



April 3, 2015

## **American Citizen Linked to al-Qaeda is Captured, Flown Secretly to U.S.** **Adam Goldman and Tim Craig, Washington Post**

An American citizen who was once thought to be a top operative in al-Qaeda has been detained in Pakistan and secretly flown to New York to face federal terrorism charges, according to U.S. officials.

Muhanad Mahmoud al Farekh, 29, did not enter a plea during a brief arraignment in federal court in Brooklyn on Thursday. Farekh, also known by the nom de guerre Abdullah al-Shami, was charged with conspiracy to provide material support to terrorists. A judge ordered him held.

Pakistani forces detained Farekh several weeks ago and recently transferred him to U.S. custody after his identity was confirmed. Officials said he was questioned by members of an interrogation team composed of FBI, CIA and Pentagon officials and then advised of his Miranda rights.

Little is known about Farekh, who is believed to have been born in Texas but to have moved with his family at a young age to Jordan, where he also has citizenship. He also attended school in Canada.

He and two other associates were studying at the University of Manitoba when, around 2007, they sold their belongings and left Winnipeg. They then traveled to Pakistan to link up with militants and fight against American forces, according to a criminal complaint filed in the Eastern District of New York.

The three called a friend in Canada when they arrived and told him they intended to become "martyrs," the complaint says.

Over the next several years, Farekh rose through al-Qaeda's ranks, later coming to the attention of U.S. intelligence officials. By 2013, he had been nominated by the Pentagon to a "kill list" of suspected terrorists.

Senior U.S. officials said consideration of that nomination stalled as the Justice Department examined whether it would be legal to kill him, given his American citizenship. The Obama administration had previously authorized the killing of Anwar al-Awlaki, a radical American-born cleric in Yemen who was determined to have presented a continuing and imminent threat to U.S. interests and who could not feasibly be captured.

Officials said there were questions about how prominent a role Farekh played in al-Qaeda. The decision not to authorize his killing frustrated members of Congress who thought the administration was dithering, officials said.

If convicted, Farekh faces a maximum of 15 years in prison.

He is the second terrorism suspect with U.S. ties to be captured or killed in Pakistan in recent months. In December, Pakistani forces killed Adnan el Shukrijumah, a senior al-Qaeda operative on the FBI's Most

# PIAB Media Highlights

## April 3, 2015

Wanted Terrorists list. Shukrijumah had been indicted in New York on charges that he played a role in the terrorist group's failed plan to attack the city's subways in 2009.

The move to bring Farekh to the United States to face federal charges is likely to draw criticism from some Republicans in Congress who believe suspected terrorists, even Americans, should not have the same rights as criminal defendants and should be held at the prison at Guantanamo Bay, Cuba.

President Obama, however, has vowed to close the facility, and no detainee has been sent there since 2008.

The federal prosecution of terrorism suspects captured overseas has become almost commonplace. Last year, a Russian citizen who was captured in Afghanistan and held there for years was indicted in U.S. federal court and charged with conspiring to murder a U.S. national and with use of a weapon of mass destruction. That case marked the first time a foreign combatant captured on the battlefield in Afghanistan had been brought to the United States to be prosecuted.

The FBI's Joint Terrorism Task Force in New York, working with federal prosecutors there, handled the case against Farekh. One of the officials briefed on the case said Farekh was interrogated at length by what is known as a High-Value Detainee Interrogation Group.

"Today's arrest demonstrates that there is no escape from the long reach of our law for American citizens who seek to do harm to our country on behalf of violent terrorists," said U.S. Attorney Loretta E. Lynch. "We will continue to use every tool at our disposal to bring such individuals to justice."

It is not clear where the interrogations of Farekh took place. In the past, officials have used Bagram air base in Afghanistan or warships to question terrorism suspects who were later brought to the United States.

Farekh's capture comes after Pakistan began a long-promised military offensive against militant forces lodged in North Waziristan, part of the tribal areas along the Afghanistan border that are used as safe havens by terrorist groups.

Pakistan claimed to have killed nearly 1,000 militants as part of the offensive.

In operations in North Waziristan and nearby regions, as well as in Karachi, Pakistani forces say they have also killed and captured numerous al-Qaeda operatives, including Shukrijumah, who was born in Saudi Arabia and was believed to have been in charge of the group's external operations.

## **NSA Touts Role in Cyber Investigations**

**Sean Lyngaas, FCW.com**

The National Security Agency has helped investigate every major cyber intrusion in the private sector in the last six months, Director Adm. Michael Rogers said, adding that he wants that collaboration to get faster and more anticipatory.

"We have got to figure out a way that we can harness the capabilities of NSA to partner with the private sector in the name of defending our nation, because NSA has some amazing technical capabilities in the information assurance arena," Rogers said April 2 at a conference hosted by AFCEA's Washington, D.C., chapter.

Rogers, who also heads U.S. Cyber Command, said the FBI, NSA and other agencies worked well with Sony Pictures Entertainment in investigating the devastating November hack on the film studio, but lamented that the work was post-mortem rather than proactive.

# PIAB Media Highlights

## April 3, 2015

"It can't just be that the only time we interact with each other is when things are going wrong," he said.

Rogers said he envisions the NSA and Cyber Command swiftly sharing cyber-threat indicators with firms, which in turn give the agencies feedback on how well they identified incoming threats. The NSA can help dissect the malware used in attacks on the private sector, then develop security signatures in response, he said. There are "always advanced indicators" of a cyberattack, "well before you get to that offensive, destructive act," he added.

Earlier at the conference, Maj. Gen. Joseph Brendler, director of plans and policy (J-5), at Cyber Command, sounded a similar note of cooperation with the private sector on cyber defense. "I think we're increasingly appreciating the importance of our public-private partnerships and the nuances associated with that," he said, adding, "that has to be founded on the appropriate regulatory framework."

Rogers' statements highlight the NSA's central role in attributing cyberattacks on U.S. assets to specific actors. In making their case that North Korea was responsible for the Sony Pictures hack, FBI officials declined to specify what role the NSA had in the attribution. But after the FBI blamed North Korea publicly in December, Rogers said the NSA fingered North Korea by tracing the malware used in the attack.

NSA's outreach to the private sector could extend to shared facilities. Rogers said he is interested in "[creating] some infrastructure out in the private sector" that Cyber Command could use outside its Fort Meade, Md., headquarters, but did not elaborate. A Cyber Command spokesperson could not be reached to elaborate on any plans for such a facility.

### **Bill Would Stop Feds from Mandating 'Backdoor' to Data**

**Erin Kelly, USA Today**

WASHINGTON — A bipartisan group of lawmakers is set to push for legislation that would bar federal agents from forcing tech companies to give them access to customers' emails, texts and photos.

"I think you have the right to go about your business without government — in a Big Brother way — listening to your phone calls or reading your emails," said Rep. Mark Pocan, D-Wis.

Pocan is sponsoring the Surveillance State Repeal Act with Rep. Thomas Massie, R-Ky. The bill includes a provision that the federal government cannot require electronics or software manufacturers to build in a mechanism to allow the government to bypass privacy technology.

The issue, which will come up this spring as part of the debate over whether to reauthorize the Patriot Act, underscores a growing struggle between federal law enforcement agencies and the tech industry over data encryption.

The bill's sponsors plan to push for the legislation after Congress returns from its two-week recess.

As consumers in the USA and overseas demand more privacy on their electronic devices, tech companies such as Apple and Google have strengthened their data encryption to protect personal information from cyber criminals and government surveillance. Privacy concerns have risen in the wake of the 2013 revelations by former National Security Agency contractor Edward Snowden that the NSA was collecting the phone data of millions of Americans.

Top officials at the FBI and the Department of Justice have responded angrily, saying encryption — especially encryption that can only be turned off by users — will hamper efforts to monitor criminal activity and catch bad guys. Federal law enforcement officials want tech companies to give them a "backdoor" into encrypted cellphones and other devices.

# PIAB Media Highlights

## April 3, 2015

"The problem," Massie said, "is that If we put in backdoors for the convenience of the government, those backdoors can be exploited by hackers as well."

The tech industry says there is no way to create a secure backdoor that cannot be exploited by cyber criminals.

"We feel quite confident that it is not technologically possible to only allow good guys to get in," said Josh Kallmer, vice president for global policy at the Information Technology Industry Council. The council's members include Apple, Facebook, Google, Microsoft and Twitter.

Although there is currently no law forcing tech companies to build in ways for the government to bypass privacy technology on electronic communication, Pocan and Massie say there is heavy pressure on companies to do so.

FBI Director James Comey has publicly chastised tech companies for installing automatic encryption into their devices and has urged Congress to pass legislation that would prohibit it. Attorney General Eric Holder also has weighed in, saying that quick access to phone data can help law enforcement officers find victims snatched by kidnappers and child molesters.

"Encryption threatens to lead us all to a very, very dark place," Comey said during a public appearance at the Brookings Institution in October. "Have we become so mistrustful of government and law enforcement in particular that we are willing to let bad guys walk away, willing to leave victims in search of justice?"

In an age of increased privacy concerns, there is no way that Congress would pass a bill to give the government greater access to electronic communications, said Patrick Eddington, the Cato Institute's policy analyst for homeland security and civil liberties.

"If anyone tried to bring up a bill that would mandate backdoors, it would fail by probably 300 votes in the House of Representatives," he said.

Eddington said the idea that encryption alone is going to shut down law enforcement is "absurd."

"The mass surveillance that the NSA and FBI have developed didn't stop the underwear bomber, the Boston Marathon bomber or the shootings at Fort Hood," he said. Eddington and other critics of mass surveillance say law enforcement agencies achieve better results with targeted surveillance of suspected criminals carried out with warrants.

An amendment by Massie and Rep. Zoe Lofgren, D-Calif., to prevent the government from forcing tech companies to install backdoors passed the House last year by a vote of 293-123 as part of a spending bill for the Defense Department. However, the amendment was stripped out in the final bill negotiated between the House and Senate.

This year, Massie and Pocan have put the provision into legislation that would repeal the Patriot Act, which is set to expire, in part, on June 1. If their legislation proves too controversial to pass, Massie said he will try again to attach the anti-backdoor provision to another must-pass spending bill.

Justice Department spokesman Peter Carr said the agency has not yet taken a position on the Pocan-Massie legislation and declined comment.

"We're not giving up," Massie said. "People are fed up. They want their privacy back."

# PIAB Media Highlights

## April 3, 2015

### **Don't Let America be Boxed in by Its Own Computers**

**Michael V. Hayden, Washington Post**

*Michael V. Hayden is a principal at the Chertoff Group, a security and risk management advisory firm with clients in the technology sector. He was director of the National Security Agency from 1995 to 2005 and the Central Intelligence Agency from 2006 to 2009.*

As director of the National Security Agency and then the Central Intelligence Agency after the Sept. 11, 2001, attacks, I fought to provide our intelligence officers with every possible advantage in their work to detect and confront threats from our enemies.

We were entering a new kind of conflict. I had grown to professional maturity in an era in which it was NATO vs. the Soviet Union, and our enemy — with its tank divisions in Eastern Europe and intercontinental ballistic missile silos in our sights — was easy to find, though hard to defeat. Today, our enemies are relatively easy to defeat, but they often are damnably difficult to find. Hence the need to create timely, actionable — even exquisite — intelligence.

In our efforts, the genius and innovation of American business has been essential. The United States enjoys a number of advantages, such as world-class information-technology companies, a mastery of the challenges and opportunities of big data and the reality that much of the world's Internet traffic is serviced by U.S. companies. These things have truly made a difference, but sometimes less can be more. Here a little bit of history might be instructive.

In the late 20th century, many viewed the world as a zero-sum game. Any U.S. loss of competitive advantage was our adversary's gain, and our security, the argument went, was correspondingly weakened as well.

Then, a key technology battleground was a measure of raw computing power known as "MTOPS" — or millions of theoretical operations per second. Successive administrations tried to protect this assumed U.S. security advantage by blocking exports of computers above a certain MTOPS limit to any but our closest allies. The NSA was always an important player in this discussion. After all, in the business of making and breaking codes, advantages in computing power were often decisive. The export barrier was seen as the NSA's friend.

By the time I became NSA director in the late 1990s, however, the calculation was no longer that simple. We still wanted an MTOPS advantage, of course, but we were fast realizing that our preferred limits were undermining the global competitiveness of the U.S. computer industry — the very industry on which we relied for our success. It was becoming clear that the overall health of that industry was more important than any MTOPS advantage against a specific target country. We still insisted on limits with regard to places such as Cuba and North Korea, but we became far more forgiving elsewhere.

This, of course, had a powerful, positive commercial impact, but the NSA didn't flip its position for commercial reasons. We did it for security reasons. On balance, this change made us stronger, not weaker, over the long haul, since retarding exports would inevitably retard the technological progress that was both our economic and our security lifeblood.

That early lesson has caused me to continue to challenge arguments that technological protectionism furthers national security. It might, but then again, it could have the opposite effect if it freezes development, alienates allies, feeds distrust or invites the creation of similar barriers abroad. I would recommend these broader considerations to those in the U.S. security enterprise with responsibility for evaluating these trade-offs today.

In a perverse way, as the saying goes, what goes around comes around. Precedents we set will be followed — or exploited — by others in an economic system that becomes more globalized and hence

## PIAB Media Highlights

### April 3, 2015

more interdependent by the day. Already others point to U.S. activities to justify their own, often nefarious, efforts. Witness the Chinese trying to create moral and legal equivalency between legitimate U.S. intelligence and their massive theft of intellectual property, or their placement of newly minted restrictions on U.S. IT firms. One wonders what the Russias and Chinas of the world will demand if U.S.-based firms are forbidden to create encryption schemes inaccessible to themselves or the government. Beyond the realm of speculation, the Chinese company Alibaba has announced plans to open a cloud data center in the United States. How will we feel when a Chinese court orders Alibaba to send data on Americans back to China, citing our own behavior as justification?

These are serious, long-term questions requiring serious, strategic answers. Possible second- and third-order effects — such as generating a stampede toward data localization or a Balkanized Internet — need to be considered alongside a still-important calculus based on more transient, tactical advantage.

U.S. intelligence was given a black eye, unfairly for the most part, by l’Affaire Snowden. It has conducted its business honorably, with restraint and oversight — perhaps more than any other country. But that has been little noted.

Today’s issues give the United States a chance to demonstrate to the world that its tough and powerful intelligence services understand what is at stake and intend to join the public discussion on how to balance the truly important privacy and security questions before us and, more important, take meaningful steps to make us stronger.