INSIDE THE DARK WEB

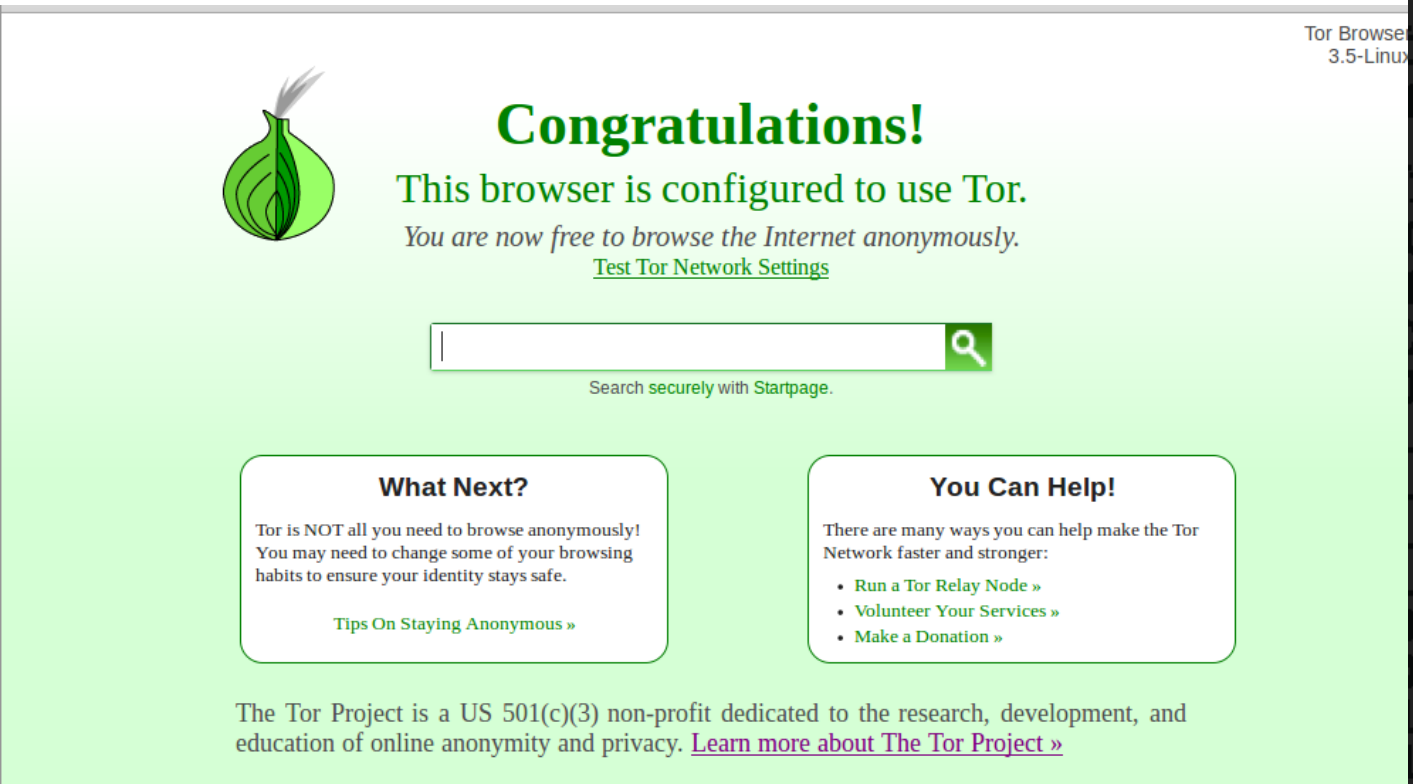
The Dark Web is supposed to be the Internet's seedy back alley, where everything from drugs to assassins to child pornography can be obtained for a price. But the real Dark Web is a lot more complicated, and it's growing—because we need it more than ever. **BY MAX EDDY**

If our popular culture is to be believed, most people assume there's a place online where the worst of the headlines you read about drugs, money laundering, murder for hire, and vast child pornography rings are born. It's called many things, though "Dark Web" is the most dramatic.

Although it's true that this Dark Web exists, it's much larger and more diverse than merely these illegal activities. What's more, the same technology that makes it possible for such marketplaces to operate in secret is also protecting political dissidents overseas and hiding everyday Internet traffic from surveillance. It may be that this digital back alley is the path toward a more secure Internet.

THE WORLD OF WEBS

Most people take the Internet at face value, but what most of us interact with is really just a slice of the information available called the Surface Web. To get to the Dark Web we have to go deeper, away from the world of standard Web addresses and onto the anonymity network called Tor. When you click on a link in Google, you're connected with the target information fairly directly. Someone accessing the same site while connected through Tor would have their request bounced randomly through volunteer computers called nodes before exiting Tor and arriving at the site, making their online movements much harder to track.

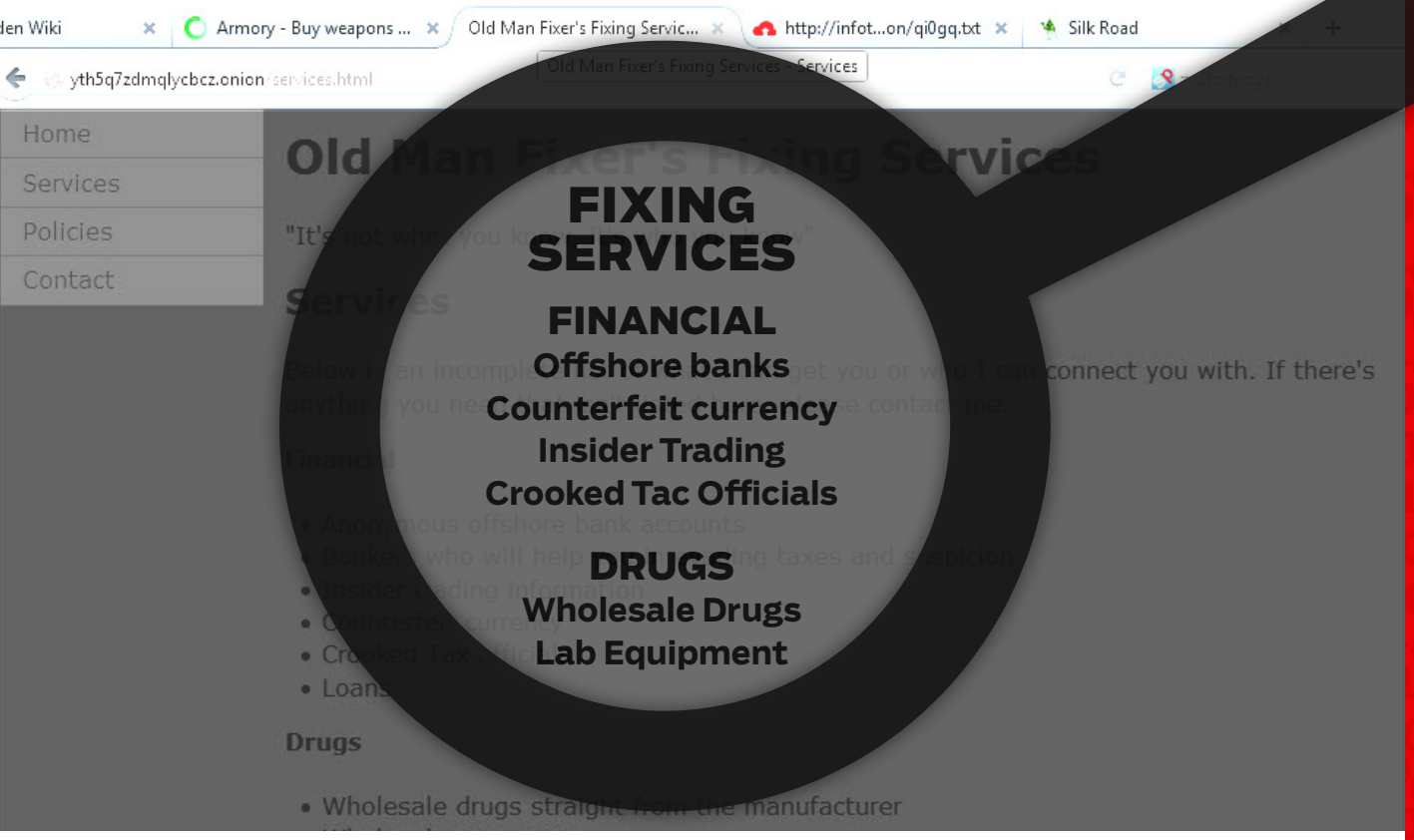


THE SURFACE WEB

The Surface Web is the Internet we use every day. It consists of publicly accessible pages that can be accessed from a mainstream Web browser and are connected to other pages by links.

THE DEEP WEB

On the other hand, the Deep Web consists of websites that are not searchable or connected to sites that have been indexed by search engines. Google wasn't born omniscient and omnipresent. Its success is built off of the work of its spiders: automated programs that follow all the links on a webpage, building a complete picture of the Surface Web we consider the Internet. Webpages without links to the larger Internet get passed over and aren't indexed. Most of this Deep Web material is innocuous. For example, if you search a database attached to the public Web, the website will return a unique URL that has no inward-facing links. This page is part of the Deep Web.



Tor can be used to access sites on the Surface Web, but servers can also be assigned special addresses that can only be reached within the Tor network. These are called hidden services, and when we're talking about the Dark Web, we're mostly talking about these sites. Of course, there are other services to hide online activity and even host hidden websites, but Tor is perhaps the most well known and well established.

Surprisingly, the onion routing protocol that powers Tor was originally developed by the U.S. Department of Defense. Tor is now a volunteer-run nonprofit operation, but it makes no secret of its roots. A page on Tor's history reads: "[Onion routing] was originally developed with the U.S. Navy in mind, for the primary purpose of protecting government communications. Today, it is used every day for a wide variety of purposes by normal people, the military, journalists, law enforcement officers, activists, and many others."

Among those "others" are some of the Internet's ne'er-do-wells. Some malware authors, for example, have used Tor to hide communication with their creations. The anonymization of the Tor network is also attractive for people carrying out illicit online activities, such as selling and purchasing illegal merchandise. When you read about illegal websites selling drugs, weapons, and child pornography, it's a safe bet that those websites are hosted within Tor.

THE DARK WEB

The Dark Web requires special technology to access. Generally, when people talk about the Dark Web, they mean websites hosted inside the Tor network. Because these sites are hidden and their visitors' traffic is not easily traced, locating the physical location of their servers is very difficult. Also, because visitor traffic is routed through Tor, it's very difficult for law enforcement or telecoms to prevent users from accessing these hidden services.

THE BAD DARK WEB

"A few years ago, if you tried to browse the Internet through Tor, it would be a very slow and very painful experience," says Kaspersky researcher Stefan Tanase. As is often the case with digital security experts, speaking with Tanase and his fellow Kaspersky associate Sergey Lozhkin required a phone call from the *PC Magazine* office in New York to Bucharest and Moscow. That part of the world produces huge amounts of spam, malware, and cyberattacks, but just so happens to also produce some of the best minds in digital security in almost equal proportions.

Tanase and Lozhkin have a unique perspective on the hidden ecosystem of the Dark Web. Although the Surface Web has search engines to index its contents and connections, there was no map of the Dark Web on Tor. Tanase and Lozhkin set out to create one.

"We started with a list of known hidden websites hosted within [Tor], so we've been crawling, accessing these websites and looking for links to other websites," says Tanase, describing their process of mimicking Google's approach in mapping the Surface Web. Though the number of hidden services on Tor is relatively small compared with the Internet at large (Tanase describes it as containing "thousands but not tens of thousands of websites"), the researchers say the Dark Web will remain a bit of a mystery, even after their explorations.

"There are a number of sites that go offline every day and some that are available for months or weeks," says Lozhkin. "In the next few hours, the sites with the same content can be available on a completely different address." The relative difficulty in simply finding hidden services, in addition to the anonymity provided by Tor, feeds the Dark Web's aura of mystery. Not to mention the exclusivity of its illegal offerings.

But even that's changing. These days, you can download a specially modified Web browser from Tor that requires little to no technical know-how to use. The

MAPPING THE DARK WEB
Kaspersky researchers Stefan Tanase (top) and Sergey Lozhkin set out to index (or map) the Dark Web, but thanks to its secretive, transient nature, much of it will always remain a mystery.

Dark Web is nearing drag-and-drop simplicity. There's even an officially supported Android client you can use to access Tor on the go. Using tactics similar to those of the Kaspersky researchers, search engines have begun to appear within the Dark Web over the last year or two. "They're like Google," says Lozhkin. "Search whatever you like. I dunno, malware, drugs, stuff like this, and get links right away."

This is what most people imagine the Dark Web to be: an electronic black market where anything is available. And the researchers I spoke with confirm that all that—and worse—is available on websites hidden within Tor. Drugs, guns, and even rhinoceros horn are for sale on the Dark Web, but those still require the physical exchange of goods. The Dark Web is, without question, far more dangerous when it comes to easily distributing illegal digital material, such as child pornography. In 2011, the Dark Web child pornography marketplace Lolita City made headlines when activists from Anonymous knocked the site offline and released information about its patrons. At the time, it was reported that the site hosted more than 100GB of sexual images of children as young as toddlers. When Eric Eoin Marques, the operator of a Tor-based webhosting service called Freedom Hosting (which hosted Lolita City and was also attacked by Anonymous), was arrested in 2013, the Irish newspaper *The Independent* wrote that Marques' customers used the service to share "graphic images [depicting] the rape and torture of prepubescent children."

HOW CAN YOU FIGHT WHAT YOU CAN'T SEE?

Andrew Conway works for Cloudmark, an antispam company that serves more than 120 major communications providers including AT&T, Verizon, Swisscom, Comcast, Cox, and NTT. When I met with Conway, he was sporting a denim outfit and white

WHAT IS A TOR HIDDEN SERVICE?

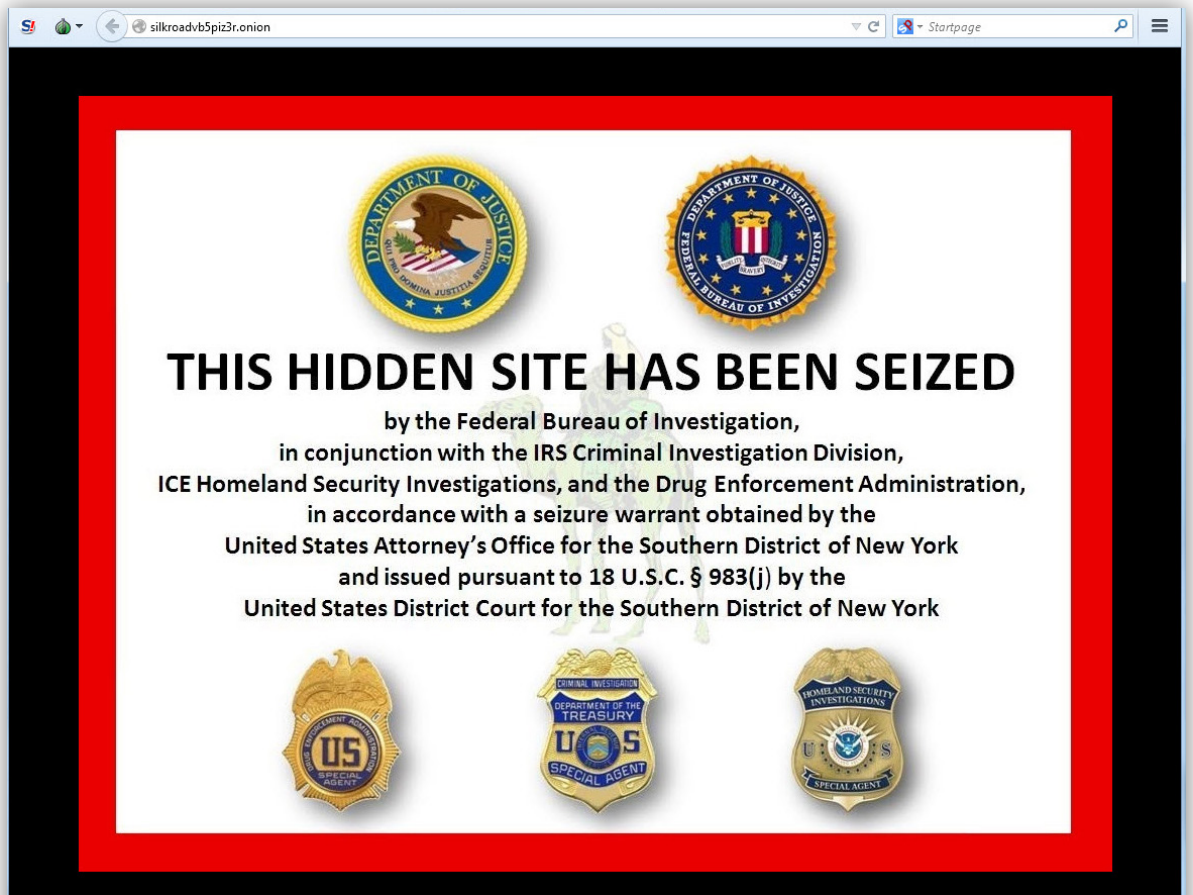
Users can also host websites on servers on the Tor network and provide hidden services; that is, websites that can only be accessed from within Tor. Hidden services are sometimes used to provide illegal merchandise and services because the physical location of the servers is difficult to ascertain.

leather vest, complete with bolo tie. It's an outfit befitting his job, where he and his coworkers go toe-to-toe technologically with the criminal networks behind spam operations. He understands criminal networks, and how money flows through these groups.

Though he was dressed like a cowboy, Conway spoke with a gentle British accent. We discussed how the U.S. law enforcement managed to take down the black market website Silk Road. It was the embodiment of the Dark Web myth: a place where a few bitcoins could get you a fake ID, heroin, or even (allegedly) an assassin.

Silk Road, which was hosted as a hidden service within Tor, vanished from the Internet in October 2013, and its alleged operator, Ross William Ulbricht (who operated the site under the name The Dread Pirate Roberts), was arrested in short order. It's surprising, because the site appeared bulletproof for so long. Conway isn't so surprised the site has vanished. "There are many nation-states or individuals who have the resources to bring Tor down for a limited period, and quite a few who could do it permanently," he says. "Eventually one of them will get annoyed enough by something that Tor is doing and take action against it."

Lozhkin says that in the case of Silk Road and its successor, Silk Road 2, law enforcement probably didn't find a secret weakness within Tor. "They didn't do



CASH ON THE DARK WEB

Dark Web sites can facilitate the exchange of goods, but they're only marketplaces. The actual medium of exchange is increasingly Bitcoin. Instead of being issued by a government and processed by banks, Bitcoin is a peer-to-peer digital currency that uses cryptographic exchanges to verify transactions—this makes it appealing for illegal transactions.

But the absence of a central authority or oversight has its own problems. Bitcoin banks and exchanges have struggled with technical issues and theft (as in the case of Mt. Gox), and the currency has gone through several periods of intense volatility. In 2013, former Federal Reserve Chairman Alan Greenspan described Bitcoin as a speculative bubble.

Many sites, including those on the Surface Web, have begun to accept Bitcoin alongside cash transactions. As of this writing, the current exchange rate in U.S. dollars is $233.39 for every Bitcoin.

anything with the Tor network or architecture," he says. Rather, the Feds likely got what they needed from undercover agents.

Or maybe loose lips sank Silk Road's ship. The owners of Tor nodes, says Lozhkin, sometimes chat on hidden forums. "These guys, they like to talk, and what they talk can be used against them," he says. It's worth noting that, as of this writing, another spinoff of Silk Road called Silk Road Reloaded has reportedly appeared on an anonymous network called I2P.

"All the Tor nodes are simple websites, and every website can have a vulnerability," Lozhkin explains. "If the law enforcement find a [vulnerability] they can easily exploit it to get inside the server. If you get access to the server side you can easily identify its location."

In the case of Silk Road, sloppy mistakes almost certainly played a part. Tanase says Silk Road's operator was managing the server from an Internet café and connecting to that server directly, not through Tor. Ironically, these are the kind of simple mistakes that criminals frequently exploit in order to attack companies and individuals.

However law enforcement identifies the server hosting hidden, law-breaking websites, the next course of action is to physically take control of the server. "They usually get the warrant for monitoring the server first and try to extract the information from the server when it's still live to track the criminals," says Tanase. Does this mean that at least some percentage of illegal hidden websites is being operated by law enforcement? "Nobody knows," he says. "I'm always wondering if they're actually sellers [running the sites] or if it's a trap set up by law enforcement.

"But this is why services like Silk Road become so popular; they're like eBay of the [Dark] Web, and offer users the chance to give reputation to each other," Tanase continues. "Law enforcement has to work quite a lot of infiltrate these markets and achieve reputation."

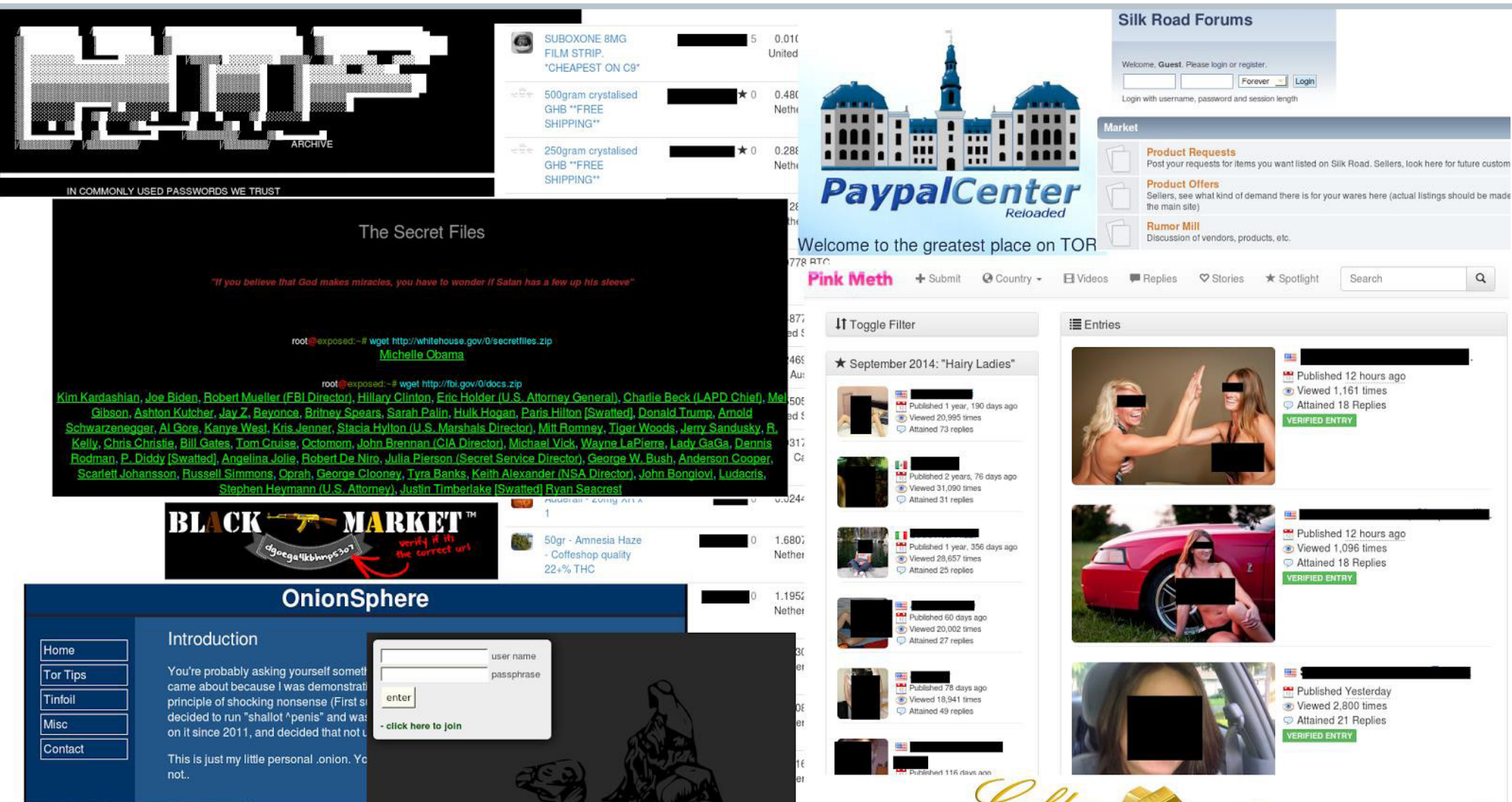
Of course, there are far more exotic attacks to use to expose the machines serving up hidden websites within Tor. Tanase says that if a single entity were in control of the bulk of the Tor nodes, they could trace traffic through the whole system. “No malicious actor or agency can do this, but the more nodes you can monitor, the greater the chances,” says Tanase. As of this writing, there appear to be approximately 6,500 Tor nodes.

Tanase and Lozhkin describe an even more audacious scheme to locate hidden services on Tor. It would require selecting all the IP addresses in a certain range—say, all the IP addresses within a country—and methodically flooding them with fake requests in a massive distributed denial of service (DDoS) attack. While that’s going on, the attackers would carefully monitor the status of a hidden Tor website. When it went down or experienced a noticeable spike in traffic, they’d know they’ve hit on the right group of IP addresses.

All the attacker would need is some hint as to where the server might be located in order to begin the attack. That’s exactly the kind of information that could be obtained from an undercover agent, or from stalking hidden forums where Deep Web operators chat.

Pulling off attacks like this would require vast resources and the will to break into Tor. Conspiracy theorists can fill in their favorite nation-state or three-letter agency of choice. Of course, that assumes that whoever would attack Tor would allow it to survive.

To actually bring down Tor, Conway says he’d expect to see a large-scale DDoS attack against the few Tor nodes that exit back to the Surface Web. “As of



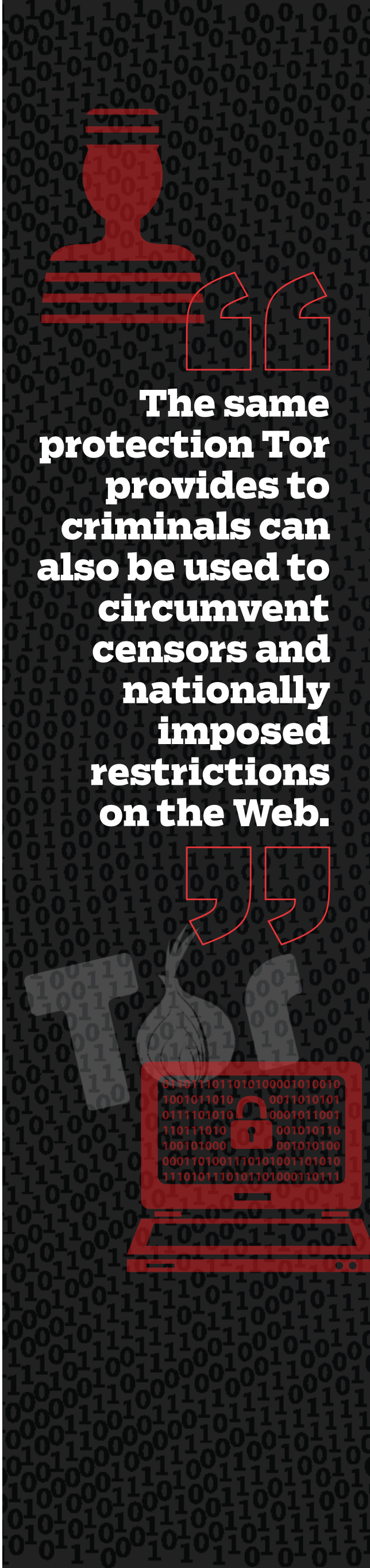
this morning there are only 1,199 of them, and many are on consumer networks," he tells me. "A DDoS attack on those IP addresses from the regular Internet, without using Tor at all, would limit the ability of Tor traffic to pass through those nodes and render the Tor network unusable."

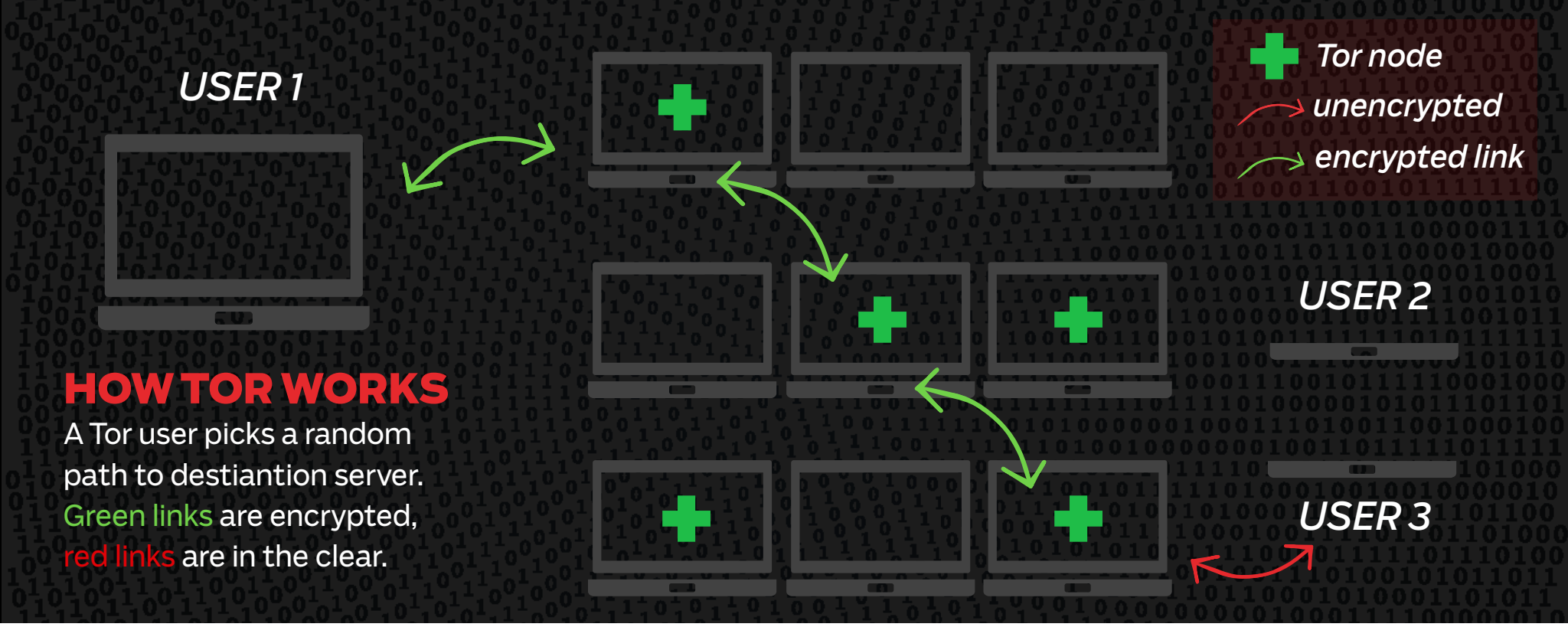
Even Tor has seemed dim on the future of hidden services. After the U.S. government seized and shuttered more than 400 websites (including Silk Road 2) in "Operation Onymus," an article appeared on the Tor blog that read, "In a way, it's even surprising that hidden services have survived so far. The attention they have received is minimal compared to their social value and compared to the size and determination of their adversaries."

THE GOOD DARK WEB

Those adversaries include law enforcement, but not always the kind that's involved in busting drug rings or prosecuting human traffickers. It's spies, the nation-states they work for, and the increasingly capable electronic expressions of force available to those states. That's because the same protection Tor provides to criminals can also be used to circumvent censors and nationally imposed restrictions on the Web.

Though it's U.S. law enforcement that most recently gutted Tor's hidden services, various branches of the federal government and DoD continue to support Tor financially. In 2014 it received funds from the U.S. Department of State Bureau of Democracy, Human Rights, and Labor, and the National Science Foundation. Previous donors include the Naval Research Laboratory and DARPA. It's clear that the U.S. government still sees value in Tor, no doubt in supporting this country's continued stated mission to promote free speech (and dissent) abroad. It's also possible that it's a handy, free, off-the-shelf tool for intelligence agents.





"One mark of human progress is the weight given to human rights," Conway tells me, citing Article 19 of the United Nations' Universal Declaration of Human Rights, which describes the right to the freedom of opinion and the expression of those opinions, as well as the right to seek and receive information. "Yet for much of the world's population, the right to seek, receive, and impart information is seriously impaired. Tor is helping to support a basic human right. Many of our basic rights can be abused, but that abuse does not justify taking the right away from everyone."

I hear much the same thing from Tanase: "You cannot ignore the good users because there's some bad users." The Dark Web, he explains, supports a surprisingly diverse ecosystem of websites. "Online stores that are selling drugs or guns, personal websites, and just simple services that are providing secure communications."

Tanase continues, "Like any technology out there, Tor is double-edged sword. It has its good parts and its worst parts. It's up to us, security researchers, to try to clean it up, right? To make sure it's only being used for good stuff."

A GNU DARK WEB

Without a doubt, 2014 was a banner year for terrifying digital security headlines. Concerns about NSA surveillance dominated public discussions for months, massive data breaches shocked and titillated the public, and the argument over net neutrality continued in a stymied U.S. Congress.

These are engineering, not political, problems for security researcher Christian Grothoff. He hopes to correct them with GNUnet, which he began in 2001 as a free-software, volunteer project to create secure peer-to-peer networking. Like Tor, it's designed with security and anonymity in mind; but unlike Tor, it does not require the underlying architecture of the Internet

(TCP/IP) to function. TCP/IP lets anyone with the know-how inspect much of users' traffic, and it relies on central authorities such as the Internet Corporation for Assigned Names and Numbers (ICANN), which manages the Domain Name System. Because GNUnet offers a secure alternative to these services, it's easy to understand why Grothoff says it could "effectively reenvision the Internet."

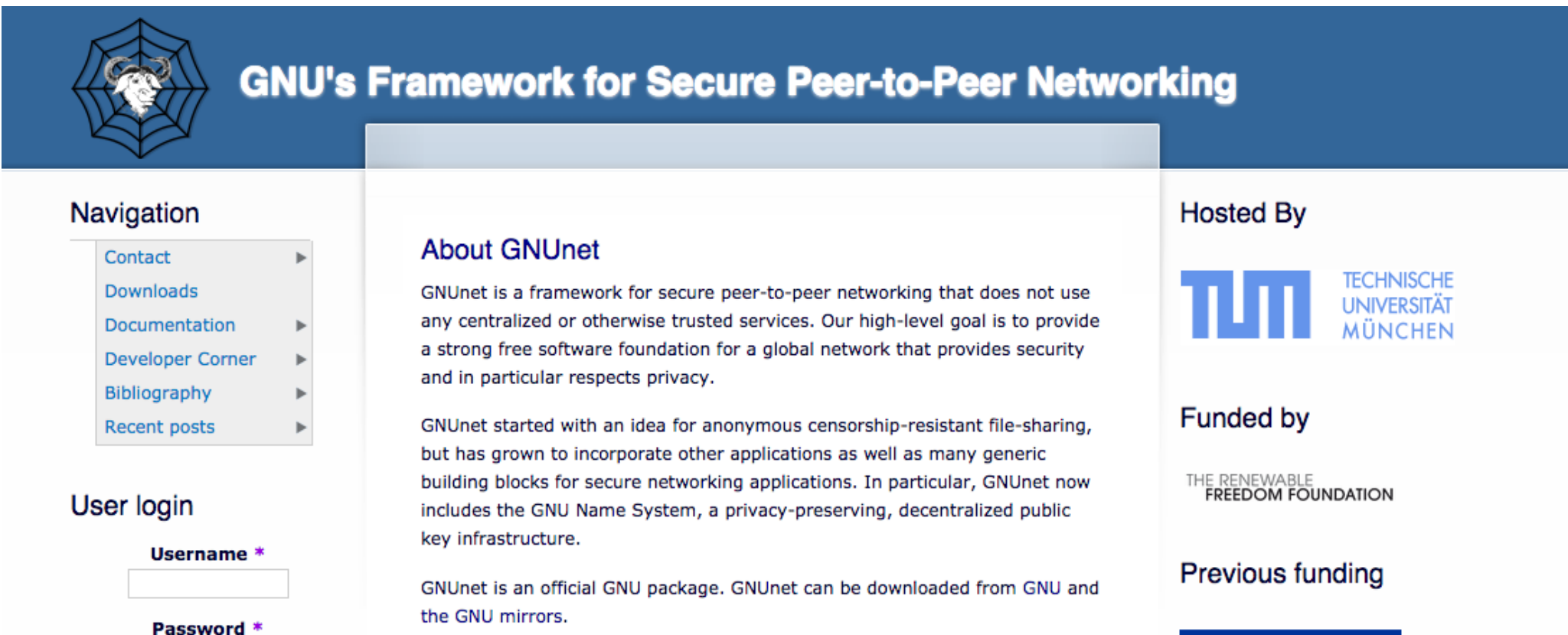
"Explain to me, why does an IP packet have to have the source IP in the packet? To route it, we only need the destination," says Grothoff. "In Tor, we can bounce it around. Or we could have new protocol where it's already encrypted."

Grothoff says GNUnet is a mesh network where individuals use privacy-preserving name resolution instead of DNS lookups for greater security without the need for central authority. By its nature, it should resist the kind of widespread surveillance the NSA has been accused of, and prevent governments from being able to segment the Internet. In other words, GNUnet is dark from the start.

"It is not enough to anonymize the access; we have to decentralize the application logic of how and where we store data," says Grothoff. For him, GNUnet is the next stage of the Internet, and he invokes the military-funded pre-Internet computer network when describing it. "Like ARPANET, except secure and for civil society."

DARK FROM THE START

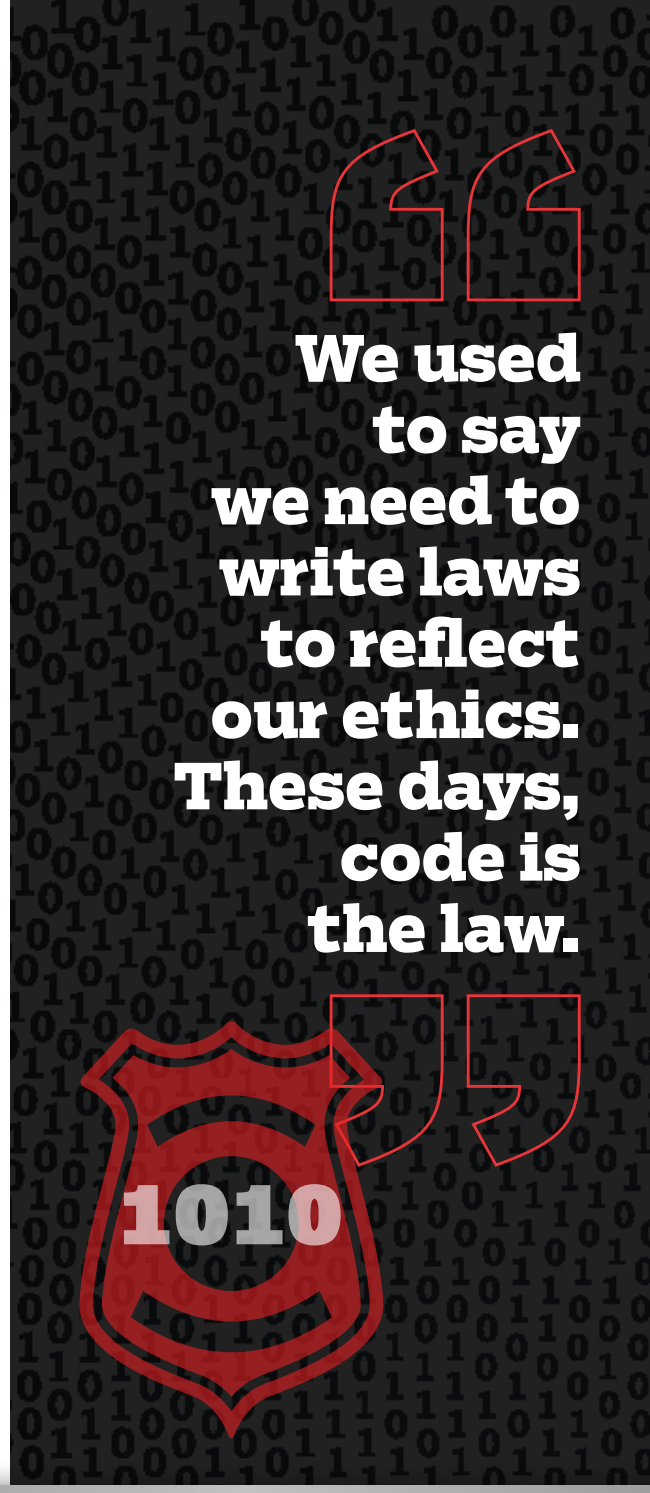
Security researcher Christian Grothoff conceived GNUnet, which is designed for security and anonymity but is not based on the same underlying TCP/IP architecture as the rest of the Internet.



Grothoff has a healthy respect for Tor, which he regards as the best tool for people with an urgent need for anonymity today. But Tor, Grothoff says, is a bolt-on solution for an Internet whose structure does not take privacy into account.

"We used to say we need to write laws to reflect our ethics," Grothoff says. "These days, code is the law. That's an old quote by now. When we write code, we should write code that is ethical, and writing code is an engineering issue.

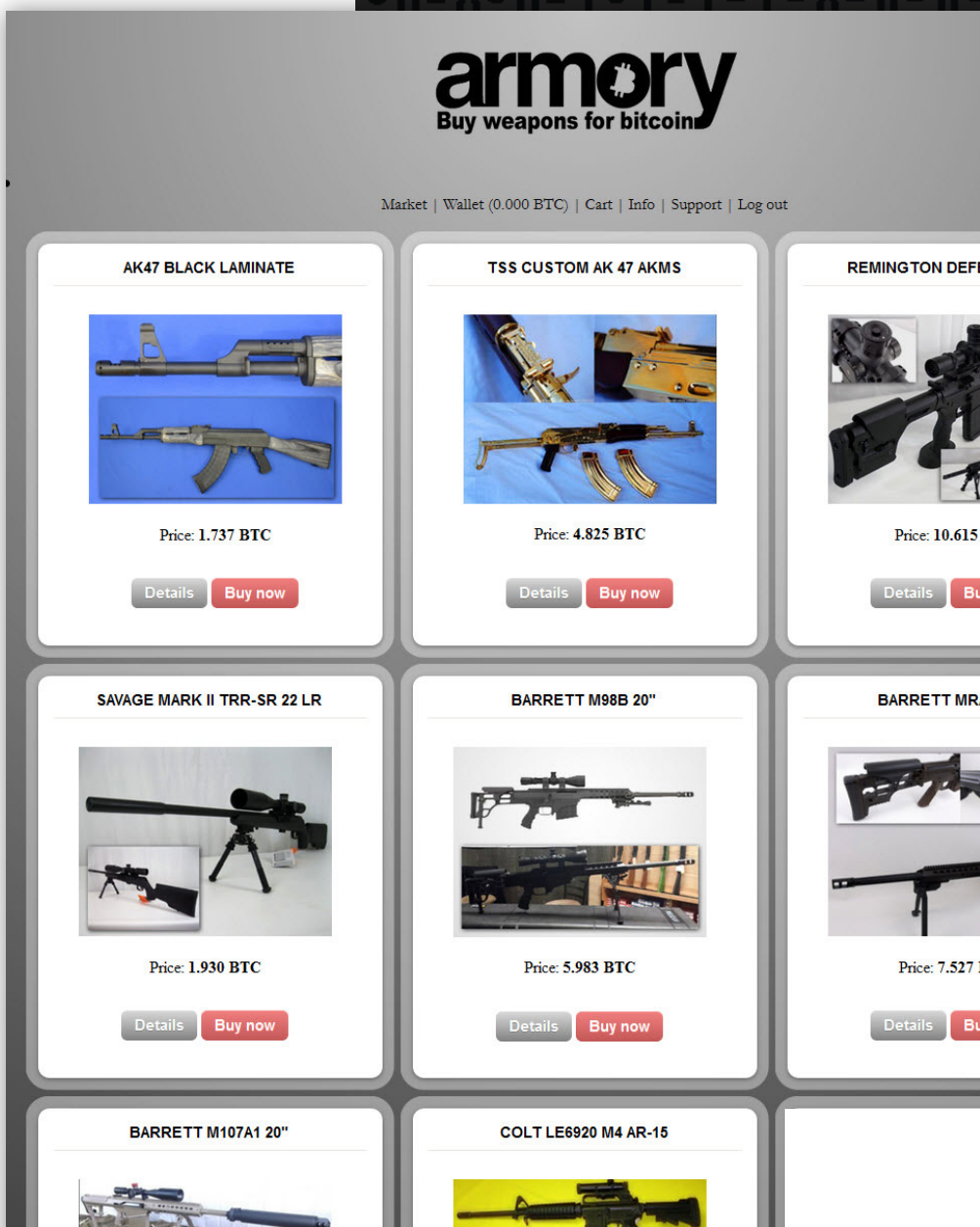
"My goal is to build, engineer, deploy a network where the technology reflects what a broad number of people can get behind," he continues. Grothoff says that, despite being in the works for more than a dozen years, GNUnet is still only for geeks right now. Although he certainly believes in the project, he has no illusions about its complexity. "We have made some progress but it's still not usable for most users, and I know that. There's some really hard issues remaining. I don't have all the answers today, but I have some good answers."



SHOULD WE MAKE THE WEB GO DARK?

In the process of writing this piece, I did traverse the Dark Web. I beheld the smoking ruins of Silk Road—now just a placeholder image left by U.S. law enforcement officials. I've seen a site that promises to kill the person of my choice for a few thousand dollars. I've priced out automatic weapons in bitcoins. I've seen links that seemed to promise underage pornography (but I didn't click on any of them).

It's disgusting, but a lot of it is elusive. Most of the links are dead, and many of the sites I can visit don't inspire the same kind of confidence



that eBay or Amazon do. Though there's something spooky about the matter-of-factness of a site that claims to offer murder at reasonable rates, I don't know if any of this is real. Accessing a website that is only viewable while my traffic is bounced around doesn't necessarily mean that the site's owners—if they exist—can follow through on their promises.

What's more, the Surface Web isn't exactly a paragon of upstanding behavior. A cursory Google search will reveal thousands of sites devoted to violent and racist causes. It's almost impossible to visit a website without advertisers collecting your data, and loading a legitimate website can trigger the download of malicious software. That's not to mention mass surveillance from nations like the U.S., or countrywide censorship like what's seen in China or Iran.

That makes me wonder what the Internet would be like if it were more like the Dark Web. Our Web would, at least in theory, be free from state-sponsored censorship and more secure by design. A lot of what we take for granted in our current economy—the passive gathering of personal data by companies for profit, for example—would vanish. But capitalism adapts. So does law enforcement, as Silk Road demonstrated.

The Internet as we know it now is a far cry from the simple collection of labs and universities that were first linked together in ARPANET, but the underlying technology isn't so different. Reinventing the Web as a tool for communication, but also one with built-in privacy, doesn't seem like such a bad idea in today's world, where the Web plays as much a role in defining us as our jobs and haircuts.

Perhaps it's not surprising that, in this environment, Tor and the Dark Web are growing. The number of volunteer nodes through which Tor traffic is routed has steadily increased. When I ask Tanase if he thinks Tor and the Dark Web will ever eclipse the Surface Web in size, he says it's very unlikely but then adds, "Never say never. People want it."