

A Response to Tor's Founding Director

Mass Subversion Is a Reality

By Bill Blunden, July 22, 2014

In the wake of a recent article on Tor¹ your author received an e-mail from Shava Nerad, the founding executive director of the Tor Project. Putting aside certain rhetorical devices that have cropped up in this debate, like name-calling or guilt-by-association, let's examine some of Shava's points to see if we can take the conversation in a constructive direction.

Choosing Sides

For example Nerad asks me which side I'm on, commenting that my article "seems more aimed to throw fear and darkness" in a manner that discourages activism. Please allow me to clarify that my intent was to caution users against assuming a false sense of security, and from putting "all of their eggs in the Tor basket."

As things stand now, higher levels of information security require a multi-layered approach and a tool like Tor is but one potential building block. To think otherwise, that you can simply install Tor and be assured of your anonymity, is to fall into a trap. To reinforce this message, consider the recent announcement by Exodus Intelligence that it has discovered zero-day exploits in TAILS OS, a Tor-enabled operating system favored by none other than Ed Snowden. Exodus will disclose the details of the corresponding flaws "in due time." A reporter from *Forbes* offers a translation²:

"That means customers could use the vulnerability however they see fit, possibly for de-anonymising anyone a government considers a target."

Soft-Pedaling OPSEC

Nerad posits that only "lazy minded people with bad opsec [operation security]" are at risk when using Tor. And while it's true that OPSEC mistakes led to the downfall of a Tor user known as the "Dread Pirate Roberts," the guy who ran the Silk Road online black market³, the FBI employed a more sophisticated approach—one that utilized software subversion and malware implants—to identify users of a Tor hidden services site⁴.

This is a blind spot that privacy advocates are neglecting. There's a tendency to present crypto as a turn-key solution without sufficiently qualifying their privacy sales pitch with the myriad of additional operational caveats. This includes obstacles like ubiquitous closed-circuit systems, credit card trails, rogue Tor relays (which is how WikiLeaks got its start⁵), meddlesome eye witnesses, browser fingerprinting⁶, social media artifacts, compromised access points, smart phone geo-tracking, Internet cookie staining, and the god awful never-ending stream of zero-day exploits. Covering all of the bases involves training, technical acumen, ingenuity, and discipline. Even professional intelligence officers get it wrong.

Paranoia

Shava also claims that I'm being "paranoid about Tor" and that the risk of subversion is small. Yet my wariness isn't necessarily directed at the Tor project per se, but at the tools that intelligence services have at their disposal to subvert Tor. Nor is the risk of subversion trivial. The Deep State is engaged in an effort that spans an entire industry, a veritable parade of corporate collaborators and defense sector monoliths⁷.

I repeat, if Snowden's documents have proven anything it's that the skeptical posture of cynics like Cryptome's John Young has been right on the money. In the NSA's own internal documents, where officials feel relaxed enough to indulge in candid discussions, the spies at the NSA admit that their goal is to undermine security and privacy across the Internet⁸. It isn't hyperbole. The nature of the risk which NSA efforts represent isn't a product of threat inflation. We're not in angels-dancing-on-the-heads-of-a-pin territory. The types of subversion techniques being deployed in the field (CIPAV, QUANTUM, FOX ACID, TURBINE, and so on) are concrete and part of the public record.

As described at length in my previous essay, hard evidence demonstrates that Tor attracts the attention of the NSA. Once more NSA spies have stated that they would actually prefer that people *keep using the technology* because they've developed the means to thwart it. The new head of the NSA, Michael S. Rogers has stated as much. This is the Deep State's way forward, mass offensive subversion⁹:

"Without referring directly to a secret N.S.A. program to place 'implants' on computer networks around the world, so American officials could see attacks in the making, he said in his written answer that the United States could make it clear that it knows where attacks are coming from and is prepared to retaliate."

The Pentagon plans to triple the number of cyber forces to 6,000 over the next couple of years, spending billions on the development of offensive weaponry¹⁰. Cyber and drones are both growth areas despite cutbacks in other parts of the Pentagon's budget.

The Nature of Cyber-Insecurity

The depiction of cryptography as a cure-all obscures a vital message which is being drowned out. While there are technical and economic factors at play, ultimately the problem of cyber insecurity is anchored in political considerations. As Karl Polyanyi observed there is no such thing as a *free market*. Markets exist as a result of government institutions and the ground rules that they establish. The same dynamic exists with regard to cyber security. Sloppy engineering and mass subversion, both of which enable the Deep State's global panopticon, transpire as a result of official policy. Top-down security for the 1% undermines society's collective security on behalf of "total population control."¹¹ Changing this will require the body politic to snap its eyes open and confront the crisis of state capture.

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.

End Notes

¹ Bill Blunden, "The NSA Wants You to Trust Tor, Should You?," *Counterpunch*, Weekend Edition July 18-20, 2014, <http://www.counterpunch.org/2014/07/18/the-nsa-wants-you-to-trust-tor-should-you/print>

² Thomas Brewster, "Exploit Dealer: Snowden's Favourite OS Tails Has Zero-Day Vulnerabilities Lurking Inside," *Forbes*, July 21, 2014, <http://www.forbes.com/sites/thomasbrewster/2014/07/21/exploit-dealer-snowdens-favourite-os-tails-has-zero-day-vulnerabilities-lurking-inside/>

³ Megan Neal, "Tor Says It's as Secure as Ever Despite the Silk Road Bust," *Vice*, October 3, 2013, <http://motherboard.vice.com/blog/tor-says-its-as-secure-as-ever-despite-the-silk-road-bust>

⁴ Kevin Poulsen, "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack," *Wired*, September 13, 2013, <http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/>

⁵ Kim Zetter, "WikiLeaks Was Launched With Documents Intercepted From Tor," *Wired*, June 1, 2010, <http://www.wired.com/2010/06/wikileaks-documents/>

⁶ Julia Angwin, "Meet the Online Tracking Device That is Virtually Impossible to Block," *ProPublica*, July 21, 2014, <http://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block>

⁷ Michael Riley, "U.S. Agencies Said to Swap Data With Thousands of Firms," *Bloomberg*, June 15, 2013, <http://www.bloomberg.com/news/print/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html>

⁸ James Ball, Julian Borger, and Glenn Greenwald, "Revealed: how US and UK spy agencies defeat internet privacy and security," *Guardian*, September 5, 2013, <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>

⁹ David E. Sanger, "N.S.A. Nominee Promotes Cyberwar Units," *New York Times*, March 11, 2014, <http://www.nytimes.com/2014/03/12/world/europe/nsa-nominee-reports-cyberattacks-on-ukraine-government.html>

¹⁰ David Sanger, "U.S. Tries Candor to Assure China on Cyberattacks," *New York Times*, April 6, 2014, <http://www.nytimes.com/2014/04/07/world/us-tries-candor-to-assure-china-on-cyberattacks.html>

¹¹ Anthony Loewenstein, "The ultimate goal of the NSA is total population control," *Guardian*, July 10, 2014, <http://www.theguardian.com/commentisfree/2014/jul/11/the-ultimate-goal-of-the-nsa-is-total-population-control>