Spy suspects allegedly used regular consumer tech

July 2 2010, By PETER SVENSSON , AP Technology Writer

This undated image taken from the Russian social networking website "Odnoklassniki", or Classmates, shows a woman journalists have identified as Anna Chapman, who appeared at a hearing Monday, June 28, 2010 in New York federal court. Chapman, along with 10 others, was arrested on charges of conspiracy to act as an agent of a foreign government without notifying the U.S. attorney general. (AP Photo)

Before James Bond heads out on a mission, he has to stop in Q's laboratory for custom-made gadgets such as an exploding watch. Life wasn't so dashing for the suspected Russian spies arrested this week: They allegedly relied heavily on off-the-shelf consumer electronics.

"In the old days, they'd have special KGB-type equipment. Now they use

normal computers, normal laptops," said Sujeet Shenoi, professor of computer science at the University of Tulsa and a frequent consultant to the FBI. "Technology is so powerful now that you don't have to have special-purpose equipment anymore."

According to the FBI's complaints that sought the arrest of the 11 suspects, the array of tools included laptops, flash memory cards and at least one prepaid cell phone. The suspects are accused of backing that up with old-fashioned spy technology such as short-wave radios, invisible ink, and a classic, manual encryption method known as a "one-time pad."

Short-wave radios were once relatively common in homes. Today, they're a bit of a giveaway if the FBI already suspects you're a spy. Not so with laptops, cell phones or flash drives. But that doesn't mean spies can feel safe. The way the Russian suspects used these gadgets was revealing to FBI agents who followed them for years.

The use of "spy-fi" is a case in point.

The FBI said that one of the suspects, Anna Chapman, would go to a coffee shop in Manhattan on Wednesdays and set up her laptop. A little while later, a minivan the FBI knew was used by a Russian official would drive by. To the naked eye, there was no contact between them.

But the FBI said it figured out that Chapman's computer was set to link wirelessly to a laptop in the minivan, using a standard, built-in Wi-Fi chip. In the short time the computers were close, they could transfer encrypted files between each other.

The agency figured this out with commercial Wi-Fi analysis software, not with something from Q's lab.

Glenn Fleishman, editor of the Wi-Fi Net News blog, said that from a

technical standpoint, the Wi-Fi link appeared to be fairly amateurish and laughably easy to sniff out. He pointed out that there's at least one other commercially available technology for short-range transmissions, known as ultra-wideband radio, that would likely have been impossible for the FBI to pick up.

On the contrary, Keith Melton, who co-authored the book "Spycraft" with the former director of the CIA's Office of Technical Service, said the use of Wi-Fi could have been "very smart" because no data passed through the Internet. The connection would have been impossible to trace - if the FBI hadn't been smart and dogged enough to have Wi-Fi analysis equipment in place at the right time.

Melton said the technique is reminiscent of a precursor to today's BlackBerry, developed by the CIA in the 1970s to give its spies in Russia some way to pass messages unseen to receivers close by. The downfall was that being caught with the equipment could lead to a death sentence.

In another example of an everyday item allegedly being used for secret communications, the FBI said Chapman bought a cell phone last Saturday under a fake name. This was probably a "prepaid" phone, which doesn't come with a contract. Because there's no long-term commitment from the buyer, the sellers don't check the IDs of the buyers. That means law enforcement don't know which numbers suspects are using, making wiretapping very difficult.

Not surprisingly, prepaid phones used once or twice and then thrown away are a favorite tool of criminals and terrorists. Faisal Shahzad, who admitted to trying to bomb New York's Times Square on May 1, used a prepaid phone. A proposed Senate bill would require buyers to show ID.

In the FBI's documents, there is no mention of the agency intercepting a call from Chapman's disposable cell phone. She bought it just after

meeting an undercover FBI agent posing as a Russian official. He told her to meet another spy the next day, but she didn't show up. Presumably, she had been suspicious of the "Russian," called her handler on the cell phone and was warned to stay away.

But again, her behavior was a giveaway, according to the FBI. She bought the phone in a Brooklyn store, then immediately threw away the bag containing the charger and the customer agreement. The FBI retrieved the bag, and found she'd given her name as "Irine Kutsov," living on "99 Fake Street."

Another person charged in the case, Richard Murphy, received a bag with cash and a memory card from a Russian official at a White Plains, N.Y., train station in 2009, according to the FBI. That would be a classic "brush pass," where conspirators walk by each other and quickly pass an item from one to the other. The FBI said it caught this exchange on surveillance video. It was only later that the agency figured out, by eavesdropping, that the bag contained a memory card.

For more than a century, spies have employed methods to miniaturize documents, usually by photographic means that require special equipment. Flash memory chips, the kind used in cameras, phones and USB drives, make it child's play to stuff thousands of documents in a tiny, concealable area.

It's surprising, then, that the spy ring is also alleged to have used one of the oldest ways to conceal writing: invisible ink. Its height of popularity in intelligence circles was World War I, Melton said. Now, it's mainly found in the toy aisle, but that doesn't mean it's obsolete.

"The beauty of it is that no one is looking for it. It's so old that it's been forgotten," Melton said.

Indeed, the FBI's complaint doesn't mention that it found any documents written in invisible ink. It just says that it overheard suspect Juan Lazaro telling his wife, Vicky Pelaez, that he was going to write something in "invisible" that she was supposed to pass along to someone on a trip to South America.

A modern update on invisible ink is digital steganography. Messages can be hidden in images, songs or other files, then uploaded to public sites on the Internet. No one's the wiser without knowing which images to look for, and how they are encoded. In three homes belonging to suspects, the FBI found disks that it suspects were used for steganography. Agents also said they found a password written on a piece of paper in the Hoboken, N.J., home of Richard and Cynthia Murphy during a 2005 search. (The couple later moved to nearby Montclair.) This allowed agents to decode more than a hundred messages between the Murphys and Moscow, the FBI said.

Although the FBI used high-tech techniques such as surveillance cameras and Wi-Fi sniffing, it got its biggest payoffs from old-fashioned, risky and expensive methods like tailing and house searches. You can use all the technology you want to hide your tracks, but if you leave the password to your secrets on your desk, old-fashioned sleuthing can still beat high-tech.