Long before new hacks, US worried by Russian spying efforts

March 17 2017, by Eric Tucker

In this May 25, 2016, courtroom drawing, defendant Evgeny Buryakov, left, stands with his attorney Scott Hershman during sentencing on espionage charges in New York. U.S. intelligence agencies have been concerned for years about Russian efforts to infiltrate American society and government. Those concerns came long before Russian intelligence agencies stood accused of interfering in the U.S. presidential election and of orchestrating a massive Yahoo data breach. It's not surprising that once the public understands the capabilities and motives of Russian intelligence "that there's a great deal of concern about their ability to gather intelligence and use it to influence real-world events," said Adam Fee,

who was lead prosecutor in the 2015 prosecution of Evgeny Buryakov, who posed as a banker in New York while spying on the U.S. for the Russian Federation.(AP Photo/Elizabeth Williams, file)

Years before Russian intelligence agencies stood accused of interfering in the U.S. presidential election and of orchestrating a massive Yahoo data breach, there was lingerie model Anna Chapman and her band of "Illegals"—Russian spies who assumed false identities and lived as deep-cover agents in middle-class America.

The busting-up of that spy ring, along with the arrest two years ago of a Russian spy who posed as a Manhattan banker and this week's announcement of an indictment of Russian agents in the Yahoo email hack, underscore long-running efforts by the American authorities to closely monitor and occasionally interrupt the Kremlin's intelligence-gathering operations.

Though allegations of meddling in the political process represent a stunning new flare-up in relations between the two countries, U.S. intelligence agencies for years have been concerned by Russian efforts to infiltrate American society and government.

"What we have seen as far as the arrests is really only scratching the surface of the real Russian activity here," said Scott Stewart, vice president of tactical analysis at the Texas-based Stratfor intelligence firm.

Many counterintelligence investigations can last for years without resulting in criminal charges, preventing the public from having a complete grasp of evidence collected or tactics that are used.

But a few sensational Justice Department prosecutions in the last decade have brought to light Russian efforts to recruit university students, gather information on the stock market and on sanctions, sway public opinion and cultivate well-placed contacts. And recent hacking allegations make clear that old-fashioned spying techniques have now been augmented by cyber expertise that can in some cases accomplish similar goals.

"They want to understand how the White House is going to work, and how Washington will respond to what Russians are doing in Europe and the Middle East," said Steven Pifer, a senior fellow at the Brookings Institution and a former foreign service officer focused on Russia.

It's not surprising that once the public understands the capabilities and motives of Russian intelligence "that there's a great deal of concern about their ability to gather intelligence and use it to influence real-world events," said Adam Fee, who helped handle the 2015 prosecution of Evgeny Buryakov, who posed as a banker in New York while spying on the U.S. for the Russian Federation.

"It's interesting to see an area you worked on splash in the forefront of the national consciousness," Fee said.

Public interest in counterintelligence operations spiked with the U.S. assessment in January that Russian intelligence agencies were responsible for the hacking of Democratic email accounts and for sharing that information with WikiLeaks, the anti-secrecy website, with the goal of aiding the Trump campaign.

That interference remains under federal investigation, but some experts see parallels between those cyberattacks and prior Russian espionage efforts.

Alarmingly to American authorities, Russian hackers engaged in more

conventional crimes, such as stealing credit and debit card account information, have in some cases piggybacked off Russian intelligence services. The Justice Department this week announced charges against two Russian intelligence agents and two hired hackers. The four were accused in a 2014 breach of at least 500 million Yahoo user accounts.

"I view cyber as merely being a new tool of espionage to pursue the same goals of espionage—whether that's recruiting, stealing information, it's basically the same things they've always done," Stewart said. "It's just a new tool to accomplish those tasks."

Probably the most notable prosecution is the 2010 case of "The Illegals"—a ring of Russian sleeper spies who burrowed into workaday America instead of more customary positions inside Russian embassies and military missions.

Tasked with developing contacts with government policymakers, the Russians took civilian positions in cities throughout the country and in some cases lived as husband and wife.

A long-running FBI investigation called "Operation Ghost Stories" revealed how the secret agents relied on specially coded radio transmissions, invisible ink and furtive cash drops as they patiently worked to develop sources and send information back to Russia.

Once captured, 10 spies charged with acting as foreign agents were swapped for four Russians who'd been imprisoned for spying for the West. An 11th suspect accused of delivering money and equipment to the secret agents was freed by a court in Cyprus and later vanished.

Chapman herself became a model and corporate spokeswoman upon her return to Russia, the saga said to have been an inspiration for the hit FX show "The Americans."

The motive was different than last year's election hack, said Glen Kopp, a prosecutor in the case.

What's similar, he added, is "the obsession with seeing the world as us versus them."

More recently, Buryakov was sentenced to two and a half years in prison for his spying efforts, which in addition to working to gain information about the New York Stock Exchange, also included an attempt to shape political opinion.

He admitted to working to sway union opinion about a Canadian company's planned deal to build aircraft in Russia—efforts known among experts as "active measures." That political engagement in some ways resembles what U.S. officials say was a Russian effort to use an email hack to politically harm Democratic presidential candidate Hillary Clinton.

"What I see in the cyberattacks last year, it's a modernized version of those active measures," Pifer said.

Counterintelligence concerns faded in the post-Cold War era as the Soviet Union splintered and as counterterrorism fears from the Middle East rose to the forefront. But more recent events have brought renewed focus on Russia, Pifer said.

The cyber realm, he said, "creates possibilities for the Russians to do things that they couldn't do before."