Mystery of NSA leak lingers as stolen document case winds up

July 7 2019, by Tami Abdollah And Eric Tucker

In this June 6, 2013 file photo, the sign outside the National Security Administration (NSA) campus in Fort Meade, Md. A high-profile raid at the home of an NSA contractor seemed to be linked to the devastating leak of U.S. government hacking tools. Three years later, the case is being resolved but whoever was behind the leak of the hacking tools remains a mystery with significant national security implications. (AP Photo/Patrick Semansky, File)

Federal agents descended on the suburban Maryland house with the flash and bang of a stun grenade, blocked off the street and spent hours questioning the homeowner about a theft of government documents that prosecutors would later describe as "breathtaking" in its scale.

The suspect, Harold Martin, was a contractor for the National Security Agency. His arrest followed news of a devastating disclosure of government hacking tools by a mysterious internet group calling itself the Shadow Brokers . It seemed to some that the United States might have found another Edward Snowden, who also had been a contractor for the agency.

"You're a bad man. There's no way around that," one law enforcement official conducting the raid told Martin, court papers say. "You're a bad man."

Later this month, about three years after that raid, the case against Martin is scheduled to be resolved in Baltimore's federal court. But the identity of the Shadow Brokers, and whoever was responsible for a leak with extraordinary national security implications, will remain a public mystery even as the case concludes.

Authorities have established that Martin walked off with thousands of pages of secret documents over a two-decade career in national security, most recently with the NSA, whose headquarters is about 15 miles from his home in Glen Burnie, Maryland. He pleaded guilty to a single count of willful retention of national defense information and faces a nine-year prison sentence under a plea deal.

Investigators found in his home and car detailed description of computer infrastructure and classified technical operations in a raid that took place two weeks after the Shadow Brokers surfaced online to advertise the sale of some of the NSA's closely guarded hacking tools. Yet authorities have

never publicly linked Martin or anyone else to the Shadow Brokers and the U.S. has not announced whether it suspects government insiders, Russian intelligence or someone else entirely.

The question is important because the U.S. believes North Korea and Russia relied on the stolen tools, which provide the means to exploit software vulnerabilities in critical infrastructure, in unleashing punishing global cyberattacks on businesses, hospitals and cities. The release, which occurred while the NSA was already under scrutiny because of Snowden's 2013 disclosures, raised questions about the government's ability to maintain secrets .

"It was extraordinarily damaging, probably more damaging than Snowden," cybersecurity expert Bruce Schneier said of the Shadow Brokers leaks. "Those tools were a lot of money to design and create."

Yet none of that is likely to be mentioned at Martin's July 17 sentencing. The hearing instead will turn on dramatically different depictions of the enigmatic Martin, a Navy veteran, longtime government contractor—most recently at Booz Allen Hamilton—and doctoral candidate at the time of his arrest.

Prosecutors allege Martin jeopardized national security by bringing home reams of classified information even as, they say, he once castigated colleagues as "clowns" for lax security measures. Soon after his arrest, they cast aspersions on his character and motives, citing a binge-drinking habit, his arsenal of unregistered weapons and online communication in Russian and other languages.

The agents who searched his house that August 2016 afternoon found a trove of documents in his car, home and a dusty, unlocked shed. The 50 terabytes of information from 1996 to 2016 included personal details of government employees and "Top Secret" email chains, handwritten notes

describing the NSA's classified computer infrastructure, and descriptions of classified technical operations.

Defense lawyers paint him as a compulsive hoarder whose quirky tendencies may have led him astray but who never betrayed his country.

"What began as an effort by Mr. Martin to be good at his job, to be better at his job, to be as good as he could be, to see the whole picture at his job, became something more complicated than that," public defender James Wyda said at a 2016 detention hearing. "It became a compulsion.

In this Oct. 5, 2016 file photo, the house of Harold Thomas Martin III is seeing in Glen Burnie, Md. A high-profile raid at the home of an NSA contractor seemed to be linked to the devastating leak of U.S. government hacking tools. Three years later, the case is being resolved but whoever was behind the leak of

the hacking tools remains a mystery with significant national security implications. (AP Photo/Jose Luis Magana)

"This was not Spycraft behavior," he added. "This is not how a Russian spy or something like that would ever conduct business."

It's unclear how Martin came to the FBI's attention, but a redacted court order from a judge suggests agents may have been looking for a Shadow Brokers link when they obtained search warrants for his Twitter account and property before the raid.

The December 2018 ruling from U.S. District Judge Richard Bennett notes that the FBI was investigating the online disclosure of stolen government property. It cites a Twitter message from an account allegedly belonging to Martin—@HAL_999999999—that requested a meeting with someone whose name is blacked out and stated "shelf life, three weeks."

In a likely reference to the Shadow Brokers disclosures, investigators said tweets from Martin's account were sent hours before stolen government records were advertised and posted online. Investigators also alleged that Martin would have had access to the same classified information as what appeared online.

The recipient of the message is redacted, although Politico reported it went to the Moscow-based cybersecurity firm Kaspersky Lab, which in turn notified the U.S. Kaspersky declined to discuss the Martin case.

The roughly 20 officers who stormed Martin's home did so with dramatic force, arriving with a battering ram and a "flash bang" device meant to cause temporary disorientation. State troopers shut down the

road as agents interrogated Martin for four hours.

Martin was never charged with disclosing information and was accused only of unlawfully retaining defense information. The Shadow Brokers, which two weeks before Martin's arrest surfaced on Twitter with the warning that it would auction off NSA hacking tools online, continued trickling out disclosures after Martin was in custody, a seeming indication that someone else may have been responsible.

Even so, his case refocused public attention on repeated government failures to safeguard some of the nation's most highly classified information, with Martin one of several contractors accused of mishandling or spilling government secrets. Most notable is Snowden, a fellow Booz Allen contractor facing U.S. charges and living in Russia.

The NSA has since done more to protect its network and security and increased the monitoring of its employees, said security and counterintelligence director Marlisa Smith.

"I won't tell you we've erased the risk of insider threat, it will never be down to zero, but we've worked very hard to mitigate and minimize the risk," Smith said.

Booz Allen scrambled to respond to Martin's arrest, hiring ex-FBI director Robert Mueller to investigate. Since Martin's arrest, the company said it has added policies to improve its review process of employees at hiring and to ensure managers are more in touch with their subordinates.

As for the mystery of who or what is behind the Shadow Brokers, there's little certainty that the government will ever publicly resolve that lingering question, especially given the classified nature of the theft and the embarrassment it caused the U.S.

"I don't know if anybody knows other than the Russians," said former NSA computer scientist Dave Aitel. "And we don't even know if it's the Russians. We don't know at this point; anything could be true."