

'Big hunt' for Russian hackers, but no obvious election link

July 28 2017, by Howard Amos, Raphael Satter And Aritz Parra



In this Wednesday, July 26, 2017 file photo, alleged hacker Pyotr Levashov, speaks during a hearing to consider his extradition to the United States, at the National Court in Madrid. The U.S. has orchestrated the arrest of five alleged Russian cybercriminals across Europe in the past nine months. The operations come at a fraught moment in relations between Russia and the U.S., where politicians are grappling with the allegation that Kremlin hackers intervened in the 2016 election. (Luca Piergiovanni/Pool Photo via AP, File)

Pyotr Levashov appeared to be just another comfortable member of Russia's rising middle-class—an IT entrepreneur with a taste for upmarket restaurants, Thai massages and foreign travel.

Then police raided his vacation rental in Barcelona, marching him out in handcuffs to face charges of being one of the world's most notorious spam lords.

Levashov's April 7 arrest was one in a series of American-initiated operations over the past year to seize alleged Russian cybercriminals outside their homeland, which has no extradition agreement with the United States.

They come at a fraught moment in relations between Moscow and Washington, where politicians are grappling with the allegation that Kremlin hackers intervened in the U.S. election to help President Donald Trump. Through their lawyers, several defendants have suggested their arrests are linked to the election turmoil. Experts say that's possible, though an Associated Press review of the cases found no firm evidence to back the claim.

"There is a big hunt underway," said Andrei Soldatov, an expert on the Russian security services and co-author of "Red Web," a book about Russian attempts to control the internet. He said the recent burst of arrests made it look like the United States was "trying to understand what's going on with a very complicated world of Russian hacking and a very complicated relationship between Russian hackers and Russian secret services."



In this Thursday, July 20, 2017 file photo, Russian computer programmer Stanislav Lisov attends a court hearing at the Spanish National Court in Madrid, on extradition request to the U.S. for alleged crimes related to the 'NeverQuest' malicious software, which syphoned 855,000 U.S. dollars (743,000 euros) from bank clients in the country. The U.S. has orchestrated the arrest of five alleged Russian cybercriminals across Europe in the past nine months. The operations come at a fraught moment in relations between Russia and the U.S., where politicians are grappling with the allegation that Kremlin hackers intervened in the 2016 election. (Luca Piergiovanni/Pool via AP, file)

But Soldatov didn't rule out another possible explanation: The imprisoned Russians may be falsely tying their arrests to Trump's election in a bid to sow confusion and politicize their cases.

"It's a very big question," he said.

"HE GOT TO EVERY MAILBOX THERE EVER WAS"

At least five Russians have been picked up in Europe as part of U.S. cybercrime prosecutions in the last nine months.



In this Thursday, July 20, 2017 file photo, Russian computer programmer Stanislav Lisov attends a court hearing at the Spanish National Court in Madrid, on extradition request to the U.S. for alleged crimes related to the 'NeverQuest' malicious software, which syphoned 855,000 U.S. dollars (743,000 euros) from bank clients in the country. The U.S. has orchestrated the arrest of five alleged Russian cybercriminals across Europe in the past nine months. The operations come at a fraught moment in relations between Russia and the U.S., where politicians are grappling with the allegation that Kremlin hackers intervened in the 2016 election. (Luca Piergiovanni/Pool via AP, file)

Evgeny Nikulin, 29, was arrested in a restaurant in Prague in October, accused of hacking into LinkedIn and Dropbox around the time that tens of millions of users there were compromised; Stanislav Lisov, 31, the alleged developer of the NeverQuest financial data-stealing software, was detained at Barcelona's airport during his honeymoon in January; and Yury Martyshev, 35, accused of helping run a service that let cybercriminals test-drive their malicious software, was recently extradited to the U.S. after being pulled off a train at the Russia-Latvia border in April. On Tuesday, Alexander Vinnik, 38, was arrested at his hotel in Greece on charges of running a money laundering ring for hackers that processed billions of dollars in digital currency.

Levashov, who made his first court appearance in Madrid for a brief hearing Wednesday, is easily the best known of the five. The 36-year-old is charged with fraud and unauthorized interception of electronic communications, but his spamming career is said to stretch back to the turn of the millennium, when the business of stuffing email inboxes full of pitches for cut-price pills and penny stocks was still largely unregulated.

Court documents trace how Levashov, using the alias Peter Severa, teamed up in 2005 with Alan Ralsky, an American bulk email baron once dubbed the "King of Spam."

Ralsky described the Russian as a master of his trade.

"He made me look like an amateur," Ralsky said in a recent interview. "He got to every mailbox there ever was."



In this screen grab taken from video on Thursday, July 20, 2017, Russian computer programmer Stanislav Lisov attends a court hearing at the Spanish National Court in Madrid, on extradition request to the U.S. for alleged crimes related to the 'NeverQuest' malicious software, which syphoned 855,000 U.S. dollars (743,000 euros) from bank clients in the country. The U.S. has orchestrated the arrest of five alleged Russian cybercriminals across Europe in the past nine months. The operations come at a fraught moment in relations between Russia and the U.S., where politicians are grappling with the allegation that Kremlin hackers intervened in the 2016 election. (AP)

Spammers can make a lot renting out their services to those peddling grey market pharmaceuticals or pornography. Ralsky said Levashov was pulling in "more money than you could shake a stick at" and traveled widely, saying he remembered getting vacation snaps of the Russian enjoying himself at a fishing cabin in Finland or the famously expensive Burj Al Arab hotel in Dubai.

By then, Levashov had crossed American law enforcement's radar.

In 2007, he was indicted under his Severa alias as part of the case where Ralsky and several associates pleaded guilty to charges including wire fraud and mail fraud. Two years later, American authorities identified Levashov by name as the operator of the "Storm" botnet, a massive network of compromised, spam-spewing computers.

In the Russian hacker community, Levashov's profile was rising too. In online forums, he promoted the idea of collaborating with Russia's spy services, according to Soldatov, the Russian intelligence expert, who said Levashov spearheaded an effort to knock out websites linked to Islamist insurgencies in southern Russia.

"He was the first Russian hacker known to have brought the FSB into the circle of the Russian hacking community," Soldatov said, referring to Russia's domestic spy agency. "His idea was to make it more patriotic."



In this Thursday, Nov. 14, 2013 file photo, Andrei Soldatov, an expert on the Russian security services and co-author of "Red Web", speaks to The Associated Press during an interview in Moscow, Russia. The U.S. has orchestrated the arrest of five alleged Russian cybercriminals across Europe in the past nine months. The operations come at a fraught moment in relations between Russia and the U.S., where politicians are grappling with the allegation that Kremlin hackers intervened in the 2016 election. (AP Photo/Alexander Zemlianichenko, File)

When Levashov was finally caught, his wife Maria drew international attention when she was quoted as saying the arrest was "linked to Trump's win." But in a conversation with The Associated Press in Madrid on Wednesday, she pulled back from those comments.

"I think there are some political reasons in this case, but I'm not sure," she said. "I don't have any evidence."

Levashov's lawyer, Margarita Repina, offered a similar qualification to her assertion that U.S. officials were "just taking hackers with any excuse to see if any of them admits involvement in the Trump issue."

"This is just an opinion," she said. "We have no evidence."

Legal documents suggest the latest effort to catch Levashov began well before the election. In a sworn declaration, FBI Agent Elliott Petersen said he began tracking Kelihos, the latest incarnation of Levashov's alleged spam botnet operation, more than two years ago.



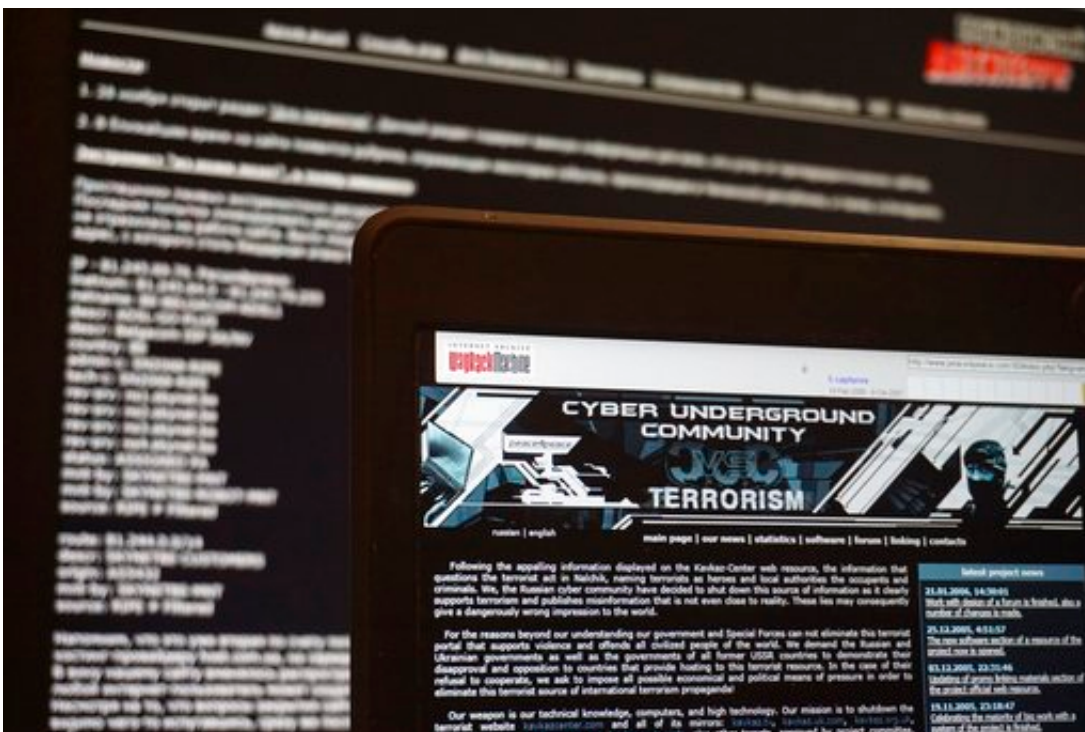
In this photo taken on Monday, July 24, 2017, a car passes the building of the Federal Security Service (FSB, Soviet KGB successor) in Lubyanskaya Square in Moscow, Russia. The U.S. has orchestrated the arrest of five alleged Russian cybercriminals across Europe in the past nine months. The operations come at a fraught moment in relations between Russia and the U.S., where politicians are grappling with the allegation that Kremlin hackers intervened in the 2016 election. (AP Photo/Alexander Zemlianichenko)

The former spam king was also skeptical that Levashov's arrest was linked to the vote.

"They've been after him for a long time," Ralsky said.

"THERE IS A CHESS GAME THAT ESCAPES US"

Levashov wouldn't be alone in floating thinly supported claims that his prosecution is related to the 2016 election. Lisov was also arrested in Barcelona and spent a month as Levashov's cellmate in Madrid. His attorney, Juan Manuel Arroyo, told an extradition hearing last week that there was "a game of chess that escapes us" between Moscow and Washington. Arroyo suggested that the American extradition request was "not normal."



In this July 24, 2017 photo, archived versions of two Russian anti-terrorism websites on a computer screen are photographed, in Paris. The now-defunct websites were the brainchild of alleged hacker Pyotr Levashov, according to Andrei Soldatov, an expert on the Russian security services. The U.S. has orchestrated the arrest of five alleged Russian cybercriminals across Europe in the past nine months. The operations come at a fraught moment in relations between Russia and the U.S., where politicians are grappling with the allegation that Kremlin hackers intervened in the 2016 election. (AP Photo/Raphael Satter)

A Spanish court document seen by AP suggests Lisov has been sought by the U.S. since Aug. 5, 2015, undermining the idea of an election link. Arroyo says he disputes the existence of any such request.

Nikulin, who is the subject of a conflicting extradition request from Russia, has been the most explicit. He told a judge in Prague that he was twice taken out of prison and offered a pardon, U.S. citizenship and refuge for his parents if he confessed to having "hacked the Democratic Party" on the Russian government's orders, an apparent reference to the embarrassing leak of Democratic National Committee emails in the heat of the U.S. race.

Nikulin said he rejected the offer, and his lawyer Vladimir Makeev later wrote a rambling letter warning Trump that the bureau was railroading Nikulin to undermine his presidency.

In an interview at his office in Moscow, Makeev said his client was being pressured by "certain unscrupulous representatives of the FBI that wish to have an impeachment carried out on president of the United States."

There's little evidence for the inflammatory claim.



In this photo taken on Monday, July 24, 2017, people walk along Nevsky prospect, the central avenue in St.Petersburg, Russia. The U.S. has orchestrated the arrest of five alleged Russian cybercriminals across Europe in the past nine months. The operations come at a fraught moment in relations between Russia and the U.S., where politicians are grappling with the allegation that Kremlin hackers intervened in the 2016 election. (AP Photo/Yevgeny Kurskov)

Nikulin was in fact questioned in the presence of an FBI agent from the bureau's San Francisco office, according to a Russian-language legal document which Makeev shared with AP.

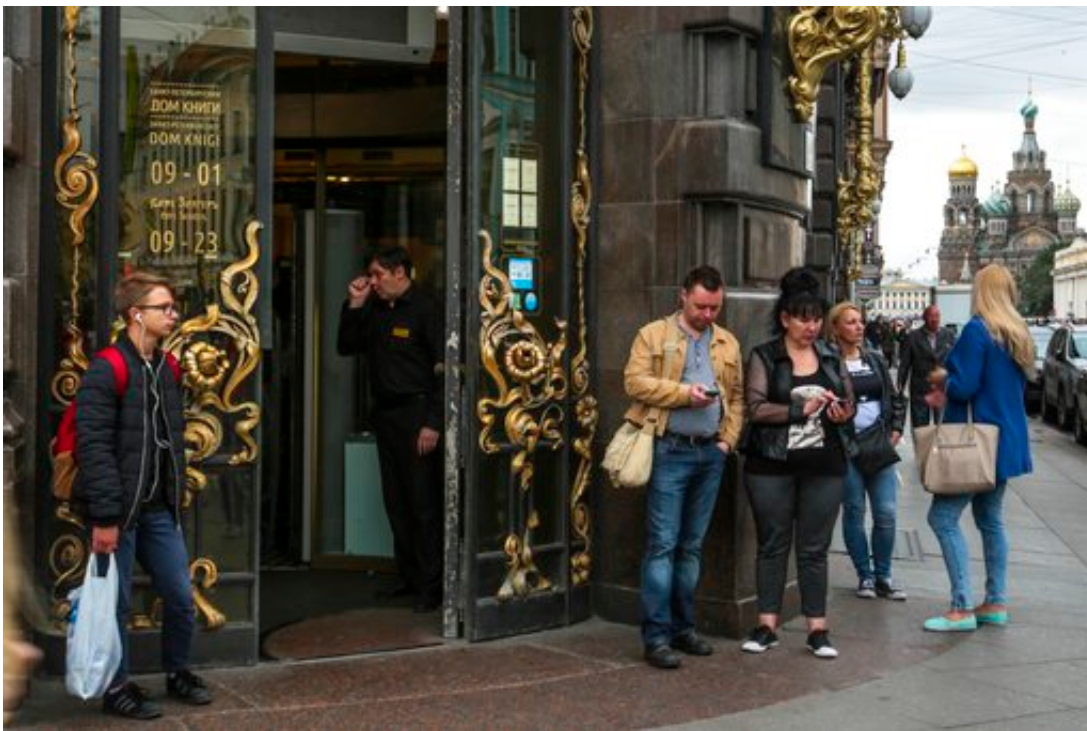
But there's no indication the agent—who was one of 10 officials, translators and defense lawyers listed as being present at the interrogation—ever discussed the election or made Nikulin an offer, much less of citizenship. The FBI would not make the agent available for an interview but a law enforcement official said no such deal was ever discussed. The official was not authorized to discuss the matter publicly

and spoke on condition of anonymity.

Martyshev's attorney did not return messages seeking comment, but the Russian pleaded not guilty to all charges at a court hearing in Alexandria earlier this month.

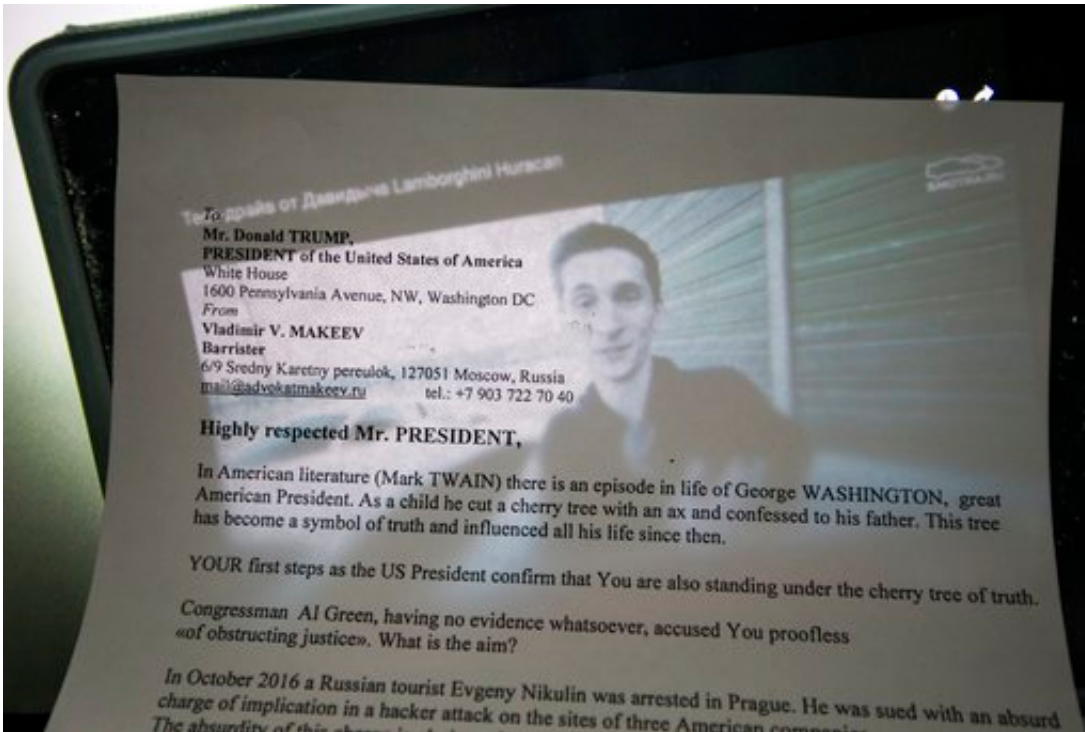
Levashov may soon be joining him in America. His extradition to the United States seems a foregone conclusion, according to Repina, his attorney. She argued that would hardly be fair given that, in Russia, the spamming he's alleged to have carried out may not even be a crime.

"In his country, Levashov has legal businesses and a family that he needs to provide for," she said. "He is a patriot."

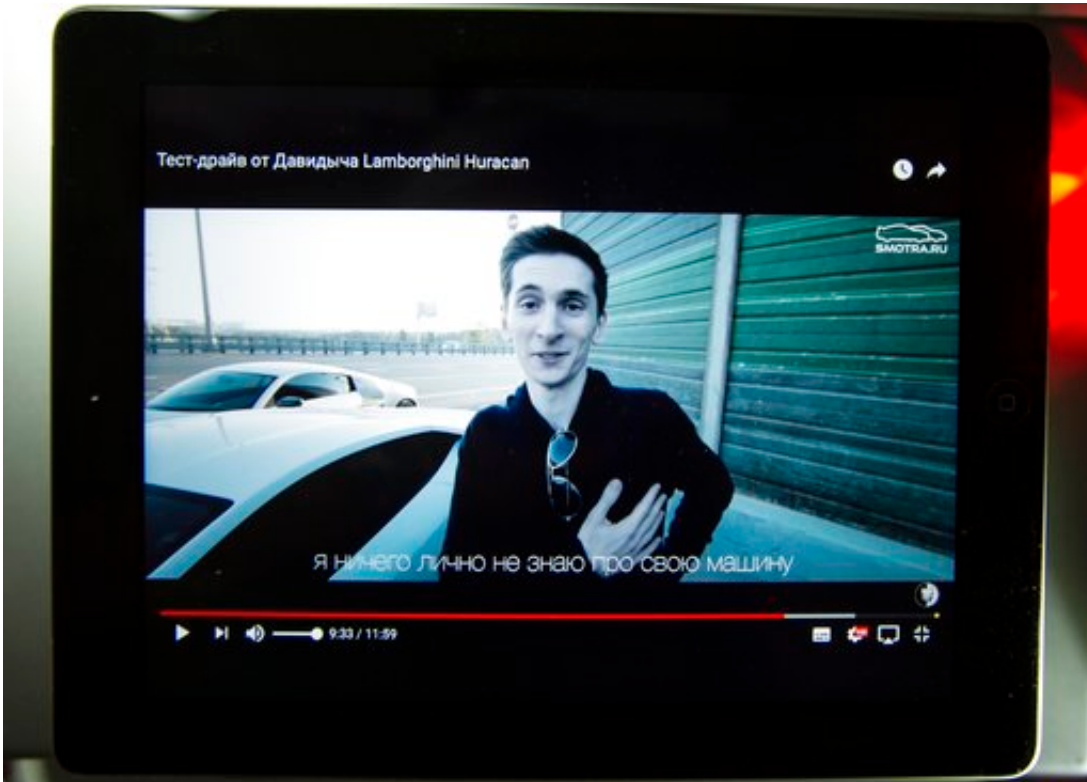


In this photo, taken on Monday, July 24, 2017, people look at their cell phones while standing at a corner of Nevsky prospect, the central avenue in St.Petersburg, Russia. The U.S. has orchestrated the arrest of five alleged Russian cybercriminals across Europe in the past nine months. The operations come at a fraught moment in relations between Russia and the U.S., where

politicians are grappling with the allegation that Kremlin hackers intervened in the 2016 election. (AP Photo/Yevgeny Kurskov)



In this Tuesday, July 25, 2017 photo, a copy of the letter written by Russian lawyer Vladimir Makeev to U.S. President Donald Trump lies on a computer screen showing archive Youtube footage dated Monday, Aug. 2, 2015 featuring suspected hacker Yevgeny Nikulin after a Lamborghini Huracan race outside Moscow, Russia. The U.S. has orchestrated the arrest of five alleged Russian cybercriminals across Europe in the past nine months. The operations come at a fraught moment in relations between Russia and the U.S., where politicians are grappling with the allegation that Kremlin hackers intervened in the 2016 election. (AP Photo/Alexander Zemlianichenko)



In this Tuesday, July 25, 2017 photo, a tablet shows archive Youtube footage dated Monday, Aug. 2, 2015 featuring Yevgeny Nikulin after a Lamborghini Huracan race outside Moscow, Russia. The U.S. has orchestrated the arrest of five alleged Russian cybercriminals across Europe in the past nine months. The operations come at a fraught moment in relations between Russia and the U.S., where politicians are grappling with the allegation that Kremlin hackers intervened in the 2016 election. (AP Photo/Alexander Zemlianichenko)



In this photo taken on Monday, July 24, 2017, Vladimir Makeev, attorney to alleged hacker Yevgeny Nikulin and a member of Moscow City Bar Association speaks to the Associated Press in Moscow, Russia. The U.S. has orchestrated the arrest of five alleged Russian cybercriminals across Europe in the past nine months. The operations come at a fraught moment in relations between Russia and the U.S., where politicians are grappling with the allegation that Kremlin hackers intervened in the 2016 election. (AP Photo/Ahmad Katib)



In this Wednesday, Aug. 19, 2015 file photo, the J. Edgar Hoover Building, The Federal Bureau of Investigation headquarters, in Washington. The U.S. has orchestrated the arrest of five alleged Russian cybercriminals across Europe in the past nine months. The operations come at a fraught moment in relations between Russia and the U.S., where politicians are grappling with the allegation that Kremlin hackers intervened in the 2016 election. (AP Photo/Andrew Harnik, File)



In this file photo taken on Thursday, March 24, 2016, the moon rises over Nevsky prospect, central avenue in St.Petersburg, Russia. The U.S. has orchestrated the arrest of five alleged Russian cybercriminals across Europe in the past nine months. The operations come at a fraught moment in relations between Russia and the U.S., where politicians are grappling with the allegation that Kremlin hackers intervened in the 2016 election. (AP Photo/Dmitri Lovetsky, file)

© 2017 The Associated Press. All rights reserved.

Citation: 'Big hunt' for Russian hackers, but no obvious election link (2017, July 28) retrieved 28 May 2023 from <https://phys.org/news/2017-07-big-russian-hackers-obvious-election.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.