PANDO
QUARTERLY
SUMMER2014

PANDOQUARTERLY
SUMMER2014

LETTER FROM THE **EDITOR**

Hey everyone and welcome to our first annual "Assholes" Special Issue.

That's a joke. Well, it's sort of a joke. At least, I hope it's a joke. In this issue, we examine a startup ecosystem in the throws of a culture shift. Note I don't say culture "crisis," because it's not clear that it is a crisis: From Uber to Snapchat, assholes are getting richly rewarded by creating products we all love.

As a consumer, entrepreneur, and a journalist, I feel mixed about the trend, as do dozens and dozens of venture capitalists and entrepreneurs I spoke with off the record over the past few months. But no one—not a single person—denied that the shift was happening.

And this highlights why we think it's important that Pando exists right now—and why we're so grateful you support our kind of journalism. From the "Techtopus" wage collusion scandal—which Mark Ames advances with his Pixar revelations in this issue—to Paul Carr's Secret bombshells to James Robinson's ongoing exposes of Indiegogo's Scampaigns, we're just as dedicated to exposing the bad actors in the tech industry as we are to encouraging the positive influences.

That's what we mean when we promise to speak truth to the new power.

Hope you enjoy the issue!
Sarah Lacy, Editor in Chief, Pando

Subscriptions www.pando.com
Advertising and other inquiries:
info@pandodaily.com

EDITOR IN CHIEF/CEO **SARAH LACY** | EDITORIAL DIRECTOR **PAUL CARR** | WEST COAST EDITOR **MICHAEL CARNEY** | EAST COAST EDITOR **DAVID HOLMES** | WRITERS **MARK AMES, GARY BRECHER, YASHA LEVINE, NATHANIEL MOTT, JAMES ROBINSON** | ILLUSTRATORS **BRAD JONAS, HALLIE BATEMAN, MARK KAUFMAN, JEANNETTE LANGMEAD** | CARTOONIST **RICHARD STEVENS** | PRINT DESIGNER **GEOFFREY ELLIS** | CTO **JAMES AYLETT** | SALES/BIZDEV **BRAD BOWERS** | MEMBERSHIPS **CHRIS GOSCINSKI** | COPY EDITOR **KATHERINE DOLAN** | EXECUTIVE ASSISTANT **KATHLEEN ZEPEDA**

PandoQuarterly › Summer 2014/Volume 1 : Issue 3 is published quarterly for $300/year by PandoMedia, 81 Langton St., Suite 4, San Francisco, CA 94103
POSTMASTER: Send address changes to PandoMedia, 81 Langton St., Suite 4, San Francisco, CA 94103
Periodicals postage pending at Las Vegas, NV and additional mailing offices | Cover art: Brad Jonas | Printed by Creel Printing LLC in Las Vegas, NV

ALMOST EVERYONE INVOLVED IN DEVELOPING TOR WAS (OR IS) FUNDED BY THE U.S. GOVERNMENT

BY YASHA LEVINE
ART BY JEANNETTE LANGMEAD AND BRAD JONAS

In early July, hacker Jacob Appelbaum and two other security experts published a blockbuster story in conjunction with the German press. They had obtained leaked top secret NSA documents and source code showing that the surveillance agency had targeted and potentially penetrated the Tor Network, a widely used privacy tool considered to be the holy grail of online anonymity.

Internet privacy activists and organizations reacted to the news with shock. For the past decade, they had been promoting Tor as a scrappy but extremely effective grassroots technology that can protect journalists, dissidents and whistleblowers from powerful government forces that want to track their every move online. It was supposed to be the best tool out there. Tor's been an integral part of EFF's "Surveillance Self-Defense" privacy toolkit. Edward Snowden is apparently a big fan, and so is Glenn Greenwald, who says it "allows people to surf without governments or secret services being able to monitor them."

But the German exposé showed Tor providing the opposite of anonymity: it singled out users for total NSA surveillance, potentially sucking up and recording everything they did online.

To many in the privacy community, the NSA's attack on Tor was tantamount to high treason: a fascist violation of a fundamental and sacred human right to privacy and free speech.

The Electronic Frontier Foundation believes Tor to be "essential to freedom of expression." Appelbaum—a Wikileaks volunteer and Tor developer—considers volunteering for Tor to be a valiant act on par with Hemingway or Orwell "going to Spain to fight the Franco fascists" on the side of anarchist revolutionaries.

It's a nice story, pitting scrappy techno-anarchists against the all-powerful US Imperial machine. But the facts about Tor are not as clear cut or simple as these folks make them out to be...

Let's start with the basics: Tor was developed, built and financed by the US military-surveillance complex. Tor's original—and current—purpose is to cloak the online identity of government agents and informants while they are in the field: gathering intelligence, setting up sting operations, giving human intelligence assets a way to report back to their handlers—that kind of thing. This information is out there, but it's not very well known, and it's certainly not emphasized by those who promote it.

Peek under Tor's hood, and you quickly realize that just everybody involved in developing Tor technology has been and/or still is funded by the Pentagon or related arm of the US empire. That includes Roger Dingledine, who brought the technology to life under a series of military and federal government contracts. Dingledine even spent a summer working at the NSA.

If you read the fine print on Tor's website, you'll see that Tor is still very much in active use by the US government:

> "A branch of the U.S. Navy uses Tor for open source intelligence gathering, and one of its teams used Tor while deployed in the Middle East recently. Law enforcement uses Tor for visiting or surveilling web sites without leaving government IP addresses in their web logs, and for security during sting operations."

NSA? DoD? U.S. Navy? Police surveillance? What the hell is going on? How is it possible that a privacy tool was created by the same military and intelligence agencies that it's supposed to guard us against? Is it a ruse? A sham? A honeytrap? Maybe I'm just being too paranoid...

Unfortunately, this is not a tinfoil hat conspiracy theory. It is cold hard fact.

A BRIEF HISTORY OF TOR

The origins of Tor go back to 1995, when military scientists at the Naval Research Laboratory began developing cloaking technology that would prevent someone's activity on the Internet from being traced back to them. They called it "onion routing"—a method redirecting traffic into a parallel peer-to-peer

In a December 2004 press release announcing its support for Tor, EFF curiously failed to mention that this anonymity tool was developed primarily for military and intelligence use.

network and bouncing it around randomly before sending it off to its final destination. The idea was to move it around so as to confuse and disconnect its origin and destination, and make it impossible for someone to observe who you are or where you're going on the Internet.

Onion routing was like a hustler playing the three-card monte with your traffic: the guy trying to spy on you could watch it going under one card, but he never knew where it would come out.

The technology was funded by the Office of Naval Research and DARPA. Early development was spearheaded by Paul Syverson, Michael Reed and David Goldschlag—all military mathematicians and computer systems researchers working for the Naval Research Laboratory, sitting inside the massive Joint Base Anacostia-Bolling military base in Southeast Washington, D.C.

The original goal of onion routing wasn't to protect privacy—or at least not in the way most people think of "privacy." The goal was to allow intelligence and military personnel to work online undercover without fear of being unmasked by someone monitoring their Internet activity.

"As military grade communication devices increasingly depend on the public communications infrastructure, it is important to use that infrastructure in ways that are resistant to traffic analysis. It may also be useful to communicate anonymously, for example when gathering intelligence from public databases," explained a 1997 paper outlining an early version of onion routing that was published in the Naval Research Labs Review.

In the '90s, as public Internet use and infrastructure grew and multiplied, spooks needed to figure out a way to hide their identity in plain sight online. An undercover spook sitting in a hotel room in a hostile country somewhere couldn't simply dial up CIA.gov on his browser and log in—anyone sniffing his connection would know who he was. Nor could a military intel agent infiltrate a potential terrorist group masquerading as an online animal rights forum if he had to create an account and log in from an army base IP address.

That's where onion routing came in. As Michael Reed, one of the inventors of onion routing, explained: providing cover for military and intelligence operations online was their primary objective; everything else was secondary:

> The original *QUESTION* posed that led to the invention of Onion Routing was, "Can we build a system that allows for bi-directional communications over the Internet where the source and destination cannot be determined by a mid-point?" The *PURPOSE* was for DoD / Intelligence usage (open source intelligence gathering, covering of forward deployed assets, whatever). Not helping dissidents in repressive countries. Not assisting criminals in covering their electronic tracks. Not helping bit-torrent users avoid MPAA/RIAA prosecution. Not giving a 10-year old a way to bypass an anti-porn filter. Of course, we knew those would be other unavoidable uses for the technology, but that was immaterial to the problem at hand we were trying to solve (and if those uses were going to give us more cover traffic to better hide what we wanted to use the network for, all the better...I once told a flag officer that much to his chagrin).

Apparently solving this problem wasn't very easy. Onion router research progressed slowly, with several versions developed and discarded. But in 2002, seven years after it began, the project moved into a different and more active phase. Paul Syverson from the Naval Research Laboratory stayed on the project, but two new guys fresh outta MIT grad school came on board: Roger Dingledine and Nick Mathewson. They were not formally employed by Naval Labs, but were on contract from DARPA and the U.S. Naval Research Laboratory's Center for High Assurance Computer Systems. For the next several years, the three of them worked on a newer version of onion routing that would later become known as Tor.

Very early on, researchers understood that just designing a system that only technically anonymizes traffic is not enough—not if the system is used exclusively by military and intelligence. In order to cloak spooks better, Tor needed to be used by a diverse group of people: Activists, students, corporate researchers, soccer moms, journalists, drug dealers, hackers, child pornographers, foreign agents, terrorists—the more diverse the group that spooks could hide in the crowd in plain sight.

Tor also needed to be moved off site and disassociated from

Naval research. As Syverson told Bloomberg in January 2014: "If you have a system that's only a Navy system, anything popping out of it is obviously from the Navy. You need to have a network that carries traffic for other people as well."

Dingledine said the same thing a decade earlier at the 2004 Wizards of OS conference in Germany:

> "The United States government can't simply run an anonymity system for everybody and then use it themselves only. Because then every time a connection came from it people would say, 'Oh, it's another CIA agent.' If those are the only people using the network."

The consumer version of Tor would be marketed to everyone and—equally important—would eventually allow anyone to run a Tor node/relay, even from their desktop computer. The idea was to create a massive crowdsourced torrent-style network made up from thousands of volunteers all across the world.

At the very end of 2004, with Tor technology finally ready for deployment, the US Navy cut most of its Tor funding, released it under an open source license and, oddly, the project was handed over to the Electronic Frontier Foundation.

"We funded Roger Dingledine and Nick Mathewson to work on Tor for a single year from November 2004 through October 2005 for $180,000. We then served as a fiscal sponsor for the project until they got their 501(c)(3) status over the next year or two. During that time, we took in less than $50,000 for the project," EFF's Dave Maass told me by email.

In a December 2004 press release announcing its support for Tor, EFF curiously failed to mention that this anonymity tool was developed primarily for military and intelligence use. Instead, it focused purely on Tor's ability to protect free speech from oppressive regimes in the Internet age.

"The Tor project is a perfect fit for EFF, because one of our primary goals is to protect the privacy and anonymity of Internet users. Tor can help people exercise their First Amendment right to free, anonymous speech online," said EFF's Technology Manager Chris Palmer.

Later on, EFF's online materials began mentioning that Tor had been developed by the Naval Research Lab, but played down the connection, explaining that it was "in the past." Meanwhile the organization kept boosting and promoting Tor as a powerful privacy tool:

> "Your traffic is safer when you use Tor."

PLAYING DOWN TOR'S TIES TO THE MILITARY...

The people at EFF weren't the only ones minimizing Tor's ties to the military.

In 2005, Wired published what might have been the first major profile of Tor technology. The article was written by Kim Zetter, and headlined: "Tor Torches Online Tracking." Although Zetter was a bit critical of Tor, she made it seem like the anonymity technology had been handed over by the military with no strings attached to "two Boston-based programmers"—Dingledine and Nick Mathewson, who had completely rebuilt the product and ran it independently.

Dingledine and Mathewson might have been based in Boston, but they—and Tor—were hardly independent.

At the time that the Wired article went to press in 2005, both had been on the Pentagon payroll for at least three years. And they would continue to be on the federal government's payroll for at least another seven years.

In fact, in 2004, at the Wizards of OS conference in Germany, Dingledine proudly announced that he was building spy craft tech on the government payroll:

> "I forgot to mention earlier something that will make you look at me in a new light. I contract for the United States Government to built anonymity technology for them and deploy it. They don't think of it as anonymity technology, although we use that term. They think of it as security technology. They need these technologies so they can research people they are interested in, so they can have anonymous tip lines, so that they can buy things from people without other countries knowing what they are buying, how much they are buying and where it is going, that sort of thing."

Government support kept rolling in well after that.

In 2006, Tor research was funded

In 2012, Tor nearly doubled its budget, taking in $2.2 million from Pentagon and intel-connected grants.

was through a no-bid federal contract awarded to Dingledine's consulting company, Moria Labs. And starting in 2007, the Pentagon cash came directly through the Tor Project itself—thanks to the fact that Team Tor finally left EFF and registered its own independent 501(c)(3) non-profit.

How dependent was—and is—Tor on support from federal government agencies like the Pentagon?

In 2007, it appears that all of Tor's funding came from the federal government via two grants. A quarter million came from the International Broadcasting Bureau (IBB), a CIA spinoff that now operates under the Broadcasting Board of Governors. IBB runs Voice of America and Radio Marti, a propaganda outfit aimed at subverting Cuba's communist regime. The CIA supposedly cut IBB financing in the 1970s after its ties to Cold War propaganda arms like Radio Free Europe were exposed.

The second chunk of cash—just under $100,000—came from Internews, an NGO aimed at funding and training dissident and activists abroad. Tor's subsequent tax filings show that grants from Internews were in fact conduits for "pass through" grants from the US State Department.

In 2008, Tor got $527,000 again from IBB and Internews, which meant that 90% of its funding came from U.S. government sources that year.

In 2009, the federal government provided just over $900,000, or about 90% of the funding. Part of that cash came through a $632,189 federal grant from the State Department, described in tax filings as a "Pass-Through from Internews Network International." Another $270,000 came via the CIA-spinoff IBB. The Swedish government gave $38,000, while Google gave a minuscule $29,000.

Most of that government cash went out in the form of salaries to Tor administrators and developers. Tor co-founders Dingledine and Mathewson made $120,000. Jacob Appelbaum, the rock star hacker, Wikileaks volunteer and Tor developer, made $96,000.

In 2010, the State Department upped its grant to $913,000 and IBB gave $180,000—which added up to nearly $1 million out of a total of $1.3 million total funds listed on tax filings that year. Again, a good chunk of that went out as salaries to Tor developers and managers.

In 2011, IBB gave $150,00, while another $730,000 came via Pentagon and State Department grants, which represented more than 70% of the grants that year. (Although based on tax filings, government contracts added up to nearly 100% of Tor's funding.)

The DoD grant was passed through the Stanford Research Institute, a cutting-edge Cold War military-intel outfit. The Pentagon-SRI grant to Tor was given this description: "Basic and Applied Research and Development in Areas Relating to the Navy Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance."

That year, a new government funder came the scene: Swedish International Development Cooperation Agency (SIDA), Sweden's version of USAID, gave Tor $279,000.

In 2012, Tor nearly doubled its budget, taking in $2.2 million from Pentagon and intel-connected grants: $876,099 came from the DoD, $353,000 from the State Department, $387,800 from IBB.

That same year, Tor lined up an unknown amount funding from the Broadcasting Board of Governors to finance fast exit nodes.

TOR AT THE NSA?

In 2013, the Washington Post revealed that the NSA had figured out various ways of unmasking and penetrating the anonymity of the Tor Network.

> "Since 2006, according to a 49-page research paper titled simply 'Tor,' the agency has worked on several methods that, if successful, would allow the NSA to uncloak anonymous traffic on a 'wide scale'—effectively by watching communications as they enter and exit the Tor system, rather than trying to follow them inside. One type of attack, for example, would identify users by minute differences in the clock times on their computers.
>
> The evidence came out of Edward Snowden's NSA leaks. It appeared that the surveillance agency had developed several techniques to get at Tor. One of the documents explained that the NSA 'pretty much guaranteed to succeed.'"

Snowden's leaks revealed another interesting detail: In 2007, Dingledine gave at a talk at the NSA's HQ explaining Tor, and how it worked.

The Washington Post published the NSA's notes from their meeting with Dingledine. They showed that Dingledine and the NSA mostly talked about the technical details of Tor—how the network works and some of its security/usability tradeoffs. The NSA was curious about "Tor's customers," and Dingledine ran down some of the types of people who could benefit from Tor: Blogger Alice, 8 yr. old Alice, Sick Alice, Consumer Alice, Oppressed Alice, Business Alice, Law Enforcement Alice...

Interestingly, Dingledine told the NSA that "the way TOR is spun is dependent on who the 'spinee' is"—meaning that he markets Tor technology in different ways to different people?

Interestingly, the Washington Post article described Dingledine's trip to the NSA as "a wary encounter, akin to mutual intelligence gathering, between a spy agency and a man who built tools to ward off electronic surveillance." Dingledine told the paper that he came away from that meeting with the feeling that the NSA was trying to hack the Tor network:

> "As he spoke to the NSA, Dingledine said in an interview Friday, he suspected the agency was attempting to break into Tor, which is used by millions of people around the world to shield their identities."

Dingledine may very well have been antagonistic during his meeting with the NSA. Perhaps he was protective over his Tor baby, and didn't want its original inventors and sponsors in the US government taking it back. But whatever the reason, the antagonism was not likely borne out of some sort of innate ideological hostility towards the US national security state.

Aside from being on the DoD payroll, Dingledine has spends a considerable amount of his time meeting and consulting with military, intelligence and law enforcement agencies to explain why Tor's so great, and instructing them on how to use it. What kind of agencies does he meet with? The FBI, CIA and DOJ are just a few... And if you listen to Dingledine explain these encounters in some of his public appearances, one does not detect so much as a whiff of antagonism towards intelligence and law enforcement agencies.

In 2013, during a talk at UC San Diego, Dingledine cheerfully recalled how an exuberant FBI agent rushed up to thank him during his recent trip to the FBI:

> "So I've been doing a lot of talks lately for law enforcement. And pretty much every talk I do these days, some FBI person comes up to me afterwards and says, 'I use Tor everyday for my job. Thank you.' Another example is anonymous tips—I was talking to the folks who run the CIA anonymous tip line. It's called the Iraqi Rewards Program..."

Over the past few years, U.S. law enforcement has taken control and shutdown a series of illegal child porn and drug marketplaces operating on what should have been untraceable, hyper-anonymous servers running in the Tor cloud.

Dingledine's close collaboration with law enforcement aside, there's the strangely glib manner in which he dismissed news about the NSA hacking into Tor. He seemed totally unconcerned by the evidence revealed by Snowden's leaks, and played down the NSA's capabilities in his comments to the Washington Post:

> "If those documents actually represent what they can do, they are not as big an adversary as I thought."

I reached out to Dingledine to ask him about his trip to the NSA and whether he warned the Tor community back in 2007 that he suspected the NSA was targeting Tor users. He didn't respond.

HOW SAFE IS TOR, REALLY?

If Dingledine didn't appear to be fazed by evidence of the NSA's attack on Tor anonymity, it's strange considering that an attack by a powerful government entity has been known to be one Tor's principle weaknesses for quite some time.

In a 2011 discussion on Tor's official listserv, Tor developer Mike Perry admitted that Tor might not be very effective against powerful, organized "adversaries" (aka governments) that are capable monitoring huge swaths of the Internet.

> "Extremely well funded adversaries that are able to observe large portions of the Internet can probably break aspects of Tor and may be able to deanonymize users. This is why the core Tor program currently has a version number of 0.2.x and comes with a warning that it is not to be used for "strong anonymity." (Though I personally don't believe any adversary can reliably deanonymize **all** tor users... but attacks on anonymity are subtle and cumulative in nature)."

Indeed, just last year, Syverson was part of a research team that pretty much proved that Tor can no longer be expected to protect users over the long term.

> "Tor is known to be insecure against an adversary that can observe a user's traffic entering and exiting the anonymity network. Quite simple and efficient techniques can correlate traffic at these separate locations by taking advantage of identifying traffic patterns. As a result, the user and his destination may be identified, completely subverting the protocol's security goals."

The researchers concluded:

> "These results are somewhat gloomy for the current security of the Tor network."

While Syverson indicated that some of the security issues identified by this research have been addressed in recent Tor versions, the findings only added to a growing list of other research and anecdotal evidence showing Tor's not as safe as its boosters want you to think—especially when pitted against determined intelligence agencies.

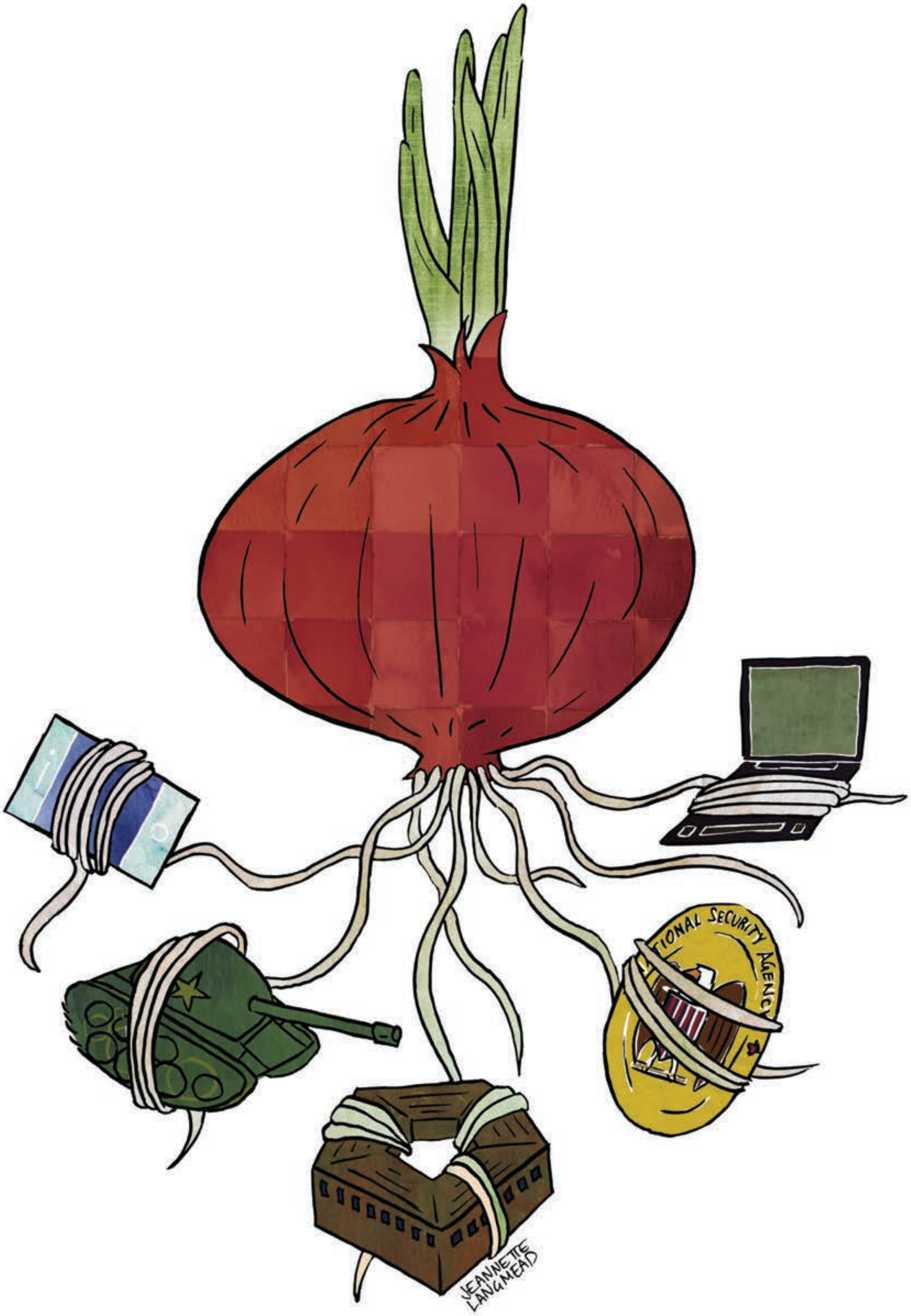
Case-in-point: In December 2013, a 20-year-old Harvard panicked overachiever named Edlo Kim learned just how little protection Tor offered for would-be terrorists.

To avoid taking a final exam he wasn't prepared for, Kim hit up on the idea of sending in a fake bomb threat. To cover his tracks, he used Tor, supposedly the best anonymity service the web had to offer. But it did little mask his identity from a determined Uncle Sam. A joint investigation, which involved the FBI, the Secret Service and local police, was able to track the fake bomb threat right back to Kim—in less than 24 hours.

As the FBI complaint explained, "Harvard University was able to determine that, in the several hours leading up to the receipt of the e-mail messages described above, ELDO KIM accessed TOR using Harvard's wireless network." All that Tor did was make the cops jump a few extra steps. But it wasn't hard, nothing that a bit of manpower with full legal authority to access network records couldn't solve. It helped that Harvard's network logging all metadata access on the network—sorta like the NSA.

Over the past few years, U.S. law enforcement has taken control and shutdown a series of illegal child porn and drug marketplaces operating on what should have been untraceable, hyper-anonymous servers running in the Tor cloud.

In 2013, they took down Freedom Hosting, which was accused of being a massive child porn hosting operation—but not before taking control of its servers and intercepting all of its communication with customers. The FBI did the same thing that same year with the online drug superstore Silkroad, which also ran its services in the Tor cloud. Although, rookie mistakes helped FBI unmask the identity of Dred Pirate Roberts, it is still a mystery how they were able


NATIONAL SECURITY AGENCY
JEANNETTE LANGMEAD

to totally take over and control, and even copy, a server run in the Tor cloud—something that is supposed to be impossible.

Back in 2007, a Swedish hacker/researcher named Dan Egerstad showed that just by running a Tor node, he could siphon and read all the unencrypted traffic that went through his chunk of the Tor network. He was able to access logins and passwords to accounts of NGOs, companies, and the embassies of India and Iran. Egerstad thought at first that embassy staff were just being careless with their info, but quickly realized that he had actually stumbled on a hack/surveillance operation in which Tor was being used to covertly access these accounts.

Although Egerstad was a big fan of Tor and still believes that Tor can provide anonymity if used correctly, the experience made him highly suspicious.

He told Sydney Morning Herald that he thinks many of the major Tor nodes are being run by intelligence agencies or other parties interested in listening in on Tor communication.

“I don't like speculating about it, but I'm telling people that it is possible. And if you actually look in to where these Tor nodes are hosted and how big they are, some of these nodes cost thousands of dollars each month just to host because they're using lots of bandwidth, they're heavy-duty servers and so on. Who would pay for this and be anonymous? For example, five of six of them are in Washington D.C. …”

> There's no way of knowing if the people running the fastest most stable nodes are doing it out of goodwill or because it's the best way to listen in and subvert the Tor network.

TOR STINKS?

Tor supporters point to a cache of NSA documents leaked by Snowden to prove that the agency fears and hates Tor. A 2013 Guardian story based on these docs—written by James Ball, Bruce Schneier and Glenn Greenwald—argues that agency is all but powerless against the anonymity tool.

“[T]he documents suggest that the fundamental security of the Torservice remains intact. One top-secret presentation, titled 'Tor Stinks', states: 'We will never be able to de-anonymize all Tor users all the time.' It continues: 'With manual analysis we can de-anonymize a very small fraction of Tor users,' and says the agency has had 'no success de-anonymizing a user in response' to a specific request.

Another top-secret presentation calls Tor “the king of high-secure, low-latency internet anonymity.”

But the NSA docs are far from conclusive and offer conflicting bits of evidence, allowing for multiple interpretations. But the fact is that the NSA and GCHQ clearly have the capability to compromise Tor, but it might take a bit of targeted effort.

One thing is clear: the NSA most certainly does not hate or fear Tor. And some aspects about Tor are definitely welcomed by the NSA, in part because it helps concentrate potential “targets” in one convenient location.

“TOR STINKS… BUT IT COULD BE WORSE

- Critical mass of targets use Tor. Scaring them away might be counterproductive.
- We can increase our success rate and provide more client IPs for individual Tor users.
- We will never get 100% but we don't need to provide true IPs for every target every time they use Tor.”

The Tor network is not as difficult to capture as it may seem…

In 2012, Tor co-founder Roger Dingledine revealed that the Tor Network is configured to prioritize speed and route traffic through the fastest servers/nodes available. As a result, the vast bulk of Tor traffic runs through several dozen of the fastest and most dependable servers: “on today's network, clients choose one of the fastest 5 exit relays around 25-30% of the time, and 80% of their choices come from a pool of 40-50 relays.”

Dingledine was criticized by Tor community for the obvious reason that funneling traffic through a handful of fast nodes made surveilling and subverting Tor much easier. Anyone can run a Tor node—a research student in Germany, a guy with FIOS connection in Victorville (which is where I was for a few months), an NSA front out of Hawaii or a guy working for China's Internet Police.

There's no way of knowing if the people running the fastest most stable nodes are doing it out of goodwill or because it's the best way to listen in and subvert the Tor network. Particularly troubling was that Snowden's leaks clearly showed the NSA and GCHQ run Tor nodes, and are interested in running more.

And running 50 Tor nodes doesn't seem like it would be too difficult for any of the world's intelligence agencies—whether American, German, British, Russian, Chinese or Iranian. Hell, if you're an intelligence agency, there's no reason not to run a Tor node.

Back in 2005, Dingledine admitted to Wired that this was a "tricky design question" but couldn't provide a good answer to how they'd handle it. In 2012, he dismissed his critics altogether, explaining that he was perfectly willing to sacrifice security for speed—whatever it took to take get more people to use Tor:

"This choice goes back to the original discussion that Mike Perry and I were wrestling with a few years ago… if we want to end up with a fast safe network, do we get there by having a slow safe network and hoping it'll get faster, or by having a fast less-safe network and hoping it'll get safer? We opted for the 'if we don't stay relevant to the world, Tor will never grow enough' route."

SPEAKING OF SPOOKS RUNNING TOR NODES…

If you thought the Tor story couldn't get any weirder, it can and does. Probably the strangest part of this whole saga is the fact that Edward Snowden ran multiple high-bandwidth Tor nodes while working as an NSA contractor in Hawaii.

This only became publicly known last May, when Tor developer Runa Sandvik (who also drew her salary from Pentagon/State Department sources at Tor) told Wired's Kevin Poulsen that just two weeks before he would try to get in touch with Glenn Greenwald, Snowden emailed her, explaining that he ran a major Tor node and wanted to get some Tor stickers.

Stickers? Yes, stickers.

Here's Wired:

"In his e-mail, Snowden wrote that he personally ran one of the "major tor exits"–a 2 gbps server named "TheSignal"–and was trying to persuade some unnamed coworkers at his office to set up additional servers. He didn't say where he worked. But he wanted to know if Sandvik could send him a stack of official Tor stickers. (In some post-leak photos of Snowden you can see the Tor sticker on the back of his laptop, next to the EFF sticker)."

Snowden's request for Tor stickers turned into something a bit more intimate. Turned out that Sandvik was already planning to go to Hawaii for vacation, so she suggested they meet up to talk about communication security and encryption.

"She wrote Snowden back and offered to give a presentation about Tor to a local audience. Snowden was enthusiastic and offered to set up a crypto party for the occasion."

So the two of them threw a "crypto party" at a local coffee shop in Honolulu, teaching twenty or so locals how to use Tor and encrypt their hard drives. "He introduced himself as Ed. We talked for a bit before everything started. And I remember asking where he worked or what he did, and he didn't really want to tell," Sandvik told Wired.

But she did learn that Snowden was running more than one Tor exit node, and that he was trying to get some of his buddies at "work"to set up additional Tor nodes…

H'mmm…So Snowden running powerful Tor nodes and trying to get his NSA colleagues to run them, too?

I reached out to Sandvik for comment. She didn't reply. But Wired's Poulsen suggested that running Tor nodes and throwing a crypto party was a pet privacy project for Snowden. "Even as he was thinking globally, he was acting locally."

But it's hard to imagine a guy with top secret security clearance in the midst of planning to steal a huge cache of secrets would risk running a Tor node to help out the privacy cause. But then, who hell the knows what any of this means.

I guess it's fitting that Tor's logo is an onion—because the more layers you peel and the deeper you get, the less things make sense and the more you realize that there is no end or bottom to it. It's hard to get any straight answers—or even know what questions you should be asking.

In that way, the Tor Project more resembles a spook project than a tool designed by a culture that values accountability or transparency.