

September 10, 2015
Paul Dietrich (@paulmd199)

MYSTIC is a program that collects the metadata of virtually every call in 5 countries (Mexico, Kenya and the Philippines), and the full content of 2 of them (Bahamas and “Country X”).

Yesterday, James Clapper apparently [confirmed](#) that “Country X” is Afghanistan. While this has been [said before](#), there is still more yet to reveal. The name of the cooperating telco has not yet been publicly identified. It is almost certainly [Afghan Wireless](#) (AWCC). I have known this for quite some time, but have held back, heeding the warning that there was risk to specific personnel, a “small technical company.” Since I have learnt that the program has been terminated, the risk, and the need for further secrecy has been removed.

But, Clapper added, Snowden "exposed so many other things that had nothing to do with" civil liberties and privacy, including information about the US intelligence community's operations that did tangible damage to operations. "He has [done] untold damage to our collection activities," Clapper said, asserting that "terrorists have gone to school on what Snowden leaked." And programs that had a real impact on the security of American forces overseas, including one program in Afghanistan, "which he exposed and Glenn Greenwald wrote about, and the day after he wrote about it, the program was shut down by the government of Afghanistan," Clapper noted.

The Evidence

First some basic background. Afghan Wireless was founded shortly after the fall of the Taliban by an Afghan-American ([Ehsan Bayat](#)) and a British Aristocrat. It is also a joint venture between an American telco (Telephone Systems International) and the Afghan government. That by itself should raise some eyebrows.

According to its own marketing material. Afghan Wireless also has access to all of Afghanistan's provinces, which is unique amongst Afghanistan's telcos. It also has a "[microwave backbone](#)" covering some 4000 kilometers.

Continuing from Cablegate: Afghan Wireless also has [virtually every bank](#) as a customer, has access to rural areas, and has some of its, infrastructure located on [military bases](#) (or at any rate, that was the plan).

All of the above is merely background, suggestive but not definitive. However a piece published by the [Daily Mail](#) removes a lot of the doubt. The founder, Mr Bayat was an FBI informer. And so much more.

But, as Mr Davis said, Mr Bayat had a secret: he was an informant for the FBI, the main US domestic counter- terrorism force. The link made an opening for Operation Foxden, a scheme the FBI planned to run jointly with the National Security Agency (NSA), the US electronic eavesdropping organisation.

The NSA offered \$30 million and technical assistance, said Mr Davis. The plan was to build extra circuits into all the equipment installed, enabling the US to *'record or listen live to every single landline and mobile phone call in Afghanistan'* and *'monitor the telephone gateways*

channelling international calls in and out of the country –(emphasis mine) gateways already being used by Bin Laden, Mullah Omar and their associates, thanks to the satellite phones given by Mr Bayat to Taliban ministers as gifts’.

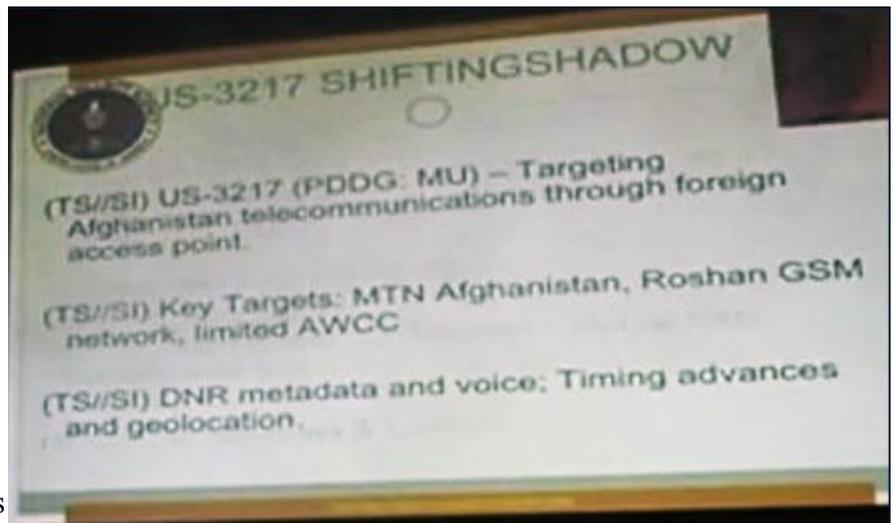
And then there's the spooks shutting down a lawsuit, ruining a business and so much more Bad Creepy Spy Stuff.

Finally, the admission itself is an important piece of evidence, it confirms that [The Intercept](#) and [The Washington Post](#)'s stories are substantially true. Without this admission, the weight of the evidence would have been strongly suggestive, but not fully conclusive. Clapper's admission seals the deal.

Crocodile Tears

When you read Clapper's statement, one gets the impression that The Evil Snowden made Afghanistan go dark. However, it was never the case that MYSTIC was the only game in town. Nor was AWCC the only targeted provider.

Afghanistan's two other major carriers, [MTN Afghanistan](#), and [Roshan GSM](#) are both targeted under SHIFTINGSHADOW. SHIFTINGSHADOW collects metadata, voice content, and geolocation data. The foreign access point has not been identified, to my knowledge.



SHIFTINGSHADOW slide. Source: [Fantasticco](#)

Yet a third program uses the now infamous “[Dirtboxes](#)” to intercept cellular communications directly. Dirtboxes are alternately termed IMSI Catchers, cell-site simulators, or [Stingrays](#). These have been in the news lately, appearing in [Oslo](#) under questionable circumstances, and also mounted on [surveillance craft](#) flying over American cities.

These are three distinct programs, as they have different [SIGADS](#). The first, part of MYSTIC should have a SIGAD starting US-3310, the second, part of OAKSTAR, is US-3217, and the third, involving Dirtboxes, is US-962A5.

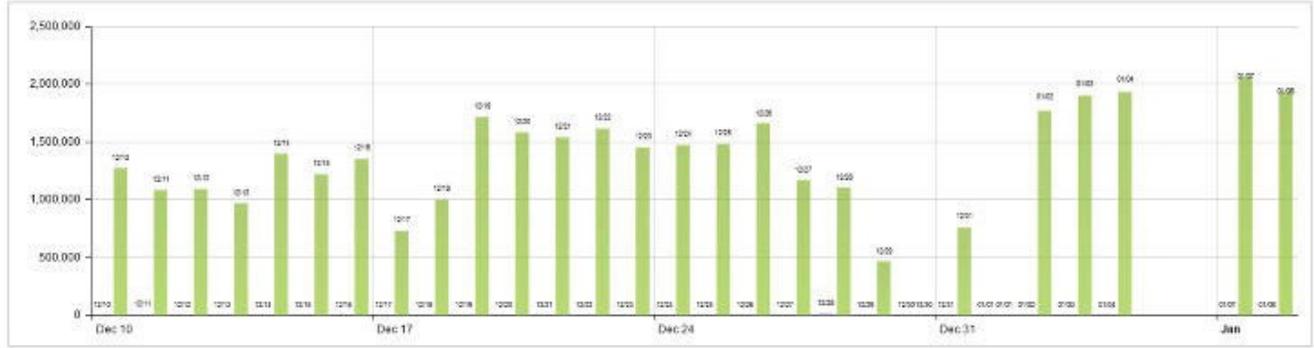
TOP SECRET//COMINT//NOFORN

FAIRVIEW		OAKSTAR	
(C) US-990	FAIRVIEW	(C) US-3206	MONKEYROCKET*
<u>BLARNEY</u>		(C) US-3217	SHIFTINGSHADOW
(C) US-984	FISA collection	(C) US-3230	ORANGECRUSH
(C) US-984X*	FAA collection	(C) US-3247	YACHTSHOP
<u>STORMBREW</u>		(C) US-3251	ORANGEBLOSSOM
(C) US-983	STORMBREW	(C) US-3273	SILVERZEPHYR
(C) US-3140	MADCAPOCELOT	(C) US-3277	BLUEZEPHYR
		(C) US-3354	COBALTFALCON
<u>SSO Corporate/TAO Shaping</u>			
(C) US-3105S1	DARKTHUNDER		
(C) US-3105S1	STEELFLAUTA		

TOP SECRET//COMINT//NOFORN

SSO Corporate Portfolio. Source, [Propublica](#)

AFGHANISTAN - Last 30 Days



Signal Profile



Most Volume



Top 5 Techs



BOUNDLESSINFORMANT Capture. Source: [Dagbladet](#)

TOP SECRET//SI//TK//NOFORN DERIVED FROM NSA/CSS//SI 1.32, DATED 08 JAN 2007, DECLASSIFY ON 20320103

BOUNDLESSINFORMANT

Global AGGREGATE DNI DNR

OVERVIEW
LAST 30 DAYS

TOTAL DNI
97,111,188,358

TOTAL DNR
124,808,692,959

SIGADS
504

CASE NOTATIONS
27,798

PROCESSING SYSTEMS
2,431

Country	DNI	DNR
Pakistan	13,516,527,385	13,759,417,233
Afghanistan	2,316,972,214	21,977,001,389
Iran, Islamic Republic of	14,101,066,499	1,733,419,401
Jordan	12,729,653,438	1,644,602,031
India	6,333,878,580	6,283,036,977

The BOUNDLESSINFORMANT totals for Afghanistan include at least 3 separate programs. Source: [The Guardian](#)