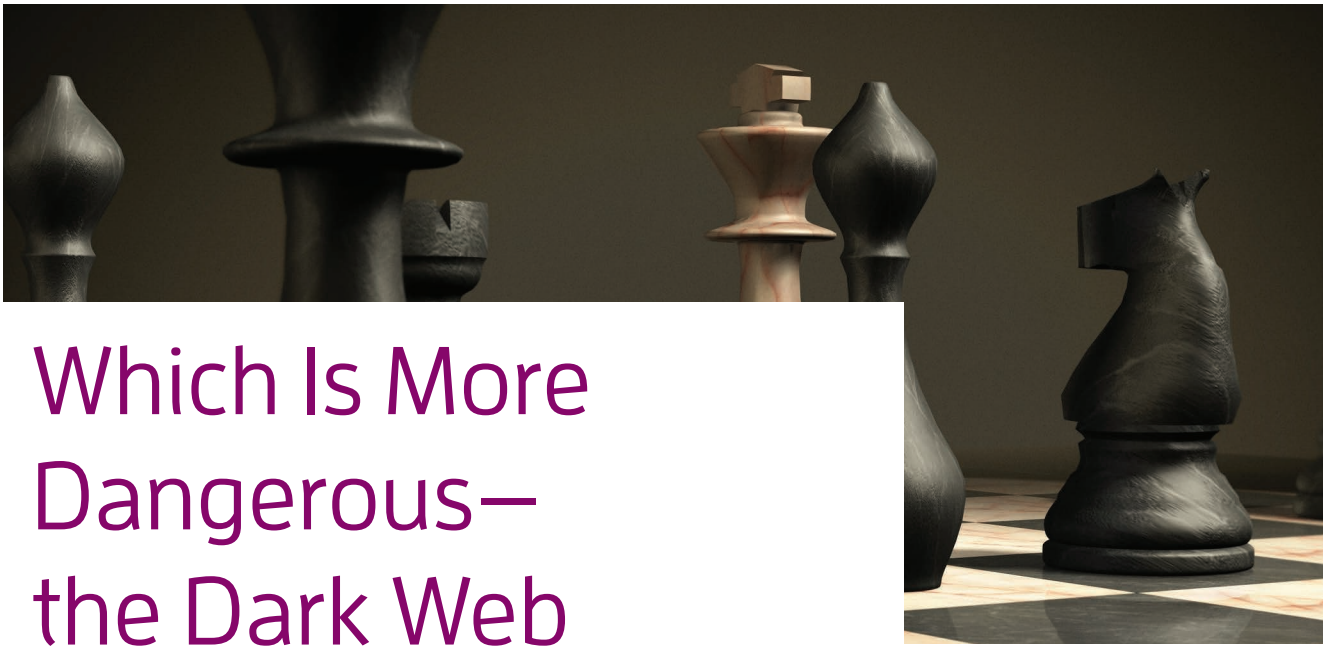

Which Is More Dangerous—the Dark Web or the Deep State?

Hal Berghel, University of Nevada, Las Vegas

Much has been made of the dark web's dangers, but democracy has more to fear from Citizens United *and the global surveillance industry than Silk Road or Tor.*

A lot has been written of late about the deep web and the dark web—including a recent article in *Computer*.[1] These terms are sometimes used interchangeably, although they're very different things. Such confusion is understandable given that the terms' meanings have morphed over time. However, the distinction between them is important because in some circles the dark web has taken on ominous overtones. Here we shall consider whether this bad reputation is really deserved.

THE DEEP WEB

The deep web is so called because it lies below the surface of "the web." In simple terms, the visible web is a collection of Internet resources that are accessible through HTTP and other compatible protocols and indexed by search engines. Such indexing is typically carried out by web spiders/crawlers that, as with Google's PageRank algorithm, identify and organize HTML hyperlinks by associating them with a measure of importance, relevance, or value.

The deep web also contains HTTP resources, but the hyperlinks aren't indexable for various reasons: the data to which they link is behind a paywall or otherwise protected site, in an unreadable format, of insufficient interest to merit indexing, part of an isolated private network, embedded in a database or data repository and only extractible by query, or dynamically generated by a networked program. Examples include information in government databases and court records, library holdings and special collections, online reference sources like encyclopedias and dictionaries, archival records such as the Human Genome Database, special-purpose directories and listings, and organizations' private or internal data resources.

Not all content on the deep web, which is an order of magnitude larger than the web, is intentionally hidden or protected—it just isn't indexed by major search

0018-9162/17/$33.00 © 2017 IEEE

EDITOR **HAL BERGHEL**
University of Nevada, Las Vegas; hlb@computer.org

engines. As Michael Bergman explains, "Searching on the Internet today can be compared to dragging a net across the surface of the ocean. While a great deal may be caught in the net, there is still a wealth of information that is deep, and therefore, missed. The reason is simple: Most of the web's information is buried far down on dynamically generated sites, and standard search engines never find it."[2]

It was obvious by the 1990s that the deep web held valuable information if one could just find it. Attempts to develop crawlers and search engines to harvest this data have met with mixed results. Of several commercial efforts started in the early 2000s—including DeepPeep, Intute, and Scirus—only Deep Web Technologies (www.deepwebtech.com) remains active. To enable searches of data from websites that change or close down, the Wayback Machine (web.archive.org), launched in 2001, archives all web content (currently more than 16 petabytes).

THE DARK WEB

Some claim the dark web is a subset of the deep web, but that's misleading. They're different by both design and purpose, and just coincidentally share Internet protocols. The deep web's invisibility is a result of its inaccessibility by search engines; its resources are contingently but not necessarily unlocatable. The dark web, in contrast, is designed to be concealed from search engines and casual web users; it's accessible only through anonymity-preserving networks that use onion routing such as Tor (www.torproject.org) and I2P (geti2p.net). These are genuinely hidden services as opposed to anonymizing, encrypted peer-to-peer file-sharing services such as Freenet (freenetproject.org) and GNUnet (gnunet.org). For those interested in more detail about anonymity, visit the Free Haven Project (www.freehaven.net).

The common denominator of dark web services is that their location or network content, or both, are hidden by design from search engines and browsers that serve the surface web such as Firefox and Chrome. These services are designated by the top-level .onion domain, whose name derives from the use of successive layers of encryption between each node or contact point in the network. Layered encryption enables only endpoints to read a message; the intermediary nodes only see the adjacent IP addresses, not that of the source or destination. The messaging can thus be thought of as a transmission chain where only adjacent links are self-revealing. (For more technical details on the most widely used onion router, Tor, visit www.torproject.org/docs/hidden-services.html.en or watch the video at media.ccc.de//32c3-7322-tor_onion_services_more_useful_than_you_think; I2P uses a variation of onion routing called garlic routing; geti2p.net/en/docs/how/garlic-routing.)

The motivation behind the dark web was complete anonymization of information exchange on the Internet: anonymization of senders and servers along with complete message encryption.[3] To achieve this, the Tor Project created a network infrastructure—now consisting of approximately 10,000 independent relays—that provides an encrypted circuit through which all traffic is routed (www.torproject.org/about/overview.html.en). This both obfuscates the random connection pathways as well as keeps the message in an encrypted tunnel. Intentional beneficiaries of the .onion framework include whistleblower repositories like WikiLeaks, WildLeaks, GlobalLeaks, and SecureDrop, all of which provide anonymity to sources and dissidents; social networking sites like Facebook and activist sites like Riseup to provide user anonymity and prevent interloping; and anonymous chat services like Ricochet. Unintentional beneficiaries are individuals and organizations that seek to conceal illicit activity. It's this latter group that has drawn negative attention to the dark web.

Criminals and deviants are naturally attracted to anonymizing services, just as they are to pool halls, crowded subways, and public restrooms, so socially unredeeming uses of the dark web are to be expected. While reports of such activity often have an alarmist tone,[4] my response is "that's true, but so what." Illegal or antisocial behavior is technology-indiscriminate. Criminals will select technology opportunistically, and their use of it in most cases says nothing about the technology itself. Anonymizing services aren't "bad faith" technologies.[5]

Too much has been made of the connection between the darker regions of cyberspace and crime. What makes the dark web useful for criminals also applies to whistleblowers and activists: complete anonymity at the transport layer. It was specifically designed by and for people who feared persecution or prosecution for their exercise of free speech. Associating the dark web with snuff films, necrophilia, child porn, illegal drug sales, terrorism, contract killing, and the like is a scare tactic used by the political elite to delegitimize the service and the spirit of individual sovereignty that inspires it. Telephony is no less guilty of such incidental alignment.

Rest assured that the ephemerality of any particular hidden service will be proportional to the deep state's interest in it, and rapid turnover will be the rule rather than the exception. As we shall see, law enforcement agencies are leading the pack in hacking these hidden services.[6]

SILK ROAD

The recent federal government investigation of the black-market site Silk Road and aggressive prosecution of its founder and operator, Ross William Ulbricht (aka Dread Pirate Roberts), illustrates the controlling elite's hysteria over the dark web. Built on Tor and bitcoin technology, Silk Road allegedly accounted for approximately $1.2 billion in sales to 960,000 customers from 2011 to 2013, producing $4 million in profit for Ulbricht. According to the 2014 grand jury indictment (www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/US%20v.%20Ross%20Ulbricht%20Indictment.pdf), he used the site to facilitate the sale or transfer of illegal drugs and other contraband, engaged in money laundering, and participated in a murder-for-hire scheme (this latter charge was ultimately dropped but retained as an "uncharged crime" in case the jury needed additional motivation to convict).

In the broader context of financial and drug crimes, Silk Road was a minor player—in 2010, expenditures on illicit drugs in the US totaled some $109 billion (obamawhitehouse.archives.gov/sites/default/files/ondcp/policy-and-research/2015_data_supplement_final.pdf). What made it and subsequent dark web marketplaces a prominent target was continuous pressure from politicians like New York Senator Chuck Schumer[7] and the fact that the prosecution of Ulbricht had no downsides for the investigating agencies and the politicians that encouraged them. Pursuing the international bankers who support more expansive transnational money laundering, or tax cheats who maintain offshore havens, can produce serious blowback from wealthy people with political teeth. Silk Road's supporters, excluding those who used it as just another illegal bazaar, were primarily libertarians and champions of individual sovereignty who together could exude at best a whimper of protest. "The dark web" was an alluring media topic that would gain notoriety for the agencies and politicians involved, and Ulbricht had no political clout—an ideal formula for becoming the target de jour.

The aggressive prosecution of Ulbricht and severity of his sentence—life imprisonment without the possibility of parole—is well documented (see, for example, Alex Winter's documentary *Deep State*). At best, the case is likely to remain an undistinguished entry in legal annals; at worst, it might be overturned by the Supreme Court and join the ranks of *Buck v. Bell* and *Miranda v. Arizona* as hallmarks of judicial overzealousness. In any event, it had no deterrent effect. In fact, Silk Road was soon followed by other cryptocurrency exchanges for anonymous online transactions including Silk Road 2.0, Atlantis, and Agora, introducing a new cat-and-mouse game for intelligence and law enforcement agencies to solidify their budgets. The dark web has its own online newsletter for those who like to keep score (darkwebnews.com).

Two aspects of the case are particularly noteworthy. One relates to constitutional law: whether the FBI violated Ulbricht's Fourth Amendment right against illegal search and seizure when it hacked into a .onion server in Iceland thought to be connected to Silk Road without a warrant.[8] For computing professionals, however, the far more interesting story involves the account of the FBI agents who hacked into this server during the investigation and claimed that its IP address was leaked "from the user login interface." According to agent Christopher Tarbell:

> *Upon examining the individual packets of data being sent back from the website, we noticed that the headers of some of the packets reflected a certain IP address not associated with any known Tor node as the source of the packets. This IP address (the "Subject IP Address") was the only non-Tor source IP address reflected in the traffic we examined. The Subject IP Address caught our attention because, if a hidden service is properly configured to work on Tor, the source IP address of traffic sent from the hidden service should appear as the IP address of a Tor node, as opposed to the true IP address of the hidden service, which Tor is designed to conceal.* When I typed the Subject IP Address into an ordinary (non-Tor) web browser, a part of the Silk Road login screen (the CAPTCHA prompt) appeared. *Based on my training and experience, this indicated that the Subject IP Address was the IP address of the SR Server, and that it was "leaking" from the SR Server because the computer code underlying the login interface was not properly configured at the time to work on Tor (www.unitedstatescourts.org/federal/nysd/422824/57-0.html#;* emphasis added*).*

Misconfigured servers that don't set up the IP tables correctly to ensure that all traffic is routed through Tor tunnels, faulty Tor installations, and flawed operational procedures can certainly produce "leaks" that breach the veil of anonymity, but this has been known to the Tor community for over a decade[9] and digital antidotes are well established. It's exceedingly difficult to imagine how an alleged billion-dollar business like Silk Road didn't have the wherewithal to hire someone to set up the servers correctly according to Tor instructions and server administration best practices. Given that probably hundreds of thousands of computing professionals worldwide know how to do this, Tarbell's account doesn't pass my smell test.

Tarbell claims to have used this data to legally obtain subscriber information on, and traffic data from, the server from Icelandic authorities, which ultimately led to Ulbricht's prosecution:

> *After Ulbricht's arrest, evidence was discovered on his computer*

reflecting that IP address leaks were a recurring problem for him. In a file containing a log Ulbricht kept of his actions in administering the Silk Road website, there are multiple entries discussing various leaks of IP addresses of servers involved in running the Silk Road website and the steps he took to remedy them. For example, a March 25, 2013 entry states that the server had been "ddosd"—i.e., subjected to a distributed denial of service attack, involving flooding the server with traffic—which, Ulbricht concluded, meant "someone knew the real IP." The entry further notes that it appeared someone had "discovered the IP via a leak" and that Ulbricht "migrated to a new server" as a result. A May 3, 2013 entry similarly states: "Leaked IP of webserver to public and had to redeploy/shred [the server]." Another entry, from May 26, 2013, states that, as a result of changes he made to the Silk Road discussion forum, he "leaked [the] ip [address of the forum server] twice" and had to change servers.

<ALT>-FAQs

The US government took pride in its takedown of Silk Road, but the war on drugs is anything but a success. Consider some figures from the US National Drug Control Strategy's *Data Supplement 2015* (obamawhitehouse.archives.gov/sites/default/files/ondcp/policy-and-research/ 2015_data_ supplement_final.pdf).

Although illicit drug expenditures in the US dropped from $154 billion in 1988 to $109 billion in 2010, during the same period the street price of cocaine dropped from $269 to $186 per gram, so each dollar spent went 30 percent farther at the user level. Between 1981 and 2012, the street price dropped from $753 per gram of 41 percent purity to $186 per gram of 44 percent purity—a whopping 75 reduction in price with a 5 percent increase in purity. The figures for heroin were similar: from 1981 to 2012, the street price dropped 85 percent while the purity tripled, so the effective price dropped by 95 percent.

While the price per pop was dropping dramatically, seizures were up for most hard drugs. From 1989 to 2014, seizures of heroin increased 370 percent from 1,311 to 4,849 kg, and from 1993 to 2014, seizures of methamphetamine rose 3,500 percent from 7 to 23,431 kg. These seizures came at an enormous cost: tens of billions of dollars per year for law enforcement operations, court proceedings, and incarcerations.

In short, since President Nixon launched the war on drugs in 1971, the government has run up a tab of hundreds of billions of dollars to produce a more plentiful supply of more potent drugs at substantially lower costs than when it started. In bureaucratese, the war on drugs has justified itself by accelerating its "burn rate."

Again, this smells fishy. Assuming "the server" in question was for Silk Road, it's not unusual for hidden or controversial services to be the object of a DDoS. But it doesn't necessarily follow that there was any IP leak. And if "the server" is a support server (say, for CAPTCHA authentication), one would expect the connection to be in an encrypted VPN tunnel. Using local network traffic analysis to inspect for traffic outside Tor server ports 9050/TCP (SOCKS proxy) and 9051/TCP (control port) to confirm no anonymity-threatening IP traffic leaks would be standard policy and a rookie-level exercise for a network administrator.

Tarbell's declaration was critical to the judge's rejection of a defense motion to suppress the evidence against Ulbricht on Fourth Amendment grounds (assets.documentcloud.org/documents/1284178/238796613-silk-road-prosecution-4th-amendment.pdf), effectively derailing the defense's case.

PARALLEL CONSTRUCTION

If freshman network configuration errors like those reported by the prosecution's chief technical witness in the Silk Road case seem improbable, revelations from investigative journalists suggest another possible explanation: the server infrastructure was compromised through "parallel construction."

Parallel construction is government-speak for concealing the real source of evidence in criminal investigations by reconstructing the chain of probable cause to implicate other (even fictional) sources, ostensibly to protect classified information and those who lives might be put at risk, such as informants or undercover agents. An August 2013 expose by Reuters reporters John Shiffman and Kristina Cooke revealed that for the past two decades the NSA's Special Operations Division had been feeding warrantless surveillance data indicating potential criminal activity unrelated to national security to federal and state agencies including the DEA, IRS, DHS, FBI, and CIA.[10] According to the story, the NSA instructed law enforcement agents with whom it shared this information to practice parallel construction to hide the source from prosecutors, courts, and especially defense attorneys. (For those interested in how one three-letter agency implemented this policy, the DEA's training bulletin on parallel construction has been released under a Freedom of Information Act request.[11])

There has been no judicial or congressional oversight of this activity, which is clearly a constitutional abuse of power. As Pulitzer Prize–winning

reporter Glenn Greenwald has noted, by circumventing accepted practices for pretrial discovery and the introduction of exculpatory evidence, parallel construction constitutes a full frontal assault on the Bill of Rights and our system of justice.[12]

US courts allow lawfully obtained substitute evidence if they have determined that it doesn't diminish the strength of the defense's case. This is especially true in the case of national security. To address the problem of defendants who try to derail their prosecution with "graymail"—the threatened revelation of state secrets—Congress passed the Classified Information Procedures Act (CIPA) in 1980. CIPA is problematic because it's inherently disadvantageous to defendants: courts makes their determinations on whether to exclude allegedly classified information ex parte and in camera (read: in secret) without the defense attorneys' participation, so there's no way to hold the courts accountable for any judicial indiscretions regarding the exculpatory potential of evidence. However, even a sympathetic reading of CIPA would concede that it wasn't created to provide a means to bypass the Constitution.

Given the government's documented use of parallel construction to circumvent the rules of evidence in criminal trials, could it have been employed in the Silk Road case? Some assert that it's not only possible, but likely. Network leaks can occur for many reasons, including anomalous cookie exchanges between Tor and non-Tor services, embedded scripts that force hidden services to make contact on public networks, and poorly behaved applications (for example, JavaScript) that meander outside the proxy. As mentioned earlier, however, savvy network administrators guard against such problems. More tellingly, the Tor Project has observed implanted imposter relays that conceivably could, through a Sybil attack, capture .onion addresses or traffic timing information from inside the network.[13] Who controls these relays remains the subject of speculation, but the US government is a prime suspect.

There's some evidence that the FBI has funded research into new tricks to compromise Tor anonymity.[14] In the case of Silk Road, a client or the server could have been compromised in such a way that its MAC address, IP address, or computer ID was leaked to a recording server. The FBI has used such techniques for decades as shown by the Carnivore packet sniffer, the Magic Lantern keylogger, the Computer and Internet Protocol Address Verifier (CIPAV) data-gathering tool, and, most recently, the Magneto Trojan horse distributed through a dark web server that anonymously hosted a good portion of the Internet's child porn.[6]

Was the evidence against Ulbricht produced through lawful network forensics or parallel construction? Who knows. What's concerning is that the government has a shady past in this regard and its behavior has been less than confidence-inspiring. Truth is always the first casualty of a deep state.

The Silk Road case is a stark reminder of the government's continued effort to subvert anonymizing services. Nearly four years ago, the encrypted email service Lavabit was forced to cease operations after authorities demanded it disclose customer SSL keys.[15] Anonymity threatens authoritarianism and its exercise of control. When big and powerful government types speak of the dark web, they emphasize criminality; when technologists and civil libertarians speak of it, the emphasis is on free expression. The difference can be explained ideologically.

To answer the question posed by the title of this article, the deep state poses a far greater danger than the dark web. Democracy has more to fear from *Citizens United* and the global surveillance industry than Silk Road or Tor. In fact, it's the visible web, not its invisible counterpart, that produces such social distortions as fake news, alt-facts, post-truths, mimetics, public deception, message distortion, and rumor propagation.[16,17] The point to bear in mind is that the deep state, to preserve its own invisibility and to protect its power base, is necessarily partisan and fickle, as recent national security advisor Michael Flynn found out to his cost. As for the technical aspects of this issue, some of you are experts in the area. Speak out. Many of my fears about parallel construction would be assuaged if impartial technologists enlarged the discussion and helped frame the narrative. Read the Silk Road court transcripts linked above and see if they pass *your* smell test.

REFERENCES

1. G. Hurlburt, "Shining Light on the Dark Web," *Computer*, vol. 50, no. 4, 2017, pp. 100–105.
2. M. Bergman, "The Deep Web: Surfacing Hidden Value," *J. Electronic Publishing*, vol. 7, no. 1, 2001; quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main.
3. A. Biryukov et al., "Content and Popularity Analysis of Tor Hidden Services," *Proc. IEEE 34th Int'l Conf. Distributed Computing Systems Workshops* (ICDCSW 14), 2014, pp. 188–193.
4. G. Owen and N. Savage, "The Tor Dark Net," Global Commission on Internet Governance paper no. 20, Centre for Int'l Governance Innovation/Royal Inst. Int'l Affairs, Sept. 2015; ourinternet-files.s3.amazonaws.com/publications/no20_0.pdf.
5. H. Berghel, "Bad Faith Technology," *Cutter IT J.*, vol. 29, no. 5, 2016, pp. 20–24.
6. K. Poulsen, "Feds Are Suspects in New Malware That Attacks Tor Anonymity, *Wired*, 5 Aug. 2013; www.wired.com/2013/08/freedom-hosting.
7. A. Greenberg, "NY Senator Calls for Renewed Crackdown on Dark Web Drug Sales," *Wired*, 27 Oct. 2014; www.wired.com/2014/10/schumer-crackdown-on-dark-web-drug-sales.
8. A. Greenberg, "Judge Rejects Defense

That FBI Illegally Hacked Silk Road—on a Technicality," *Wired*, 10 Oct. 2014; www.wired.com/2014/10/silk-road-judge-technicality.
9. "Tor and the Silk Road Takedown," blog, The Tor Project, 2 Oct. 2013; blog.torproject.org/blog/tor-and-silk-road-takedown.
10. J. Shiffman and K. Cooke, "U.S. Directs Agents to Cover up Program Used to Investigate Americans," Reuters, 5 Aug. 2013; www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805.
11. M. Masnick, "Parallel Construction Revealed: How the DEA Is Trained to Launder Classified Surveillance Info," *Techdirt*, 3 Feb. 2014; www.techdirt.com/articles/20140203/11143926078/parallel-construction-revealed-how-dea-is-trained-to-launder-classified-surveillance-info.shtml.
12. A. Goodman, "Glenn Greenwald on How Secretive DEA Unit Illegally Spies on Americans, Covers up Actions," *Democracy Now!*, 5 Aug. 2013; www.democracynow.org/2013/8/5/glenn_greenwald_on_how_secretive_dea_unit_illegally_spies_on_americans_covers_up_actions.
13. "Tor Security Advisory: 'Relay Early' Traffic Confirmation Attack," blog, The Tor Project, 30 July 2014; blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack.
14. A. Greenberg, "Tor Says Feds Paid Carnegie Mellon $1M to Help Unmask Users," *Wired*, 11 Nov. 2015; www.wired.com/2015/11/tor-says-feds-paid-carnegie-mellon-1m-to-help-unmask-users.
15. K. Poulsen, "Edward Snowden's Email Provider Shuts Down amid Secret Court Battle," *Wired*, 8 Aug. 2013; www.wired.com/2013/08/lavabit-snowden.
16. H. Berghel, "Alt-News and Post-Truths in the 'Fake News' Era," *Computer*, vol. 50, no. 4, 2017, pp. 110–114.
17. K. Viner, "How Technology Disrupted the Truth," *The Guardian*, 12 July 2016; www.theguardian.com/media/2016/jul/12/how-technology-disrupted-the-truth.

HAL BERGHEL is an IEEE and ACM Fellow and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.