Russian hackers posed as IS to threaten military wives

By By RAPHAEL SATTER

Published: 2018-05-08 · Archived: 2026-04-05 16:14:30 UTC

PARIS (AP) — Army wife Angela Ricketts was soaking in a bubble bath in her Colorado home, leafing through a memoir, when a message appeared on her iPhone:

“Dear Angela!” it said. “Bloody Valentine’s Day!”

“We know everything about you, your husband and your children,” the Facebook message continued, claiming that the hackers operating under the flag of Islamic State militants had penetrated her computer and her phone. “We’re much closer than you can even imagine.”

Ricketts was one of five military wives who received death threats from the self-styled CyberCaliphate on the morning of Feb. 10, 2015. The warnings led to days of anguished media coverage of Islamic State militants’ online reach.

Except it wasn’t IS.

The Associated Press has found evidence that the women were targeted not by jihadists but by the same Russian hacking group that intervened in the American election and exposed the emails of Hillary Clinton’s presidential campaign chairman, John Podesta.

The false flag is a case study in the difficulty of assigning blame in a world where hackers routinely borrow one another’s identities to throw investigators off track. The operation also parallels the online disinformation campaign by Russian trolls in the months leading up to the U.S. election in 2016.

Links between CyberCaliphate and the Russian hackers — typically nicknamed Fancy Bear or APT28 — have been documented previously. On both sides of the Atlantic, the consensus is that the two groups are closely related.

But that consensus never filtered through to the women involved, many of whom were convinced they had been targeted by Islamic State sympathizers right up until the AP contacted them.

“Never in a million years did I think that it was the Russians,” said Ricketts, an author and advocate for veterans and military families. She called the revelation “mind blowing.”

“It feels so hilarious and insidious at the same time.”

‘COMPLETELY NEW GROUND’

As Ricketts scrambled out of the tub to show the threat to her husband, nearly identical messages reached Lori Volkman, a deputy prosecutor based in Oregon who had won fame as a blogger after her husband deployed to the Middle East; Ashley Broadway-Mack, based in the Washington, D.C., area and head of an association for gay and

lesbian military family members; and Amy Bushatz, an Alaska-based journalist who covers spouse and family issues for Military.com.

Liz Snell, the wife of a U.S. Marine, was at her husband's retirement ceremony in California when her phone rang. The Twitter account of her charity, Military Spouses of Strength, had been hacked. It was broadcasting public threats not only to herself and the other spouses, but also to their families and then-first lady Michelle Obama.

Snell flew home to Michigan from the ceremony, took her children and checked into a Comfort Inn for two nights.

"Any time somebody threatens your family, Mama Bear comes out," she said.

The women determined they had all received the same threats. They were also all quoted in a CNN piece about the hacking of a military Twitter feed by CyberCaliphate only a few weeks earlier. In it, they had struck a defiant tone. After they received the threats, they suspected that CyberCaliphate singled them out for retaliation.

The women refused to be intimidated.

"Fear is exactly what — at the time — we perceived ISIS wanted from military families," said Volkman, using another term for the Islamic State group.

Volkman was quoted in half a dozen media outlets; Bushatz wrote an article describing what happened; Ricketts, interviewed as part of a Fox News segment devoted to the menace of radical Islam, told TV host Greta Van Susteren that the nature of the threat was changing.

"Military families are prepared to deal with violence that's directed toward our soldiers," she said. "But having it directed toward us is just complete new ground."

'WE MIGHT BE SURPRISED'

A few weeks after the spouses were threatened, on April 9, 2015, the signal of French broadcaster TV5 Monde went dead.

The station's network of routers and switches had been knocked out and its internal messaging system disabled. Pasted across the station's website and Facebook page was the keffiyeh-clad logo of CyberCaliphate.

The cyberattack shocked France, coming on the heels of jihadist massacres at the satirical magazine Charlie Hebdo and a kosher supermarket that left 17 dead. French leaders decried what they saw as another blow to the country's media. Interior Minister Bernard Cazeneuve said evidence suggested the broadcaster was the victim of an act of terror.

But Guillaume Poupard, the chief of France's cybersecurity agency, pointedly declined to endorse the minister's comments when quizzed about them the day after the hack.

"We should be very prudent about the origin of the attack," he told French radio. "We might be surprised."

Government experts poring over the station's stricken servers eventually vindicated Poupard's caution, finding evidence they said pointed not to the Middle East but to Moscow.

Speaking to the AP last year, Poupard said the attack "resembles a lot what we call collectively APT28."

Russian officials in Washington and in Moscow did not respond to questions seeking comment. The Kremlin has repeatedly denied masterminding hacks against Western targets.

'THE MEDIA PLAYED RIGHT INTO IT'

Proof that the military wives were targeted by Russian hackers is laid out in a digital hit list provided to the AP by the cybersecurity company Secureworks last year. The AP has previously used the list of 4,700 Gmail addresses to outline the group's espionage campaign against journalists , defense contractors and U.S. officials . More recent AP research has found that Fancy Bear, which Secureworks dubs "Iron Twilight," was actively trying to break into the military wives' mailboxes around the time that CyberCaliphate struck.

Lee Foster, a manager with cybersecurity company FireEye, said the repeated overlap between Russian hackers and CyberCaliphate made it all but certain that the groups were linked.

"Just think of your basic probabilities," he said.

CyberCaliphate faded from view after the TV5 Monde hack, but the over-the-top threats issued by the gang of make-believe militants found an echo in the anti-Muslim sentiment whipped up by the St. Petersburg troll farm — an organization whose operations were laid bare by a U.S. special prosecutor's indictment earlier this year.

The trolls — Russian employees paid to seed American social media with disinformation — often hyped the threat of Islamic State militants to the United States. A few months before CyberCaliphate first won attention by hijacking various media organizations' Twitter accounts, for example, the trolls were spreading false rumors about an Islamic State attack in Louisiana and a counterfeit video appearing to show an American soldier firing into a Quran .

The AP has found no link between CyberCaliphate and the St. Petersburg trolls, but their aims appeared to be the same: keep tension at a boil and radical Islam in the headlines.

By that measure, CyberCaliphate's targeting of media outlets like TV5 Monde and the military spouses succeeded handily.

Ricketts, the author, said that by planting threats with some of the most vocal members of the military community, CyberCaliphate guaranteed maximum press coverage.

"Not only did we play right into their hands by freaking out, but the media played right into it," she said. "We reacted in a way that was probably exactly what they were hoping for."

___

Satter reported from Paris. Associated Press writers Michael Conroy in Bloomington, Indiana; Jeff Donn in Plymouth, Massachusetts; and Desmond Butler in Washington contributed to this report.

___

Online:

Satter can be reached at: http://raphaelsatter.com
