



What we do and still don't know about the Paris attack

Matt A. Mayer

March 21, 2016 11:42 am | *AEIdeas*

In a detailed [news report from Europe](http://www.irishtimes.com/news/world/europe/paris-attacks-terrifyingly-fatal-layers-of-resources-and-tactics-1.2580749) (<http://www.irishtimes.com/news/world/europe/paris-attacks-terrifyingly-fatal-layers-of-resources-and-tactics-1.2580749>), we learn just how extensive the terrorist network in Europe is and, even more chilling, how sophisticated their activities are. The three key conclusions coming out of the Paris attack in November center on terrorists' use of technology, their use of a broad network of sympathizers, and their high-level bomb-making skills. These findings make it all the more critical that the US strengthen screening programs and get past the lawsuit between Apple and the FBI to find longer-term solutions to the use of technology by terrorists.



(http://www.aei.org/wp-content/uploads/2016/03/RTSB8L7_paris_attacks_captured_bruges-e1458574574251.jpg)

Reporters stand in front of a prison in Bruges where Salah Abdeslam is being held, Belgium, March 19, 2016. REUTERS/Eric Vidal.

When it comes to using technology, the Paris attackers secured boxes of cellphones to use and ditch to avoid detection. It wasn't just the acquisition of a large number of cellphones, however, that shows their adaption. It was their careful use of cellphones that bears minding. As the report states, "Most striking is what was not found on the phones: not a single email or online chat from the attackers has surfaced so far. Even though one of the disposable phones was found to have had a Gmail account, with the username "yjeanyves1", the police discovered it was empty, with no messages in the sent or draft folders." The absence of such evidence indicates the heavy use of encrypted technology:

But the three teams in Paris were comparatively disciplined. They used only new phones that they would then discard, including several activated minutes before the attacks, or phones seized

from their victims. According to the police report and interviews with officials, none of the attackers' emails or other electronic communications have been found, prompting the authorities to conclude that the group used encryption. What kind of encryption remains unknown.

The report notes a survivor's account from the Bataclan theater, "one of the gunmen pulled out a laptop, propping it open against the wall...she saw a line of gibberish across the screen: 'It was bizarre - he was looking at a bunch of lines, like lines of code. There was no image, no internet,' she said. Her description matches the look of certain encryption software." With Congress' continued failure to [move forward on a national commission](http://www.aei.org/wp-content/uploads/2016/01/National-commission-on-terrorists-use-of-technology-is-needed.pdf) (<http://www.aei.org/wp-content/uploads/2016/01/National-commission-on-terrorists-use-of-technology-is-needed.pdf>) our ability to determine the "worst-best" solution to the complex struggle between law enforcement's need to track terrorist and the citizenry's right to use encryption to secure their lives is compromised.

On the use of sympathizers, the report notes that the terrorists "have exploited weaknesses in Europe's border controls to slip in and out undetected, and worked with a high-quality forger in Belgium to acquire false documents. The scale of the network that supported the attacks, which took 130 lives and wounded 813 people, has also surprised officials, as President François Hollande of France acknowledged on Friday." It is hard enough to track the bad guys with the huge flow of refugees that allows them to blend in. It will be even harder if European citizens or immigrants help hide them in the countless neighborhoods across Europe where they can easily disappear into the fabric of everyday life.

These weaknesses go well beyond border controls and sympathizers helping hide terrorists. It goes straight to the ability of member states to cooperate to identify terrorist for watch list and screening programs. As Alain Chouet, the former head of French Intelligence admitted, "We don't share information. We even didn't agree on the translations of people's names that are in Arabic or Cyrillic, so if someone comes into Europe through Estonia or Denmark, maybe that's not how we register them in France or Spain." Due to political and legal hurdles, "security services are constrained by the inability or unwillingness of countries to share intelligence about potential terrorists."

If Europe can't figure out who is and is not a potential terrorist and terrorists are able to employ "high-quality forgers" in combination with their ability to obtain legitimate identification papers, America's vulnerabilities increase dramatically. With [our reliance on European processes](http://www.aei.org/publication/crucial-loopholes-in-visa-programs-must-be-closed/) (<http://www.aei.org/publication/crucial-loopholes-in-visa-programs-must-be-closed/>), programs like the Visa Waiver Program could more easily be used to travel to the US, especially for high-level bomb makers and other unknown terrorist leaders.

It is clear that the Paris attack had the use of a very good bomb maker. As the report notes:

But creating an effective bomb can be tricky, and the success in setting off bomb after bomb is indicative of the group's training and skill...The autopsy [of one suicide bomber] showed that a piece of string with a flap of adhesive tape at one end, believed to be the detonation cord, was wrapped around the limb. Along with TATP residue, they again found electrical wires, a nine-volt alkaline battery to drive the detonation, and pieces of metal, including bolts, that had been mounted on the suicide belt as projectiles.

The story quotes Peter Bergen noting that "[t]o make an effective TATP bomb requires real training, which suggests a relatively skilled bomb-maker was involved in the Paris plot, since the terrorists detonated several bombs. It also suggests that there was some kind of bomb factory that, as yet, appears to be undiscovered, because putting together such bombs requires some kind of dedicated space."

The fact that we still have not located the bomb factory used to make the Paris suicide belts is troubling. We need to find that location in order to do a full forensic sweep of it to capture DNA and fingerprints. With fingerprints, we may not know the bomb maker's name, but we will be able to get him by his fingerprints should he attempt to travel or gets arrested for other activities.

As our knowledge of the Paris attacks increases, it places greater urgency on our need to evolve to meet today's terrorist threats. We'll hopefully learn more with the capture of Salah Abdeslam.

Learn more: [National commission on terrorists' use of technology is needed](http://www.aei.org/publication/national-commission-on-terrorists-use-of-technology-is-needed/)
(<http://www.aei.org/publication/national-commission-on-terrorists-use-of-technology-is-needed/>) | [Our dangerous reality](http://www.aei.org/publication/our-dangerous-reality/)
(<http://www.aei.org/publication/our-dangerous-reality/>) | [Apple v. FBI encryption case shows that lawsuits are inherently polarizing](http://www.aei.org/publication/apple-v-fbi-encryption-case-shows-that-lawsuits-are-inherently-polarizing/)
(<http://www.aei.org/publication/apple-v-fbi-encryption-case-shows-that-lawsuits-are-inherently-polarizing/>)

This article was found online at:

<http://www.aei.org/publication/what-we-do-and-still-dont-know-about-the-paris-attack/>