Mass surveillance can't catch terrorists. That's the uncomfortable truth

The spread of encryption post-Snowden has ensured that collecting everyone's details en masse is no longer any guarantee

Snooping: Ulrich Mühe in The Lives of Others (2006) Photo: Buena Vista

By Thomas Rid

2:35PM GMT 16 Nov 2015

The Paris terrorists almost certainly used encrypted communications to plan their attacks – after all, the man identified as their mastermind, Abdelhamid Abaaoud, is based in Syria. He would have needed some way to transmit his plans to the gunmen. So, as we in Britain consider the draft Investigatory Powers Bill, the question must be asked: could better government interception, or the banning of encryption, have prevented such an atrocity?

Let us tackle the second question first. The terrorists' use of encryption is no surprise. Indeed it would have been surprising had they not encrypted their electronic communications, given the ready availability of high-grade, end-to-end encryption technologies (end-to-end encryption means that no company in the middle is trusted, only the parties actually communicating with each other can read the messages).

We must face this fact. Criminals may be stupid, but professional militants are not. Hard targets will use advanced encryption. That is a digital fact of life today.

Most of Google's services are encrypted. Facebook is encrypted. WhatsApp is encrypted. Apple offers highly sophisticated forms of encryption on its products. And as the draft Investigatory Powers Bill acknowledges several times, removing encryption may not be practicable for such service providers. Worse, though Apple or Facebook might respond to government requests to hand over data, several encryption services do not even rely on such trusted companies or third parties (PGP or Tor are examples).

America has understood these limitations, and clarified that it will not try to ban or regulate encryption. Even the Trans-Pacific Partnership agreement includes a clause that states cryptography cannot be banned or regulated. Clearly, the cryptography train has left the station. In Britain, the Prime Minister and the Home Office must face this fact. Some criminals may be stupid, but professional militants are not. Hard targets will use advanced encryption. That is a digital fact of life today.

The tougher and more important question is this: if the Paris attackers used encryption to plan the strikes, did they defeat our spies' tools to discover and thwart their plans: bulk interception?

Bulk interception is the collection of large amounts of internet data, sometimes from thick undersea cables. This vast quantity of data is stored, sifted through, minimised, and kept in databases for a limited time. These databases can be legally queried with so-called selectors, such as email addresses, telephone numbers, or login names.

It is known as a "target discovery technique" – a method to identify suspects who can then be targeted more specifically (for instance by hacking into their phones). But there is a problem. As the overall volume of encrypted internet traffic has gone up and up, more and more of the intercepted data has become inaccessible – even to intelligence agencies.

This is because it is not just the content of messages that is encrypted but also, and contrary to widely held opinion, meaningful communications data (or metadata) too. This data – the who, when, and where of online messaging – is also increasingly transmitted in encrypted or truncated form.*

The conclusion is disturbing: bulk interception, our fallback method of getting some handle on encrypted communications in order to prevent attacks, may be failing. What some misleadingly call “mass surveillance,” may not nearly be as useful (or as scary) as both proponents and critics think.

That doesn’t mean bulk intercept is becoming totally useless. Keeping data in large databases for a limited amount of time is a bit like CCTV surveillance: the data may be forensically useful after the fact. Indeed such interception may have already revealed the links between the Paris attackers and IS in Syria. But it is not very helpful to prevent attacks.

Bulk interception, our fallback method of getting some handle on encrypted communications in order to prevent attacks, is failing

The world has changed since 2013, and it is time to acknowledge a harsh truth: the Snowden leaks have had a nasty effect. The operating environment for intelligence agencies in Western democracies is now less permissive. By contrast it is more permissive for spies in autocratic regimes – and for terrorists too. So while some, in Britain and elsewhere, satisfy themselves with generating much sound and fury in the debate over encryption, we should realise that it is a backwards-looking, self-serving, and easy argument to have.

The forward-looking and much harder discussion is about intelligence and law enforcement capabilities and methods that will actually work against the next generation of extremists.

Thomas Rid is a professor in the Department of War Studies at King's College London. His new book, Rise of the Machines (Norton/Scribe), will be out in 2016

** This sentence has been updated. It originally, incorrectly, read: "the who, when, and where of any mobile phone call or email"*