betrayed CIA assets to the KGB and defected to the Soviet Union in 1985.[18]

## Dispatching Zhomov

Sometime in 1986, Valentin Klimenko, chief of the SCD's First Department, was directed by either his immediate superior—legendary SCD chief Rem Krasilnikov—or KGB Chairman Viktor Mikhailovich Chebrikov to dispatch a dangle against CIA's Moscow Station with the apparent intent of feeding the SCD omniscience narrative to CIA.[19] On December 22, 1986, Klimenko allegedly met with Aleksandr Zhomov in private, off of official KGB property, and directed him to develop a "plan for something special for our American special service boys" within one month.[20] Zhomov, 32, broke the mold of previous dangles run by the KGB in several ways, all of which were designed to make Zhomov appear as legitimate as possible in the eyes of CIA.[21] These aberrations included several aspects.

### *Rank and standing*

Zhomov was a staff officer in the First Department of the SCD, which was responsible for counterintelligence against Americans in Moscow, and he had served in the KGB for 10 years.

### *Responsibility*

Zhomov was the direct supervisor for all surveillance teams tasked to follow CIA officers in Moscow on a day-to-day basis; he also later described himself as Klimenko's executive assistant. Both descriptions suggest he worked with the First Department's Second Section—the unit responsible for countering intelligence operations emanating from the US Embassy—and either duty would provide him access to a veritable gold mine of intelligence of value to Western services, particularly CIA.[22]

### *Training*

Zhomov spoke English with near-native fluency, indicating a significant investment in him by the KGB, especially given the fact that he was a domestic counterintelligence officer, as opposed to a foreign operations officer.

To be selected as a provocation, an officer like Zhomov must have had Klimenko's absolute confidence and, given that Klimenko claimed he was directly tasked with running the operation, Klimenko must have had Cherbikov's absolute confidence as well.

## Running the Provocation

Zhomov's primary mission appears to have been to convince the Americans that the '85–86 losses were a result of the SCD's skills in following CIA officers, combined with poor tradecraft on the parts of US case officers and sources.[23] That SCD omniscience narrative provided benign explanations for the losses that, if believed, would both have a demoralizing effect on the CIA and deter it from looking inward for a mole.

Coincidentally, the narrative played into a growing paranoia in Moscow Station that the SCD had developed unshakable, "ultradiscreet surveillance" capabilities that CIA could not evade.[24] This paranoia was born of both the '85–86 losses and internal investigations, initiated on the basis of earlier KGB disinformation, that were in the process of ruling against the possibility of a technical penetration of Moscow Station. Available open sources do not indicate whether or not Ames shared those views with his KGB handlers prior to the development of the chosen deception narrative.

The entire operation was crafted to reinforce the SCD omniscience narrative, including the contact procedures Zhomov was to use and the feed he provided US intelligence. Zhomov's posting was to be his cover to contact CIA's chief of station (COS) in Moscow, Jack Downing. First, he would add to his portfolio the personal responsibility for monitoring Downing. This would ostensibly allow him to penetrate the tight KGB surveillance bubble around Downing and pass documents providing initial bona fides, a note outlining motivations for an offer of service to CIA, and instructions for future contact. This is precisely what happened one night in May 1987 in the last car of the *Red Arrow* overnight train between Moscow and Leningrad, which Downing was known to take on a regular basis.[25] Zhomov reportedly introduced himself as "Edwin" in his initial note to Downing.[26]

This first batch of documents included recent surveillance photos of Downing and his wife, along with a very long note by Zhomov. This note had three parts.[27] First was an accurate outline of Zhomov's position and responsibilities in the SCD, but without his name or a pseudonym. Second was an explanation of his purported motives: a mixture of growing frustration with the Soviet system and a failing marriage combining into a desire to leave for America, and thus an offer to spy for CIA to secure its good graces. Third was instructions for a communications plan ("commo plan") dictated by Zhomov: future contact was to be impersonal and at Zhomov's discretion but would utilize his role as Downing's surveillance officer.[28] Ironically, Zhomov's immediate and explicit willingness to spy for CIA, along with the offer of a thoroughly preconceived commo plan, would have been considered tell-tale signs of a dangle in the eyes of the SCD's foreign operations colleagues in the KGB's First Chief Directorate.[29]

This commo plan was designed by the SCD so it could control all aspects of Zhomov's contact with CIA personnel to the point of domination. In a double-agent operation, the concept of "control" can best be understood as:

> *. . . the capacity of a case officer (and his service) to generate, alter, or halt agent behavior by using or indicating his capacity to use physical or psychological means of leverage.... The degree to which an agent's communications can be controlled runs closely parallel with the degree to which he is physically controlled. Communications control, at least partial is essential: the agent himself is controlled to a considerable extent if his communications are controlled.* [30]

By that definition, the details of the commo plan ensured maximal SCD control over both the physical movements of, and communications between, Zhomov and Downing. Downing was to park his car at one of several restaurants or movie theaters listed in the note on each Friday night, leave his car unlocked, and go inside to the chosen establishment for a meal or film. Zhomov would enter Downing's car under the pretext of rifling Downing's briefcase for recently arrived diplomatic mail and deposit new documents in the briefcase. Should Downing wish to communicate with Zhomov, he was to include a specially marked envelope in his briefcase that Zhomov would know to take with him, effectively turning Downing's briefcase into a letter drop that was to be the primary channel of communication and contact. Brush passes on the *Red Arrow* would be secondary, but still possible given Zhomov's knowledge of Downing's movements.

These restrictive contact methods not only played into Zhomov's role as chief of surveillance on Downing, but also eliminated any chance for Downing to carefully interrogate Zhomov in person. The denied-area operational environment presented by Moscow—a key element of how the SCD intended to ensure control over the entire operation—inherently precluded face-to-face meetings with sources exceeding about four to seven minutes. Also, any request Downing made for such a meeting elsewhere in Russia could be refused by Zhomov on the grounds that he, of all people, could not be expected to escape the surveillance at which he claimed the SCD so excelled, especially given that they were his people and would notice his absence. Zhomov's posting also precluded a meeting outside the USSR, as SCD officers had lacked occupational excuses for travel abroad. Through these measures, the KGB also reinforced its own defensive counterintelligence position: the risk of Zhomov actually attempting to defect was considerably mitigated through the SCD's control over the operating environment and subsequently the tempo and nature of contact.

Construction of the "bodyguard of truth"[31] designed to safeguard Zhomov against intense CIA scrutiny continued with his second batch of documents, delivered via the planned letter drop procedures one Friday in June 1987. These documents, meant to attest to Zhomov's access, described an upcoming offensive counterintelligence campaign by the KGB. In the coming months, the SCD was planning to dispatch a number of provocations against Moscow Station, specially selected for their attractiveness to US intelligence interests, in order to keep CIA so busy vetting false volunteers that it would be unable to make time for real sources that may volunteer.[32]

Beginning in July and continuing over four more months, the KGB dutifully ran dangles matching descriptions provided in Zhomov's production.[33] Zhomov thus was seen by CIA as having provided valid, valuable information along a plausible line of access. (It is unknown what tradecraft Moscow Station employed in handling these dangles, but it was likely low-level tradecraft that SE Division had reason to believe was previously exposed or could risk exposure.) Having thus established his bona fides via production, Zhomov finally passed along the lie of the SCD omniscience narrative. During another letter drop in June, Zhomov turned over a complete and accurate list of all CIA sources arrested by the KGB in 1985 and 1986, as well their fates, but attributing all losses to the SCD omniscience narrative.[34] Internal KGB assessments of Downing and his predecessor as Moscow COS were included as well.[35] Both pieces of information fit rationally into Zhomov's demonstrated access.

### *Contemporaneous CIA Perspective*

At the time Zhomov appeared on CIA's radar, there was immense concern over determining the cause of the '85–86 losses. Beginning in January 1986, steps were taken within the SE Division to increase compartmentalization and to make inquiries, through offensive counterintelligence operations, into possible causes for the losses.[36] Those offensive operations returned only negatives, indicating that there had not been a penetration of the communication lines between the SE Division at headquarters and stations abroad.[37]

During 1986, two cases occupied much of the counterintelligence efforts regarding the '85–86 losses. First was Mister X, a self-declared—but anonymous—KGB officer who sent six letters to a CIA officer in Bonn between March and October 1986.[38] In these letters, Mister X claimed that a recently lost CIA source had been compromised by a technical penetration of Moscow Station. Mister X was later concluded to be fictional and his claims to be KGB were disinformation.[39] Second was Clayton Lonetree, a Marine Corps guard at the US Embassy in Moscow, who was caught in a honeypot by the KGB in 1985.[40] However, Lonetree knew little of use to the KGB and turned himself in to the CIA station chief in Vienna in 1986. SE Division closely followed the Naval Investigative Service case against Lonetree and, following his court martial in August 1987, debriefed him extensively before determining that he did not facilitate a KGB technical penetration of Moscow Station.[41]

All of these efforts occurred in the context of CIA's decades-long recovery from the tenure of James Angleton as chief of counterintelligence. Beginning in the early 1960s and continuing until his forced retirement in 1974, Angleton formed and operated under an intricate set of hypotheses in which the KGB was nearly omnipotent, all Soviet volunteers and defectors were likely provocations, and the KGB had a highly placed penetration in CIA. This state of affairs and its effects at CIA were summed up by one of its former chiefs of counterintelligence, Paul Redmond, in 2010:

> *Because there was a belief that the Soviets had penetrated the CIA during the 1960s and the early 1970s,* [Angleton's Counterintelligence Staff] *reigned supreme, paralyzing operations against the Warsaw Pact by assuming that the KGB knew of and controlled all operations. During the tenure of* [Director of Central Intelligence] *William Colby in the mid-1970s, there was a reaction to this mindset that destroyed CI at the CIA and* [led] *to spies in the Agency going undetected and the flowering of opposition-controlled cases.*[42]

It was in this environment that, in July 1971, CIA case officer Burton Gerber published a study of sources and volunteers that had been condemned as provocations by Angleton; Gerber correctly determined that most of them had likely been genuine and not under opposition control.[43, 44] His study was part of an ongoing and fierce internal debate within CIA over the validity of Angleton's theories. Following Angleton's departure, Gerber's paper found strong support and became quite influential, contributing to a renewed willingness by the SE Division to engage the Soviet human intelligence target, and—as explored below—eventually contributed to the asset-validation philosophy of the SE Division as it related to the KGB.[45]

The ill effects of the post-Angleton period extended to asset validation practices within CIA and, according to Redmond, included a "refusal of officers to believe their cases could be a fabricator or controlled by the opposition, particularly when promotions were involved," often in cases involving Warsaw Pact and Soviet sources.[46] This hindered asset validation efforts and increased the likelihood that dispatched double agents could go undetected or that legitimate ones could be tripled and returned to Soviet control. At the same time, CIA was grappling with the challenges of asset validation within denied areas. Again, Redmond is instructive:

> *Asset validation is a very difficult task, particularly when the source is handled in a "denied area" and there are few, if any, other sources of "collateral" information on which to rely for comparison.… In the absence of any sources of its own within the opposition service to warn them, Western services running cases in denied areas have had to rely on the value of the intelligence provided, corroboration of its validity by other sources, if available, and the operational circumstances surrounding the case—particularly how it started.*[47]

The author believes that this statement can be taken as indicative of CIA's philosophy on asset validation in denied areas. While that philosophy is sound, it labors under constraints that are both self-evident and significant. Therefore, officers working denied area cases must be intimately familiar with the tradecraft, preferences, and foibles of the particular opposition service they are laboring to operate against. These tailored insights supplement the four methods of asset validation possible in denied-area cases—identified by Redmond as penetration of the opposition, value of intelligence produced by the source, corroboration of said intelligence by other sources, and analysis of the case's origins—by making officers better able to detect patterns that could help determine whether or not a given source is under opposition control.

A relevant example of such a pattern in the case of GTPROLOGUE was foreshadowed by a key aspect of Gerber's 1971 study. One of the study's conclusions was that in none of the surveyed cases had the KGB dangled a staff officer, out of concern over the possibility of a real defection; as time went on, this conclusion became something akin to an operational rule of thumb within SE Division: the KGB did not dangle staff officers.[48] (Evidence also indicates that FBI agents during the Cold War separately arrived at, and also generally held, the view that the KGB "would never send a staff officer" as a dangle because of the risks involved if the officer chose to genuinely switch sides.[49])

By the time Zhomov's operation was conceived and launched by the KGB, the "staff officer theory" was apparently accepted, albeit informal, doctrine within much of SE Division. (However, it should be noted that nothing in open sources indicates that, in his 1971 study, Gerber ever suggested that the fact that the KGB had not previously dangled a staff officer could be treated as a guarantor of similar behavior in the future.) Given Ames's numerous postings within SE Division and his explicit coaching of the KGB on improving its provocation techniques, it is probable that he informed the KGB of the staff officer theory.

Shortly after Zhomov approached Downing for the first time in May 1987, the then-unidentified SCD officer was assigned the cryptonym GTPROLOGUE by SE Division.[50] Debate ensued over the new source's legitimacy that same month among SE Division's leaders at CIA Headquarters, mirroring similar debates probably taking place within Moscow Station. Despite the prevalence of the staff officer theory, some viewed GTPROLOGUE as unsettlingly well-timed and well-placed, particularly in light of CIA's desire for inside knowledge of the '85-86 losses.[51] The decision to run GTPROLOGUE and see where he took CIA was made by Gerber, who had been chief of SE Division since summer 1984, and his counterintelligence-minded deputy Redmond on the following explicit premise: if GTPROLOGUE were a legitimate volunteer, he would be a valuable source; conversely, should CIA determine him to be a dangle, his reporting would help indicate topics about which the KGB hoped to mislead CIA.[52]

CIA acquiesced to GTPROLOGUE's requested commo plan. In an effort to reduce the potential for compromise while maximizing opportunities for contact, Downing limited his trips on the *Red Arrow* to once every three months, and spent every Friday night at one of GTPROLOGUE's designated sites. While these logistics meant primary contact with GTPROLOGUE occurred through the letter drop, Downing discovered that GTPROLOGUE would make contact only about once a month, and that the Friday chosen for contact was unpredictable.[53] Available evidence indicates that no additional methods of contact ever were used between GTPROLOGUE and CIA.

When the SCD dangle campaign foretold by GTPROLOGUE's reporting came to pass, the SE Division's leadership directed Moscow Station to run the provocations, despite knowing their true allegiances. This decision was based on a desire to protect GTPROLOGUE: should the provocations be rejected, suspicion in the SCD could fall on him.[54] Soon, the running of these dangles occupied a majority of the station's resources, officers, and time—all with CIA knowledge that no reliable intelligence was being produced. This situation continued even though one instance of particularly sloppy tradecraft by the KGB blatantly revealed that two of the dangles were, in fact, provocations.[55] Had the KGB been taking those provocations seriously, rather than viewing them as ancillary aspects of the larger Zhomov operation, it should have taken steps to firm up the apparent legitimacy of the dangles in question in the aftermath of the error. However, there are no indications that the KGB made any such efforts, and available information indicates that CIA continued to run both dangles involved, rather than dropping them as could have been justified by the information exposed through the KGB's error in tradecraft.

"Shopping lists" of desired intelligence and questions aimed to test GTPROLOGUE's legitimacy were passed via the letter drops, and apparently no long debriefings allowing for face-to-face assessment of the source ever occurred. After his initial production about the SCD dangle campaign and the SCD omniscience account of the '85–86 losses, GTPROLOGUE never again delivered intelligence that could be described as "certain to hurt [the KGB]."[56] For his efforts, CIA evidently paid GTPROLOGUE "a good deal of money," although there is no clear indication of how or how much.[57] Assertions that he was given upward of $1 million as part of a joint CIA-FBI program aimed at tempting KGB officers to provide intelligence on the '85–86 losses are unproven, and have been made on the basis of what could be interpreted as a post hoc fallacy.[58]

In light of GTPROLOGUE's material attributing the '85–86 losses to the SCD omniscience narrative, SE Division counterintelligence officers working on the losses began to push for questions to be passed to GTPROLOGUE that were designed specifically to test his legitimacy as a penetration. But it appears that the idea of putting such questions to GTPROLOGUE was resisted by elements of SE Division's leadership, which raised a concern common to sensitive cases that questioning the asset too sharply would "make him mad."[59] The questions that eventually were put to GTPROLOGUE were met with answers the wary counterintelligence officers found to be "vague or improbable."[60] Whenever a "hard question" testing his legitimacy did get put to GTPROLOGUE, he would demur and claim that he was holding out on providing his most sensitive intelligence until after CIA had safely extracted him from Russia.[61] However, at no point did he ever request a timeline or express an immediate desire for extraction—a significant red flag.

## Uncovering GTPROLOGUE

Eventually, CIA learned GTPROLOGUE's identity through the debriefing of Sergey Papushin, a former SCD officer who defected to the FBI in New Jersey in November 1989.[62] Papushin, who had been acquainted with Zhomov during the former's KGB days, identified a photo of GTPROLOGUE as his former colleague during questioning by CIA, although he did not indicate an awareness of Zhomov's role as a double agent. But Papushin's knowledge of Zhomov did not gel with GTPROLOGUE's reporting about himself: while GTPROLOGUE claimed his marriage had essentially failed, and that this failure had contributed to his desire to defect, Papushin claimed that Zhomov was in fact happily married and doted upon his daughter.[63]

Over time, a combination of the drop-off in the quality GTPROLOGUE's production, poor answers to operational testing questions, and the discrepancies raised by Papushin's reporting all stoked the ongoing debate within SE Division (and the station) as to GTPROLOGUE's legitimacy as a bona fide volunteer versus a double agent. By April 1990, the five people on the GTPROLOGUE operational bigot list at CIA Headquarters were taking informal internal straw polls as to his true allegiance after each exchange between GTPROLOGUE and the new Moscow COS, Mike Cline. In these straw polls, a majority only declared GTPROLOGUE legitimate about 50 percent of the time.[64] Eventually, SE Division decided to deploy a "no exit" approach to determine GTPROLOGUE's legitimacy: attempting a mutually agreed exfiltration operation of Zhomov in July 1990.[65] On April 5, 1990, the final decision to go through with an exfiltration was made by Deputy Director for Operations Richard Stolz, supported by the recommendation of then-SE Division Chief Milt Bearden.[66]

## Failure and Extraction

Before the April 5 decision, SE Division developed an exfiltration operation to take GTPROLOGUE out of Russia by having him travel to Estonia and pass from there to Helsinki by ferry on a US passport altered by CIA Technical Services.[67] Several weeks before, extraction had been floated to GTPROLOGUE along with a request for photos to be used in the passport. GTPROLOGUE agreed, provided the requested photos, and later was passed the passport via a dead drop in Moscow.[68]

GTPROLOGUE now was supposed to leave Russia for Estonia on July 10, 1990, but by July 14 he still had not arrived in Helsinki.[69] On July 14, Cline was asked to take the *Red Arrow* with his wife to Leningrad, on the off chance that GTPROLOGUE would attempt a brush pass to explain why he had not followed through on the exfiltration.[70]

A man, possibly GTPROLOGUE, did conduct a brush pass to Cline's wife that night aboard the *Red Arrow*. The passed note expressed "exasperation and rage," decrying the identity provided for the exfiltration as too risky to use and telling CIA that the writer was going to have to lie low and would initiate future contact when he felt it was safe.[71] After the *Red Arrow* arrived in Leningrad, the Clines found themselves under especially heavy surveillance and quickly noticed that GTPROLOGUE was blatantly part of their usual KGB surveillance team. Combined with the contents of the final passed note, these events led SE Division's leadership to conclude that GTPROLOGUE had been under KGB control for his entire operational life as a CIA asset, and effectively ended CIA's dealings with him.[72]

Ames' connections to GTPROLOGUE provide, at most, odd postscripts to the case. In 1989, some of GTPROLOGUE's reporting on dangles apparently led CIA to discard the reporting of a Russian volunteer (Sergey Fedorenko, a former academic who had been permitted to leave the Soviet Union) as possibly under KGB control, when in fact he was not.[73] Ironically, Ames was one of the few individuals in CIA at the time who disputed the applicability of GTPROLOGUE's intelligence to the defector.[74] Ames, acting as an unwitting playback mechanism for the SCD, later would pass information to the KGB throughout 1990 warning it of GTPROLOGUE's existence, but was apparently reassured by his handler that GTPROLOGUE would not betray Ames to CIA.[75] Ames's reporting on GTPROLOGUE may also have been viewed as something of a test of Ames by his handlers in Line KR of the KGB's First Chief Directorate (FCD). Knowing the true nature of GTPROLOGUE's activity, the KGB could compare operational details from SCD to material passed to FCD by Ames; discrepancies or alignments between these two data sets could be used to gauge Ames' access and continued willingness to (or not to) share information.

## Missed Warning Signs

In hindsight, the GTPROLOGUE case presented a number of counterintelligence flags to CIA before he was offered exfiltration and its aftermath. Those flags, taken in sum and relation to one another, make the case useful as a cautionary tale. They also exemplify the complexity of asset validation, never a simple task even in the most straightforward of situations: a flag that is truly a cause for concern in one case may also appear in the case of a bona fide asset as well. And in the case of GTPROLOGUE, efforts to discern the truth behind such flags were complicated by a denied area operational environment, Zhomov's potential as a high-value counterintelligence asset, and contradictory data. The primary flags were:

### *Limited Production*

Zhomov exhibited a continuing evasiveness regarding requests for certain information commensurate with his access. Despite the use of some valid feed and Zhomov's position as a staff officer, CIA counterintelligence officers would note later that Zhomov still had claimed the kind of limited reporting ability that had characterized past KGB-controlled dangles. Namely, that he claimed to only have peripheral or infrequent access to information that should have been easily available given his rank and posting.[76]

### Impeded Validation Efforts

CIA's efforts aimed at validating the case were substantially impeded and, at best, met with mixed results. These included Zhomov's poor responses to vetting questions and his limited production. This situation was compounded by the fact that CIA's ability to engage in a continuous and ongoing program of operational testing was severely limited in two ways. First, the impersonal commo plan dictated by Zhomov limited contact only to brush passes and letter drops. Second, the entire case took place within Soviet Russia (primarily Moscow), a denied area that presented all of the obstacles outlined by Redmond above, and also inherently precluded debriefings or long meetings. The fact that the denied area setting generally maximized the KGB's ability to contain the risks it faced in running the operation cannot be understated.

### Lack of Operational Control

Zhomov insisted on controlling the initiation and tempo of all contact, which of course was to be run through the impersonal commo plan and already was constrained by the denied-area conditions of the environment. A key to running agents successfully is fostering emotional dependence on their handlers and for handlers to maintain sufficient capacity to exercise physical or psychological means of leverage over the agents.[77] But in this case, it was GTPROLOGUE's CIA handlers who were dependent on him;  none of those handlers had any leverage over him except threats of compromise or noncooperation, neither of which had much utility.

### Weakness of Alleged Motives

Zhomov appeared to lack a coherent account for the powerful motive necessary to cross the major psychological line of engaging in espionage against his own service. The defector Papushin's independent reporting directly contradicted Zhomov's own reporting on his home life, and thus undermined the credibility of Zhomov's alleged motive for spying. Also, while claiming both a desire to leave the USSR and to be saving information of further interest to CIA for his eventual debriefing in the United States, Zhomov never requested a timeline for his exfiltration.[78]

### Topicality of Assignment and Production

That the SCD officer whom CIA would perhaps most have liked to run as a defector-in-place—not too high up in rank, with plausible access to intelligence of immediate interest, able to get close to CIA personnel without arousing suspicion—volunteered as a source was perceived by some as too good to be true. While "too good" and "true" are not by any means mutually exclusive characteristics of an asset, the former always heightens scrutiny to ensure the latter.

### Errors in Opposition Tradecraft

As discussed above, a particular error in the KGB's handling of the SCD dangles that GTPROLOGUE "compromised" to CIA led to the blatant exposure of two of the dangles as under hostile control. If the KGB were taking its new dangle campaign as seriously as GTPROLOGUE claimed, that error should have further aroused CIA's skepticism. Instead, it seems that Moscow Station attributed the error to endemically poor SCD tradecraft, which should have appeared inconsistent with GTPROLOGUE's reporting of the SCD omniscience narrative that claimed that the SCD of recent years was at the top of its game.

To CIA's credit, neither the SCD omniscience narrative nor Zhomov's legitimacy were taken as de facto truths by its officers. But while the omniscience narrative was not taken as fact at any time by any member of the SE Division—at most, it was taken as an avenue of investigation worthy of attention as a possible explanation for the '85–86 losses—it still certainly reinforced how the operational risks of Moscow presented a possible explanation. Available accounts also clearly indicate that SE Division's leadership harbored varying levels of suspicion toward Zhomov throughout the case and the division's counterintelligence staff regularly expressed their growing concerns.[79] At the onset of the case, then-SE Division chief Gerber and his deputy Redmond were suspicious of GTPROLOGUE, and as the case went on those suspicions never abated. When Gerber left his post as chief of the SE Division in 1989, he was still skeptical of GTPROLOGUE. By that time, SE Division counterintelligence officers also had begun to develop their own apprehensions about the case. While those counterintelligence officers' views were resisted by Gerber's successor, Bearden, even he and his senior staff clearly harbored their own concerns regarding Zhomov's true allegiances.

A potential reason for an apparent lack of harsher scrutiny of GTPROLOGUE is "the hunger": that driving desire of case officers for success in the form of a spectacular intelligence coup. That is, it is possible that there may have been a desire on the part of the case officers and managers to make the best of as potentially valuable a case as GTPROLOGUE, despite concerns over the source's legitimacy. According to a former Directorate of Operations division chief, this practice certainly is not unheard of.[80] (A possible parallel may be drawn with FBI cases where high-level criminals being run as confidential informants take advantage of the trust of their handlers in order to facilitate criminal agendas.[81]) As mentioned above, there also were indications during the latter stages of the case that the SE Division's leadership apparently felt that Zhomov was such a highly placed source that questioning him sharply could have risked withdrawal of his cooperation.

### *Offensive Resourcefulness*

In the running of Zhomov, the KGB displayed significant resourcefulness by breaking from traditional constraints that CIA had detected in earlier Soviet operations—particularly using a staff officer as a dangle and using highly sensitive valid feed material—and the resulting provocation operation was exceptional. The operation was tailored to fill a gap in CIA knowledge that the KGB knew to be of pressing interest to its adversary. Zhomov was presented as having plausible access to relevant vital information, and his rank and posting played on the SE Division's internal preconceptions about volunteering KGB officers. That the KGB chose Zhomov in particular, given his rank and posting, was essential to the operation's success. Access to the sort of intelligence he provided would have seemed highly improbable otherwise, and such information coming from a less-qualified source likely would have been treated with greater suspicion. All of these elements fulfilled traditional key requirements for a successful dangle operation.[82]

The KGB effectively established the "bodyguard of truth" around the lie of Zhomov's true allegiance, by serving up an entire SCD dangle campaign to validate GTPROLOGUE's reporting. While costly, in a single stroke that campaign validated GTPROLOGUE to CIA and deftly tied down Moscow Station. Also, the operation was launched at a time when CIA was recovering from severe setbacks in its competition with the KGB, and thus was more likely to be susceptible to a well-crafted dangle.[83] Finally, the KGB ran Zhomov at CIA for several years, giving the operation plenty of time to bear fruit.

By the standards of former chief of CIA counterintelligence James Olson, Zhomov netted at least six types of positive results that a double agent operation can produce for a controlling service.[84] He was able to reveal CIA denied area tradecraft (including an exfiltration route); assess CIA personnel (particularly chiefs of station); serve as a deception channel regarding the causes of the '85–86 losses; expose CIA collection requirements; tie up Moscow Station resources through the futile activity of running dangles, including himself; and, more than likely, take CIA money.[85] The operation also presented the SCD with potential opportunities to arrest CIA officers or cast doubt on the validity and information of genuine volunteers through Zhomov's reporting. Conversely, during his time as GTPROLOGUE, Zhomov's reporting was almost entirely unproductive for CIA, with two qualified exceptions: he did produce an accurate list of the assets CIA had lost during 1985 and 1986 (although that list was presented in the context of the SCD omniscience narrative), and he forewarned upcoming dangles in Moscow (that still resulted in a drain on CIA resources).

In its success as a counterintelligence effects-based operation, the dangling of GTPROLOGUE was also a textbook deception operation when measured against the standards of strategic deception operations mounted by the Allies during World War II.[86] The operation was ostensibly aimed at making CIA *do* something (i.e., not look inward for the source of the losses), rather than simply *believe* something. It was not mounted simply because the KGB had the resources to do so, but was part of a concentrated disinformation campaign with a simple unitary objective: dissuade, or at least distract, CIA from engaging in a mole hunt.

As noted, Zhomov claimed a limited reporting ability to his CIA handlers despite his rank and position within SCD.[87] In hindsight this is not terribly surprising. The KGB was taking a significant risk in dangling a staff officer, and apparently pursued every available means to mitigate that risk over the course of the operation. It is likely the KGB only felt comfortable engaging in such a gambit because it knew the SCD would have home field advantage in the denied area that was Russia, allowing the SCD to maximize its control over both the operation and Zhomov personally. That it supplemented such a safeguard by having Zhomov follow reporting habits that helped justify limited reporting, to avoid giving away more valid feed than absolutely necessary, makes sense. Perhaps the only glaring weaknesses in the operation from the perspective of the KGB's tradecraft was Zhomov's flimsy motives as GTPROLOGUE and the apparent lack of reinforcement of those motives through GTPROLOGUE's reporting to CIA.

## Conditional KGB Success

Dangling Zhomov was largely a success for the KGB as an offensive counterintelligence operation. It clearly fulfilled its potential against CIA as an effects-based operation at the operational and tactical levels, and there is evidence, although ambiguous, that it fulfilled a strategic objective as well. Operationally, Zhomov's "revelation" of a dangle program cleverly tied up some CIA resources in Moscow while simultaneously contributing to both his bona fides and (indirectly) the credibility of the SCD omniscience narrative. Tactically, the impersonal commo plan allowed the KGB to introduce a degree of physical control over the movements of GTPROLOGUE's CIA handlers. In a broader sense, the counterintelligence benefits of running such a successful dangle helped increase KGB knowledge of CIA, as noted above.

At the strategic level, Zhomov's feed about the '85–86 losses and SCD omniscience was meant to serve as part of the bodyguard of lies the KGB was constructing around the truth of Ames's betrayal. There is no evidence to support the conclusion that Zhomov's reporting convinced CIA to seriously consider the SCD omniscience narrative as a more viable cause than a human penetration. But an argument could be made that the KGB's primary strategic aim was just to buy time by temporarily diverting counterintelligence attention from an active asset through presentation of an alternate narrative. If this was in fact the KGB's actual intention, then the operation would more properly be considered a strategic counterintelligence success, as opposed to a strategic deception. (In this case, a useful way to conceive of the difference between achievements in strategic counterintelligence and in strategic deception would be that the former amounts to more of an "operational deception" than the latter, which is closer in equivalency to a "national deception."[88])

As a matter of historical record, CIA counterintelligence did not begin to focus on Ames until November 1989, when he was still one of several individuals under examination; a more exclusive concentration on him only developed in spring 1991.[89] The Foreign Intelligence Service (SVR), the post-Soviet successor to the KGB FCD, continued to run Ames until his arrest in 1994, the result of an intensive mole hunt by CIA and the FBI.

The two principal SCD officers involved in the GTPROLOGUE case went on to have long and successful careers within the Federal Security Service (FSB), the post-Soviet successor to SCD. Valentin Klimenko served in a variety of senior roles, rising to the rank of at least lieutenant general while in FSB-CIA liaison roles in Moscow and serving as the FSB representative in Israel in approximately 2003.[90] After retiring, he published in 2018 an autobiography titled *Notes of a Counterintelligence Officer*, which discussed the Zhomov case in some detail.[91]

Zhomov would become a prolific figure within the FSB and something of a perennial nemesis for CIA. He continued to serve in SCD's First Department through its transition into the FSB's American Department and its current incarnation as the elite Department of Counterintelligence Operations (DKRO) within the FSB's Counterintelligence (First) Service.[92] During this time, some of his known exploits include the arrest of Alexander Zaporozhsky (an SVR counterintelligence officer who helped CIA identify Ames as a penetration), serving as the FSB's liaison to CIA in Moscow, and playing a significant role in the 2010 Vienna spy swap between the United States and Russia.[93] For an undetermined period of time between approximately 2010 and at least 2019, Zhomov was the chief of DKRO; he eventually reached the rank of Colonel-General.[94]

In a broader historical context, GTPROLOGUE is an example of CIA's troubled experience with hostile double agents during the 1980s, when a few select services—particularly the Soviets, East Germans, and Cubans—badly burned the agency. As a result of earlier cases, in 1987 CIA had already begun to "[develop] a formalized counterintelligence review process, known as the Agent Validation System" to ensure thorough testing of sources for hostile control;[95] the AVS was formally introduced to the Directorate of Operations in 1991.[96]

## Conclusions

Zhomov as GTPROLOGUE exemplifies an effective dangle. From operational setting to asset credentials to contact methods to feed, each aspect of the KGB's operation was structured with an innovativeness worthy of emulation. To quote John le Carré's fictional spymaster George Smiley, "It would be beautiful in another context."[97] The KGB successfully structured the operation to seize and withhold the initiative from CIA (within the context of the case), while still working to maximize Zhomov's attractiveness as a source. The operation also demonstrated the historical truth that if you can tell an adversary something it desperately wishes to know more about, it will listen even if it suspects you are lying. All of these elements are the clearest signs that Ames's reporting on CIA knowledge of past KGB double agents may have informed the planning of the Zhomov operation. The weakest aspects of the KGB's running of Zhomov were his alleged motives; more thoroughly backstopping those could have potentially further strengthened GTPROLOGUE's apparent legitimacy.

However, this case does not simply provide insight into the mounting of effective dangles. It also drives home the difficulty of asset validation. In particular, efforts to validate GTPROLOGUE grappled with the added complications of conducting the process in a denied area and conducting it when examining a potential high-value counterintelligence asset. The flags discussed above arose from, or were exacerbated by, these added layers of complexity. Operational and practical constraints created an inability to engage in preferred methods and amounts of testing. And particularly in counterintelligence operations where the collection target is an aware and hostile actor, as much operational testing as possible is desirable to address doubts that may arise over time.[98]

Because a highly placed penetration poses a potentially significant weapon against the running service if doubled (as controlled at the outset of a case or later in the future), no single metric can be considered to excuse a CI asset from close scrutiny; production alone should not be taken as a solid indication of bona fides. All six traditional methods of asset validation—corroborating production through other sources; specific taskings and operational testing; collecting intelligence on the asset in question; polygraphing the asset; penetrating the local service to uncover potential information on the asset in question; and surveillance of the asset—should be considered carefully and pursued as necessary to return the strongest possible judgment as to an asset's reliability. That judgment then should be reevaluated constantly and actively, as it can never be taken for granted what has or has not happened to sources since they last established bona fides, with the intention of carrying out the sort of programmatic approach to evaluation tempered by officers' instincts meant to be realized by the AVS. In the case of Zhomov, the KGB wisely conducted the operation in the denied area it controlled, resulting in a blanket impediment to all avenues of asset validation.

All intelligence professionals always must be ready to accept something entirely new, including in the tradecraft of adversaries, because everything happens once for the first time. This logic never should be far from a counterintelligence officer's mind. Detection of such critical anomalies in operations often arises as the result of spirited internal debates on delicate aspects of cases, including the reliability of assets. Concerns raised during these debates should be taken seriously by all parties involved. Discounting potential issues about a source's bona fides, whether from a fear of irking the source with additional operational testing or from a desire to believe in an asset's potentially high-value reporting; letting the hunger, no matter how well intentioned, override the necessary skepticism intrinsic to human intelligence operations may very well backfire. Such considerations should not be seen as valid reasons for reluctance to subject an asset to operational testing that is as vigorous as possible. ■

# Endnotes

1. Michael Sulick, *American Spies: Espionage against the United States from the Cold War to the Present* (Georgetown University Press, 2014), 192–93.
2. Victor Cherkashin and Gregory Feifer, *Spy Handler: Memoir of a KGB Officer: the True Story of the Man who Recruited Robert Hanssen and Aldrich Ames* (Basic Books, 2005), 260; Sandra Grimes and Jeanne Vertefeuille, *Circle of Treason: A CIA Account of the Traitor Aldrich Ames and the Men He Betrayed*, (Naval Institute Press, 2012), 103; Sulick, 194.
3. Tennent H. Bagley, *Spy Wars: Moles, Mysteries, and Deadly Games* (Yale University Press: 2007), 105–106.
4. Harry Rositzke, *The KGB: The Eyes of Russia* (Doubleday, 1981), 48–49.
5. Vasiliy Mitrokhin, *KGB Lexicon: The Soviet Intelligence Officer's Handbook* (Routledge, 2006), 173, 231–32, 261.
6. Ibid., 261.
7. Ibid., 198.
8. Paul Redmond, "The Challenges of Counterintelligence," in *The Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson (Oxford University Press, 2012), 545.
9. William R. Johnson, *Thwarting Enemies at Home and Abroad* (Georgetown University Press, 2009), 92, 98, 113–14; Peter Deriabin and T.H. Bagley, *KGB: Masters of the Soviet Union* (Hippocrene Books, 1990), 251–52, 266–67; Richards J. Heuer, Jr., "Soviet Organization and Doctrine for Strategic Deception," in *Soviet Strategic Deception*, edited by Brian D. Dailey and Patrick J. Parker (D.C. Heath and Company, 1987), 35, 40.
10. Mitrokhin, 146–47.
11. John Diamond, *The CIA and the Culture of Failure: U.S. Intelligence from the End of the Cold War to the Invasion of Iraq* (Stanford Security Studies, 2008), 230.

12. Heuer, 41.
13. Pete Earley, *Confessions of a Spy: the Real Story of Aldrich Ames* (G.P. Putnam's Sons, 1997), 92.
14. Grimes and Vertefeuille, 21.
15. Diamond, 230; Earley, 139.
16. Earley, 139; Diamond, 230–31; David Wise, *Nightmover*, (Harper Collins, 1995), 114–15.
17. Cherkashin and Feifer, 261; Bagley 227.
18. Sulick, 115–23.
19. Milt Bearden and James Risen, *The Main Enemy: The Inside Story of the CIA's Final Showdown with the KGB* (Presidio Press, 2003), 197.
20. Ibid., 196.
21. Ibid., 196, 291; Cherkashin and Feifer 260–61.
22. John Barron, *KGB: The Secret Work of Soviet Secret Agents* (Reader's Digest Press, 1974), 81.
23. Grimes and Vertefeuille 118; Bearden and Risen, 295.
24. Bearden and Risen, 293, 299.
25. Ibid., 289–91; Grimes and Vertefeuille claim (117, 211) that the GTPROLOGUE case began in June 1988, but the preponderance of available information, including Bearden's and Risen's timelines, place its beginning in May 1987.
26. Andrei Soldatov, "Департамент контрразведывательных операций (ДКРО) ФСБ" Agentura.ru (2022). https://agentura.ru/profile/federalnaja-sluzhba-bezopasnosti-rossii-fsb/departament-kontrrazvedyvatelnyh-operacij-dkro/.
27. Bearden and Risen, 291; Grimes and Vertefeuille 119.
28. Bearden and Risen, 291–92.
29. Pete Earley, *Comrade J: The Untold Secrets of Russia's Master Spy in America After the End of the Cold War* (Berkley Books, 2007), 49–50.
30. F.M. Begoum, "Observations on the Double Agent," *Studies in Intelligence* 6, No. 1 (1962), 65, 66; available at https://cia.gov/resources/csi/studies-in-intelligence/archives/vol-6-no-1/observations-on-the-double-agent/.
31. Thaddeus Holt, *The Deceivers: Allied Military Deception in the Second World War* (Skyhorse Publishing, 2007), 72n.
32. Bearden and Risen, 295.
33. Ibid., 298–99.
34. Ibid., 295, 297; Grimes and Vertefeuille, 118.
35. Bearden and Risen, 297–98.
36. Grimes and Vertefeuille, 102–103.
37. Bearden and Risen, 153–56.
38. Ibid., 169–70, 190–91.
39. Grimes and Vertefeuille, 103-104.
40. Ibid., 108.
41. Ibid., 110–11.
42. Redmond, 540.
43. Bearden and Risen, 23–24.
44. David E. Hoffman, The Billion Dollar Spy (2015), 23–24.
45. Grimes and Vertefeuille, 24.
46. Redmond, 545.
47. Ibid., 545–6.
48. Grimes and Vertefeuille, 24; Bearden and Risen, 23, 296; Hoffman, 24; Cherkashin and Feifer, 261; Bagley 227.
49. David Wise, "When the FBI Spent Decades Hunting for a Soviet Spy on Its Staff," *Smithsonian Magazine* (October 2013). http://www.smithsonianmag.com/history/when-the-fbi-spent-decades-hunting-for-a-soviet-spy-on-its-staff-15561/.
50. Bearden and Risen, 296.
51. Ibid., 296–97.
52. Ibid., 297.
53. Ibid., 298.
54. Ibid., 298–99.
55. Ibid., 299.
56. Ibid., 422.
57. Grimes and Vertefeuille, 119.
58. Benjamin B. Fischer, "Spy Dust and Ghost Surveillance: How the KGB Spooked the CIA and Hid Aldrich Ames in Plain Sight," *International Journal of Intelligence and Counterintelligence* 24, No. 2 (2011), 287, 294; Fischer, "Doubles Troubles: The CIA and Double Agents," *International Journal of Intelligence and Counterintelligence* 29, No. 1 (2016), 51–52; Earley, *Confessions*, 259, 294.

59. Grimes and Vertefeuille, 118.
60. Ibid., 119.
61. Bearden and Risen, 423.
62. Ibid., 421, 395; Grimes and Vertefeuille, 118–9
63. Grimes and Vertefeuille, 118–9.
64. Bearden and Risen, 422.
65. Ibid., 422.
66. Ibid., 424.
67. Ibid., 435.
68. Ibid., 422, 435.
69. Ibid., 435.
70. Ibid..
71. Ibid., 436.
72. Ibid., 437.
73. Grimes and Vertefeuille, 123–24.
74. Ibid., 124; Earley, *Confessions*, 272.
75. Earley, *Confessions*, 276–77, 287; Wise, 191.
76. Grimes and Vertefeuille, 21, 24; Heuer, 36–40.
77. Begoum, 65.
78. Bearden and Risen, 423.
79. Grimes and Vertefeuille, 118–19; Bearden and Risen, 296–97, 422–23.
80. Author interviews with former CIA executive; spring 2014.
81. Author interview with Dr. John Fox, FBI historian; April 7, 2014.
82. Johnson, 106, 109, 113, 128, 197.
83. Holt, 58.
84. James M. Olson, *Fair Play: the Moral Dilemmas of Spying* (Potomac Books, 2006), 234n13.
85. According to a former CIA case officer with extensive Soviet operations experience, "Money paid is not money lost. It is money invested, even with a dangle. It sends a message to those witting back in the mother ship of KGB headquarters that the CIA is good to its word: they pay and they follow through—all attributes a volunteer wants to see before taking the step off the cliff." Author interview with former CIA operations officer, spring 2018.
86. Holt, 50–51, 53, 58, 71, 72.
87. Grimes and Vertefeuille, 21, 24; Heuer, 36–40.
88. Begoum, 62.
89. Grimes and Vertefeuille, 120–21, 125–26, 129–30, 142–43.
90. Bearden and Risen, 522; Rolf Mowatt-Larssen, "US and Russian Intelligence Cooperation during the Yeltsin Years" (February 11, 2011). https://www.belfercenter.org/publication/us-and-russian-intelligence-cooperation-during-yeltsin-years.
91. Filip Kovacevic (@chekistmonitor), "Valentin Klimenko was a top-ranking #KGB CI officer in the 1980s; in charge of the 1st Sec. of the 1st Dept. of the SCD, focusing on the U.S. Embassy & CIA station in Moscow.", Twitter/X, May 10, 2023, 11:00 AM, <https://x.com/ChekistMonitor/status/1656313194359709700>; Valentin Klimenko, Notes of a Counterintelligence Officer (International Relations, 2018). http://loveread.ec/view_global.php?id=85044. Klimenko's account of the Zhomov case contradicts available English-language sources in a number of critical aspects that are not corroborated by any other sources; for this reason, as well as Klimenko's affiliation and implied associated agenda, his statements regarding the case must be viewed with skepticism and were not treated as a reliable source of data for this analysis.
92. Joe Parkinson and Drew Hinshaw, "Inside the Secretive Russian Security Force That Targets Americans", *Wall Street Journal* (July 7, 2023). https://www.wsj.com/articles/fsb-evan-gershkovich-russia-security-force-dkro-e9cf9a49.
93. Gordon Corera, *Russians Among Us* (HarperCollins, 2020), 51–59, 114–16, 285–86, 297–98.
94. Kevin P. Riehle, *The Russian FSB: A Concise History of the Federal Security Service* (Georgetown University Press, 2024), 32; Soldatov.
95. Olson, 253n25.
96. Melissa Boyle Mahle, *Denial and Deception: An Insider's View of the CIA* (Nation Books, 2006), 231–32.
97. John le Carré, *Tinker, Tailor, Soldier, Spy* (Pocket Books, 2002), 332–33.
98. Beogum, 71. ■