The New York Times | https://nyti.ms/2jFJaoO

EUROPE

Russians Charged With Treason Worked in Office Linked to Election Hacking

By SCOTT SHANE, DAVID E. SANGER and ANDREW E. KRAMER JAN. 27, 2017

WASHINGTON — Ever since American intelligence agencies accused Russia of trying to influence the American election, there have been questions about the proof they had to support the accusation.

But the news from Moscow may explain how the agencies could be so certain that it was the Russians who hacked the email of Hillary Clinton's campaign and the Democratic National Committee. Two Russian intelligence officers who worked on cyberoperations and a Russian computer security expert have been arrested and charged with treason for providing information to the United States, according to multiple Russian news reports.

As in most espionage cases, the details made public so far are incomplete, and some rumors in Moscow suggest that those arrested may be scapegoats in an internal power struggle over the hacking. Russian media reports link the charges to the disclosure of the Russian role in attacking state election boards, including the scanning of voter rolls in Arizona and Illinois, and do not mention the parallel attacks on the D.N.C. and the email of John Podesta, Mrs. Clinton's campaign chairman.

But one current and one former United States official, speaking about the classified recruitments on condition of anonymity, confirmed that human sources in Russia did play a crucial role in proving who was responsible for the hacking.

The former official said the agencies were initially reluctant to disclose their certainty about the Russian role for fear of setting off a mole hunt in Moscow.

The public disclosure of the arrests, and the severity of the treason charge, come at a delicate moment for President Trump.

He has been loath to accept the intelligence agencies' conclusion that Russia tried to help him win, which he sees as part of an effort to delegitimize his election.

The Russian role will loom over the conversation with Mr. Putin that Mr. Trump is scheduled to have on Saturday since it was the Russian president who James R. Clapper Jr., the former director of national intelligence, told Congress ordered the hacking and leaking.

One topic of the phone conversation is likely to be the sanctions that the Obama administration imposed on Russia, including ones that were imposed in December in retaliation for the election hacking.

For months, Mr. Trump rejected the finding that Russia was behind the hacking, accusing the intelligence agencies of incompetence and political bias. After a classified briefing in New York a month ago, he grudgingly accepted that Russia had a role, while playing down the hacking by noting that China and other countries also hacked the United States.

Steven L. Hall, a former C.I.A. head of Russian operations, said it was "very tempting and certainly reasonable" to connect the arrests to the American intelligence findings.

But he added a cautionary note: "The rule of law doesn't apply in Russia, and they manipulate the law to do whatever they want to do. So what they call treason may not be what we call treason."

Mark Galeotti, a Russia expert at the Institute of International Relations in Prague, noted that the intelligence agencies' report on the election attack found with "high confidence" that Russia had carried out the election attack, which involved fake news stories and propaganda as well as the hacks and leaks.

"It was always pretty obvious that they had more than just the computer evidence," Mr. Galeotti said. "The arrests are a big deal."

The arrests, according to reports by the Russian newspaper Kommersant and Novaya Gazeta, among others, were made in early December and amounted to a purge of the cyberwing of the F.S.B., the main Russian intelligence and security agency.

Those arrested by the agency's internal affairs bureau included Sergei Mikhailov, a deputy director of the Center for Information Security, the agency's computer security arm, and Ruslan Stoyanov, a senior researcher at a prominent Russian computer security company, Kaspersky Lab.

A nationalist publication, Tsargrad, and RBC, a respected business newspaper, identified on Friday a third suspect, Dmitry Dokuchayev.

Described as a former hacker who used the online pseudonym Forb, Mr. Dokuchayev had agreed to work for the F.S.B. to avoid prosecution for credit card fraud, a rampant crime in Russia.

RBC also reported an alternative theory about the counterintelligence investigation, saying it may have begun after a hacking group, Shaltai Boltai, or Humpty Dumpty, stole the emails of a senior Russian official a year ago. By this account, the investigation of email theft led to Mr. Dokuchayev.

Both Novaya Gazeta, an outlet for the liberal opposition, and the hard-line nationalist Tsargrad reported that the F.S.B. added a theatrical touch to the arrest of Mr. Mikhailov.

Agents arresting the suspected spy placed a bag over his head in the midst of a congress of senior intelligence agency officers in Moscow and led him from the room, the two publications reported.

"The arrest was certainly colorful," Tsargrad's report said. "Mikhailov was led from the congress of F.S.B. colleagues with a bag on his head."

The virtually simultaneous appearance of at least four prominent news reports on the arrests, citing numerous anonymous sources, suggested that the normally opaque Russian government wanted the information out, though it was unclear why.

A prominent Russian criminal defense lawyer on Friday confirmed that the authorities in Moscow were prosecuting at least one computer security expert for treason.

The confirmation by the Russian lawyer, Ivan Pavlov, in written answers to questions from The New York Times, came the closest so far to a formal acknowledgment of the arrests.

Mr. Pavlov declined to identify his client or elaborate on the reason for the indictment for "betraying the state," punishable by up to 20 years in a penal colony.

The report in Novaya Gazeta said the F.S.B. began the internal investigation after news media reports that a United States cybersecurity company, ThreatConnect, had linked the election hacking to a Siberian server company.

That company, King Servers, was otherwise used largely for criminal and marginal computer activities, such as distributing pornography and counterfeit goods, by the admission of its owner.

The report said the investigation led to Mr. Mikhailov, a senior officer involved in tracking criminal computer activity in Russia.

The hints suggested that the Russian government may be signaling that it might, however indirectly through a treason trial, reveal details of election hacking, which would have the potential to damage Mr. Trump's administration.

But there is another explanation, if something of a counterintuitive one: Documenting a Russian role in the electoral hacks could also serve Moscow's foreign policy interests by underscoring the extent and power of the Kremlin's reach in the world.

Cyberattacks, mixed with information warfare, have proven a vital tool for the Kremlin, used in Europe and the Baltics before the attack on the United States election. And now, there is evidence of new meddling in France and Germany, both of which have major elections this year.

The Russian Foreign Ministry has denied any role in the hacking.

ThreatConnect, the cybersecurity company that released the report about King Servers, said its analysis was based on information published by the F.B.I.

ThreatConnect declined to comment after the arrests in Moscow.

Scott Shane and David E. Sanger reported from Washington, and Andrew E. Kramer from Moscow. Adam Goldman contributed reporting from Washington.

A version of this article appears in print on January 28, 2017, on Page A1 of the New York edition with the headline: Russian Arrests Pose Tantalizing Clues in Hacking.
