

# CRYPTOME

## Darknet Sweep Casts Doubt on Tor

### Tor Will Be Defeated Again, and Again, and Again

By **Bill Blunden**, November 7, 2014

When [news](#) broke of Silk Road 2.0's seizure by law enforcement a lot of people probably wrote it off as an isolated incident. Silk Road 2.0 was the successor to the original Silk Road web site and like its predecessor it was an underground bazaar for narcotics, fueled by more than \$8 million in Bitcoin transactions and operated as a [hidden service](#) on the Tor anonymity network.

According to the [criminal complaint](#) filed against Blake Benthall, the alleged 26-year-old operator of Silk Road 2.0, law enforcement officers caught their suspect using old fashioned police work. Specifically they sent in a mole, or what the text of the complaint refers to as an *HSI-UC* (a Homeland Security Investigations agent operating in an Undercover Capacity). Anyway, the undercover spy was wildly effective, gaining access to the Silk Road 2.0 discussion forum while the scheme was still in its formative stages and eventually acquiring administrative access to the web site after it launched.

But it turns out that the Silk Road 2.0 takedown was just the appetizer of a much larger main course called *Operation Onymous*. Onymous, as in anything but anonymous. Within a matter of hours it was [announced](#) that a joint operation involving dozens of officers from the FBI, the DHS, and Europol had taken down a grand total of 414 hidden services on the Tor network. This wasn't just a single bust, no sir. This was a global dragnet that resulted in the arrest of 17 suspects.

The success of this international operation raises a question: **how did they locate the hidden servers and identify the people who managed them?**

In this instance Tor hidden services failed to live up to their namesake. Was the sudden collapse of several hundred Tor *“.onion”* domains the result of traditional police tradecraft—developing informants, patiently waiting for opportunities, doggedly following leads— or were security services quietly wielding advanced technical methods?

All told the cops are pretty tight-lipped. *Wired Magazine* [asked](#) Troels Oerting, head of the European Cybercrime Center, this very question and he replied:

*“This is something we want to keep for ourselves... The way we do this, we can't share with the whole world, because we want to do it **again and again and again.**”*

Even with the discretion of insiders like Oerting there have been recent developments that hint at what's going on behind closed doors. For instance, the FBI has just [proposed](#) that the U.S. Advisory Committee on Rules and Criminal Procedure alter federal search and seizure rules so that law enforcement agents can hack into machines that have been “concealed through technological means.” This is no doubt a thinly veiled reference to Tor.

The FBI's request infers that public gripes against ostensibly strong encryption by officials like FBI Director James Comey, GCHQ Director Robert Hannigan, and former NSA General Counsel Stewart Baker are mere theater. The feds already have tools at their disposal to [defeat](#) encryption-based tools like Tor. In fact, an internal NSA documents [admits](#) that "[A] critical mass of targets use Tor. Scaring them away from Tor might be counterproductive."

Really? I wonder why?

This past summer I [questioned the wisdom](#) of netizens putting all their eggs in the Tor basket, as did other writers like *Pando's* [Yasha Levine](#). Granted there were protests voiced by advocates, some of which I [responded](#) to. Still, the public record demonstrates that Tor isn't a guarantee against the intrigues a knowledgeable adversary. And now we clearly see the purported security of the Tor anonymity network unraveled on a grand scale. Not just for one or two illicit websites but hundreds. As to whether it's possible for an app to safeguard essential civil liberties... the techno-libertarians of Silicon Valley can eat crow.

The reality is that the Deep State's minions aim to eradicate genuine anonymity for [everyone but themselves](#). [The steady erosion of privacy is a part of a long-term campaign to consolidate control](#) as economic inequality accelerates and perpetual war expands. The looming Malthusian disaster born of our leaders' unenlightened self-interest will be a [brutal spectacle](#) and the members of the ruling class want to make sure that they'll have a good view.

**Bill Blunden** is an independent investigator whose current areas of inquiry include information security, anti-forensics, and institutional analysis. He is the author of several books, including *The Rootkit Arsenal* and *Behold a Pale Farce: Cyberwar, Threat Inflation, and the Malware-Industrial Complex*. Bill is the lead investigator at Below Gotham Labs.