The Washington Times

Brussels terrorism revives calls in Congress for deciphering on demand

Andrew Blake

March 23, 2016

Investigators aren't certain how Islamic State terrorists coordinated Tuesday morning's triple bombings in Brussels, but as in past attacks, lawmakers are saying the perpetrators used strong encryption and are pushing efforts to ensure all digital communications can be deciphered on demand.

Deliberate or not, the terrorist group, also known as ISIS, is influencing the international debate over encryption and governments' growing inability to access digital evidence such as emails and texts because of the increasing prevalence of technology that can evade eavesdropping.

Lawmakers this week renewed calls for anti-encryption legislation, "before the blood has dried" in the Belgian capital, as libertarian scholar Julian Sanchez of the Cato Institute was quick to quip on Twitter.

Indeed, Rep. Adam B. Schiff of California, the top Democrat on the House Permanent Select Committee on Intelligence, responded with a statement issued before much of the country had learned about the attacks hours earlier.

"We do not know yet what role, if any, encrypted communications played in these attacks — but we can be sure that terrorists will continue to use what they perceive to be the most secure means to plot their attacks," he said.

By Wednesday morning, the chairman of the House Homeland Security Committee had already announced his conclusions.

"It's this encryption idea, the idea that they can communicate in 'dark space' like they did in Paris — like what I think probably happened here in the Brussels case — that concerns us the most. If you can't see their communications, you can't stop it," Rep. Michael T. McCaul, Texas Republican, told Fox News.

This readiness to blame end-to-end encryption was expected, given the immediate response in the aftermath of similar assaults carried out by jihadis who have "gone dark." But Tuesday's attack unfolded not only in the midst of the fiery encryption debate in the U.S., but also just as the government's arguments suffered two of its biggest blows to date.

Hours before three bombs were detonated in Brussels, attorneys for the U.S. government told a District Court judge in California that they won't for now be needing Apple's assistance in

unlocking an encrypted, password-protected iPhone owned by San Bernardino killer Syed Farook, putting a pause on a dramatic showdown between Washington and Silicon Valley.

Privacy proponents were awarded a slight, albeit temporary, win with the Apple case on hold, and uncertainly now exists over whether the FBI will still ask the company to subvert its own security features after acquiring the hacking skills of, according to Reuters, an Israeli security firm.

"It's important that the government take all steps possible before asking for wide-reaching powers that would dramatically impact the future of cybersecurity for years to come," Rep. Darrell E. Issa, California Republican, said in a statement. "It's now clear that, in this case, they hadn't."

Days earlier, a French police report obtained by The New York Times noted that the terrorists responsible for the Paris attacks in November hadn't necessarily evaded authorities because of encryption, but rather relied on disposable "burner" phones to communicate without leaving a clear trail of clues.

Nevertheless, what could have been a key moment in the tech sector's fight against the government's demands has been derailed by alarms from Capitol Hill.

In addition to calls for a legislative solution to the government's "going dark" dilemma, reports quickly circulated this week concerning a supposed warning issued by Islamic State sympathizers that encouraged followers to use encryption.

In a Tuesday interview with Business Insider, Michael S. Smith, an adviser to Congress' Task Force on Terrorism and Unconventional Warfare, said explicitly that the message came from the Islamic State "tech support team."

"By making it known that they are using these technologies, they are fundamentally undermining confidence among civilian populaces that our technologically superior governments can effectively manage threats posed by this terrorist group," he said.

However, others questioned the authenticity of an English-language memo that, according to security analysts, provided little guidance for would-be jihadis.

"This is not operational guidance for ISIS terrorists. It does not recommend encryption to evade security forces. There is no practical advice here for real terrorists," The Grugq, an information security researcher, wrote in a blog post this week. "It's basically the jihadi equivalent of 'sending thoughts and prayers.'"

Before the Brussels attacks, the Senate reportedly was preparing to introduce a bill that would establish civil penalties for companies that don't decrypt data when compelled by authorities. Its main Democratic backer, Sen. Dianne Feinstein of California, said authorities "must use all the tools at our disposal to fight back."

In the House, Mr. McCaul said an effort to create a national commission devoted to the "going dark" issue is more likely to pass now than ever. "I think after the events of today, it's important that Congress does something and that Congress acts," he said Tuesday.