The Washington Times

Brussels attacks fuel already fiery encryption debate

Andrew Blake

March 22, 2016

The top-ranking Democrat on the House Intelligence Committee was quick to suggest on Tuesday that the individuals responsible for carrying out deadly attacks across Belgium earlier that morning had relied on strong encryption to stay off the radar of authorities.

“We do not know yet what role, if any, encrypted communications played in these attacks,” Rep. Adam Schiff, California Democrat, said in a statement sent out early Tuesday.

“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 added.

Officials say that at least 31 people have been declared dead so far after bombs were detonated early Tuesday at the Brussels airport and a at metro station in the Belgium capital.

No group has formally taken credit yet for the blasts, but Mr. Schiff said that the bombings “bear all the hallmarks” of being either inspired by or coordinated with the help of the Islamic State terror group, whose members previously claimed responsibility for the attacks that killed 130 in Paris last November.

Law enforcement officials have previously suggested that last year’s tragedy in Paris and a shooting-spree in San Bernardino, California, the following month may had been carried out by individuals who evaded authorities by communicating with strong end-to-end encryption that can’t be deciphered.

This week, however, The New York Times reported that antiterrorism police have since told France’s Interior Ministry that the persons responsible for the November attacks had relied on disposable “burner” phones to speak with one another without leaving a lengthy trail of clues.

On Monday, the U.S. Justice Department filed a court motion suggesting that investigators have found a way to unlock the supposedly impenetrable iPhone that had been recovered from one of the two San Bernardino shooters and in turn ignited a fiery debate between Silicon Valley and Washington, D.C., over the merits of strong encryption.

Julian Sanchez, a senior fellow at the Cato Institute, a libertarian think-tank, was quick to chide Mr. Schiff on Twitter for suggestion that encryption aided the perpetrators of Tuesday morning's attacks "before the blood has dried."

"Reflexive crypto scapegoating gives the reassuring impression there's a silver bullet for intel failure," Mr. Sanchez added.

In his statement, Mr. Schiff said the U.S. "must continue to build the capacity of our partners and allies to improve their intelligence and law enforcement capabilities."

"We must use all the tools at our disposal to fight back," Sen. Dianne Feinstein, California Democrat and vice chairwoman of the Senate Intelligence Committee, said in a statement on Tuesday. "The way to prevent attacks like this is to develop good intelligence and always be vigilant."

In the wake of the San Bernardino rampage, Ms. Feinstein vowed to introduce legislation that would ensure authorities could access and decipher encrypted data as companies like Apple and Google make it easier for consumers to protect their personal data with strong encryption. On his part, Mr. Schiff said in December that a legislative solution seemed "feasible or even desirable."

A day earlier, meanwhile, two House committees on Monday announced the establishment of a congressional working group that will "examine, research and make recommendations for potential policy solutions to protect the benefits of encryption — namely, the privacy and security of our personal information in a digital age — while seeking ways for law enforcement to have the tools it needs to investigate crime."