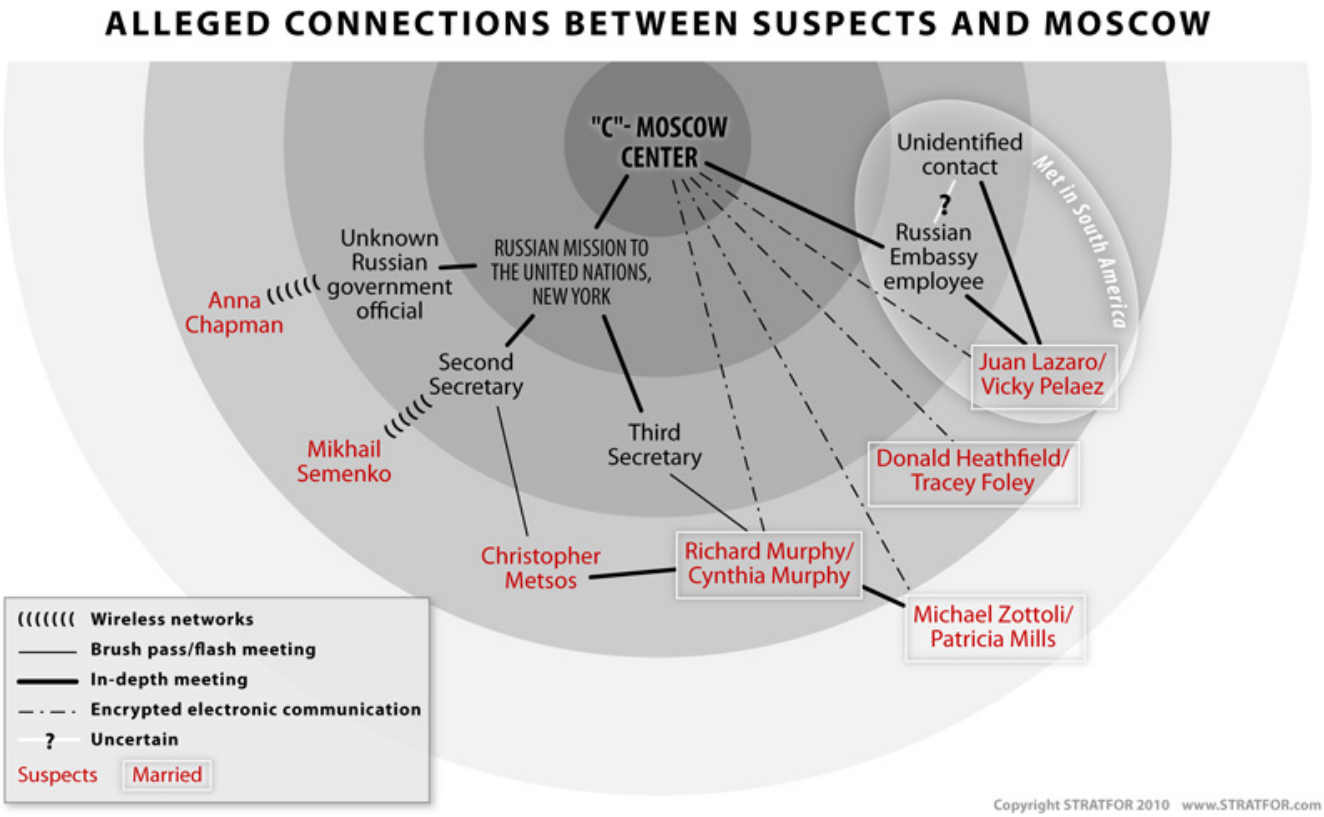
By Fred Burton and Ben West

The U.S. Department of Justice announced June 28 that an FBI counterintelligence investigation had resulted in the arrest on June 27 of 10 individuals suspected of acting as undeclared agents of a foreign country, in this case, Russia. Eight of the individuals were also accused of money laundering. On June 28, five of the defendants appeared before a federal magistrate in U.S. District Court in Manhattan while three others went before a federal magistrate in Alexandria, Va., and two more went before a U.S. magistrate in Boston. An 11th person named in the criminal complaint was arrested in Cyprus on June 29, posted bail and is currently at large.

The number of arrested suspects in this case makes this counterintelligence investigation one of the biggest in U.S. history. According to the criminal complaint, the FBI had been investigating some of these people for as long as 10 years, recording conversations in their homes, intercepting radio and electronic messages and conducting surveillance on them in and out of the United States. The case suggests that the classic tactics of intelligence gathering and counterintelligence are still being used by Russia and the United States.

Cast of Characters



The following are the 11 individuals detained in the investigation, along with summaries of their alleged activities listed in the criminal complaint:

Christopher Metsos
Claimed to originally be from Canada.Acted as an intermediary between the Russian mission to the United Nations in New York and suspects Richard Murphy, Cynthia Murphy, Michael Zottoli and Patricia Mills.Traveled to and from Canada.Met with Richard Murphy at least four times between February 2001 and April 2005 at a restaurant in New York.Was first surveilled in 2001 in meetings with other suspects.Left the United States on June 17 and was detained in Cyprus on June 29, but appears to have skipped bail.

Richard and Cynthia Murphy
Claimed to be married and to be U.S. citizens.First surveilled by the FBI in 2001 during meetings with Mestos.Also met with the third secretary in the Russian mission to the United Nations.Communicated electronically with Moscow.Richard Murphy's safe-deposit box was searched in 2006 and agents found a birth certificate claiming he was born in Philadelphia; city officials claim there is no such birth certificate on record.Engaged in electronic communications with Moscow.Traveled to Moscow via Italy in February 2010.

Donald Heathfield and Tracey Foley
Claimed to be married and to be natives of Canada who are naturalized U.S. citizens.FBI searched a safe-deposit box listed under their names in January 2001. FBI discovered that Donald Heathfield's identity had been taken from a deceased child by the same name in Canada and found old photos of Foley taken with Soviet film. Engaged in electronic communications with Moscow.Tracey Foley traveled to Moscow via Paris in March 2010.

Michael Zottoli and Patricia Mills
Claimed to be married and to be a U.S. citizen (Zottoli) and a Canadian citizen (Mills).First surveilled in June 2004 during a meeting with Richard Murphy.Engaged in electronic communications with Moscow.

Juan Lazaro and Vicky Pelaez
Claimed to be married and to be a naturalized U.S. citizen born in Peru (Pelaez) and a Peruvian citizen born in Uruguay (Lazaro).First surveilled at a meeting in a public park in an unidentified South American country in January 2000.Evidence against Vicky Pelaez was the first gathered on the 11 suspected operatives.Lazaro appeared to communicate with a diplomat at the Russian Embassy in an unidentified South American country.Engaged in electronic communications with Moscow.

Anna Chapman
First surveillance mentioned was in Manhattan in January 2010.Communicated with a declared diplomat in the Russian mission to the United Nations on Wednesdays.Knowingly accepted a fraudulent passport from an undercover FBI agent whom she believed to be a Russian diplomatic officer June 26, but turned it in to the police the next day shortly before her arrest.

Mikhail Semenko

First surveillance mentioned in the criminal complaint was in June 2010 in Washington.Revealed to an undercover officer that he had received training and instruction from "the center" (a common term for the Moscow headquarters of Russia's Foreign Intelligence Service, or SVR).Accepted a payment of $5,000 and followed orders given by an undercover FBI agent posing as a Russian diplomatic officer to deliver the money to a drop site in Washington.

Their Mission

According to the FBI, some of the alleged "undeclared agents" moved to the United States in the 1990s, while others (such as Anna Chapman) did not arrive until 2009. The FBI says nine of the suspects were provided with fake identities and even fake childhood photos and cover stories (part of what would be called a "legend") in order to establish themselves in the United State under "deep cover." Chapman and Semenko used their own Russian identities (Chapman is divorced and may have taken her surname from her former husband). The true nationalities of the other suspects are unknown, but several passages in the criminal complaint indicate that most of them were originally from Russia. The Russian SVR allegedly provided the suspects with bank accounts, homes, cars and regular payments in order to facilitate "long-term service" inside the United States, where, according to the criminal complaint, the individuals were supposed to "search [for] and develop ties in policymaking circles" in the United States.

The FBI criminal complaint provides evidence that two of the deep-cover couples (Heathfield/Foley and Lazaro/Palaez) and the two short-term cover agents (Semenko and Chapman) were operating without knowledge of each other or in connection with the other two couples and Metsos, who did interact. This suggests that they would not have formed one network, as is being reported, but perhaps discrete networks. The criminal complaint provides evidence indicating that most of the operatives were being run out of the SVR residence at the U.N. mission.

It is unclear exactly how successful the 11 accused individuals were in finding and developing those ties in policymaking circles. The criminal complaint accuses the individuals of sending everything from information on the gold market from a financier in New York (a contact that Moscow apparently found helpful, since it reportedly encouraged further contact with the source) to seeking out potential college graduates headed for jobs at the CIA. The criminal complaint outlines one recorded conversation in which Lazaro told Pelaez that his handlers were not pleased with his reports because he wasn't attributing them properly. Pelaez then advised Lazaro to "put down any politician" (to whom the information could be attributed) in order to appease the handlers, indicating that the alleged operatives did not always practice scrupulous tradecraft in their work. Improperly identifying sources in the field ultimately diminishes the value of the information, since it cannot be adequately assessed without knowing where it came from. If these kinds of shortcuts were normally taken by Pelaez, Lazaro and others, then it would reduce their value to the SVR and the harm that they may have done to the United States. The suspects were allegedly instructed by their handlers in the United States and Russia to not pursue high-level government jobs, since their legends were not strong enough to withstand a significant background investigation. But they allegedly

were encouraged to make contact with high-level government officials, in order to have a finger on the pulse of policymaking in Washington.

Tradecraft

The criminal complaint alleges that the suspects used traditional tradecraft of the clandestine services to communicate with each other and send reports to their handlers. The suspects allegedly transmitted messages to Moscow containing their reports encrypted in "radiograms" (short-burst radio transmissions that appear as Morse code) or written in invisible ink, and met in third countries for payments and briefings. They are also said to have used "brush passes" (the quick and discreet exchange of materials between one person and another) and "flash meets" (seemingly innocuous, brief encounters) to transfer information, equipment and money. The criminal complaint also gives examples of operatives using coded phrases with each other and with their operators to confirm each other's identities.

In addition to the traditional tradecraft described in the criminal complaint, there are also new operational twists. The suspects allegedly used e-mail to set up electronic dead drops to transmit encrypted intelligence reports to Moscow, and several operatives were said to have used steganography (embedding information in seemingly innocuous images) to encrypt messages. Chapman and Semenko allegedly employed private wireless networks hosted by a laptop programmed to communicate only with a specific laptop. The FBI claims to have identified networks (and may have intercepted the messages transmitted) that had been temporarily set up when a suspect was in proximity to a known Russian diplomat. These electronic meetings occurred frequently, according to the FBI, and allowed operatives and their operators to communicate covertly without actually being seen together.

Operations are said to have been run largely out of Russia's U.N. mission in New York, meaning that when face-to-face meetings were required, declared diplomats from the U.N. mission could do the job. According to the criminal complaint, Russian diplomats handed off cash to Christopher Metsos on at least two occasions, and he allegedly distributed it to various other operatives (which provided the grounds for the charge of money laundering). The actual information gathered from the field appears to have gone directly to Russia, according to the complaint.

It is important to note that the accused individuals were not charged with espionage; the charge of acting as an undeclared agent of a foreign state is less serious. The criminal complaint never alleges that any of the 11 individuals received or transmitted classified information. This doesn't mean that the suspects weren't committing espionage. (Investigators will certainly learn more about their activities during interrogation and trial preparation.) According to the criminal complaint, their original guidance from Moscow was to establish deep cover. This means that they would have been tasked with positioning themselves over time in order gain access to valuable information (it is important to point out that "valuable" is not synonymous with "classified") through their established occupations or social lives. This allows agents to gain access to what they want without running unnecessary security risks.

Any intelligence operation must balance operational security with the need to gather intelligence. Too much security and the operative is unable to do anything; but if intelligence

gathering is too aggressive, the handlers risk losing an intelligence asset. If these people were operating in deep cover, the SVR probably invested quite a bit of time and money training and cultivating them, likely well before they arrived in the United States. According to information in the criminal complaint, the suspects were actively meeting with potential sources, sending reports back to Moscow and interacting with declared Russian diplomats in the United States, all the while running the risk of being caught. But they also took security measures, according to the complaint. There is no evidence that they attempted to reach out to people who would have fallen outside their natural professional and social circles, which could have raised suspicions. In many ways, these individuals appear to have acted more like recruiters, seeking out people with access to valuable information, rather than agents trying to gain access to that information themselves. However, all we know now is based on what was released in the criminal complaint. An investigation that lasted this long surely has an abundance of evidence (much of it likely classified) that wasn't included in the complaint.

Counterintelligence

According to authorities, the suspected operatives were under heavy surveillance by U.S. counterintelligence agents for 10 years. Working out of Boston, New York and Washington, the FBI employed its Special Surveillance Group to track suspects in person; place video and audio recorders in their homes and at meeting places to record communications; search their homes and safe-deposit boxes; intercept e-mail and electronic communications; and deploy undercover agents to entrap the suspects.

Counterintelligence operations don't just materialize out of thin air. There has to be a tip or a clue that puts investigators on the trail of a suspected undeclared foreign agent. As suggested by interviews with the suspects' neighbors, none of them displayed unusual behavior that would have tipped the neighbors off. All apparently had deep (but not airtight) legends going back decades that allayed suspicion. The criminal complaint did not suggest how the U.S. government came to suspect these people of reporting back to the SVR in Russia, although we did notice that the beginning of the investigation coincides with the time that a high-level SVR agent stationed at Russia's U.N. mission in New York began passing information to the FBI. Sergei Tretyakov (who told his story in the book by Pete Earley called "Comrade J," an abbreviation of his SVR codename, "Comrade Jean"), passed information to the FBI from the U.N. mission from 1997 to 2000, just before he defected to the United States in October 2000. According to the criminal complaint, seven of the 11 suspects were connected to Russia's U.N. mission, though evidence of those links did not begin to emerge until 2004 (and some as late as 2010). The timing of Tretyakov's cooperation with the U.S. government and the timing of the beginning of this investigation resulting in the arrest of the 11 suspects this week suggests that Tretyakov may have been the original source who tipped off the U.S. government. So far, the evidence is circumstantial — the timing and the location match up — but Tretyakov, as the SVR operative at Russia's U.N. mission, certainly would have been in a position to know about operations involving most of the people arrested June 27.

Why Now?

Nothing in the complaint indicates why, after more than 10 years of investigation, the FBI decided to arrest the 11 suspects June 27. It is not unusual for investigations to be drawn out for years, since much information on tradecraft and intent can be obtained by watching foreign

intelligence agencies operate without knowing they are being watched. Extended surveillance can also reveal additional contacts and build a stronger case. As long as the suspects aren't posing an immediate risk to national security (and judging by the criminal complaint, these 11 suspects were not), there is little reason for the authorities to show their hand and conclude a fruitful counterintelligence operation.

It has been suggested that some of the suspects were a flight risk, so agents arrested all of them in order to prevent them from escaping the United States. Metsos left the United States on June 17 and was arrested in Cyprus on June 29, however, his whereabouts are currently unknown, as he has not reported back to Cypriot authorities after posting bail. A number of the suspects left and came back to the United States numerous times, and investigators appear not to have been concerned about these past comings and goings. It isn't clear why they would have been concerned about someone leaving at this point.

The timing of the arrests so soon after U.S. President Barack Obama's June 25 meeting with Russian President Dmitri Medvedev also raises questions about political motivations. Medvedev was in Washington to talk with Obama in an attempt to improve relations between the two countries on the day the FBI officially filed the criminal complaint. The revelation of a network of undeclared foreign agents operating in the United States would ordinarily have a negative effect on relations between the United States and the foreign country in question. In this case, though, officials from both countries made public statements saying they hoped the arrests would not damage ties, and neither side appears to be trying to leverage the incident. Indeed, if there were political motivations behind the timing of the arrests, they remain a mystery.

Whatever the motivations, now that the FBI has these suspects in custody it will be able to interrogate them and probably gather even more information on the operation. The charges for now don't include espionage, but the FBI could very well be withholding this charge in order to provide an incentive for the suspects to plea bargain. We expect considerably more information on this unprecedented case to come out in the following weeks and months, revealing much about Russian clandestine operations and their targets in the United States.

(c) Stratfor http://www.stratfor.com/ Reproduced with permission. All rights reserved.