The Tor Project: Applying Censorship Resistance Research to the Field

4rd QUARTER OF PROJECT, Q3 OF THE YEAR: July 1 2015 – September 30 2015

Project Overview

Part one: Pluggable transport integration

Part two: Testing and network simulation improvements

Part three: Enhanced outreach

Foreign Assistance Framework: Internet Freedom Specific Indicators:

Q3 Project Timeline (July 1, 2015 – September 30, 2015) – Activity Summary

Pluggable transport integration

Project Objectives:

Outputs for the Quarter:

Outcomes:

Challenges:

Successes:

Testing and network simulation improvements

Project Objectives:

Outputs for the Quarter:

Outcomes:
Challenges:

Successes:

Enhanced outreach

Project Objectives:

Outputs for the Quarter:

Outcomes:

Challenges:

Successes:

Press:

Next Quarter’s Planned Activities:

Pluggable Transport Integration

Testing and network simulation improvements

Enhanced Outreach
Project Overview

The project contains three main activities:

Part one: Pluggable transport integration

Tor will work to safely deploy transport technology to resist censorship, especially censorship based on deep packet inspection. This will be achieved by working with researchers to improve the usability, portability, security and code maintainability for transports; integrating mature transports into experimental bundles for real users and feeding those results into further improvements; and improving and maintaining the application programming interface between Tor and the pluggable transport layer.

Part two: Testing and network simulation improvements

Tor will improve the correctness and stability of the core Tor software by streamlining and automating the process of launching a complete test; designing and scripting an automated test suite to exercise and stress as much of Tor’s functionality as possible; and extending Tor’s controller interface to allow better monitoring.

Part three: Enhanced outreach

To increase awareness and improve the sustainability of the Tor technology and research, Tor will develop dynamic messaging and targeted campaigns aimed at end users and volunteers. Tor will identify partner organizations for outreach activities, including diaspora populations from countries with low press freedom rankings, open source development groups, and NGOs supporting civil society.
Foreign Assistance Framework: Internet Freedom Specific Indicators:

a. Number of unique users of circumvention technology or secure communication technology (measured monthly):

Looking at the graph below of directly-connecting Tor users in Q2 and Q3, we can see the number remain consistently around two million users/day.

The total number of bridge relay users remained around 20,000, though as the following graph shows, there was a slight decline at the end of July beginning of August - we are still investigating the causes:
When Pluggable Transport use is broken down by transport type, the results of our work become clearer. For instance, our cloud-service change to avoid excess charges is shown by the drop in July. Another visible trend is the adoption of obfs4, whose user base has grown consistently since its launch in April, and which is intended to take the place of obfs3 in due course.

b. Number of civil society actors trained in circumvention or digital safety techniques:

**Result:** 389 civil society actors trained in circumvention or digital safety techniques:

<table>
<thead>
<tr>
<th>Actors trained</th>
<th>Country</th>
<th>Event and/or partner organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>U.S.</td>
<td>(various: WH LGBT Tech Innovation, Congressional visits)</td>
</tr>
<tr>
<td>50</td>
<td>U.S.</td>
<td>Library Freedom Project at Cherry Hill Public Library</td>
</tr>
<tr>
<td>50</td>
<td>Ireland</td>
<td>Library Freedom Project at Royal Academy Dublin</td>
</tr>
<tr>
<td>45</td>
<td>U.S.</td>
<td>Library Freedom Project at Wallingford Library Connecticut</td>
</tr>
<tr>
<td>12</td>
<td>U.S.</td>
<td>Library Freedom Project at MCPL Bloomington Indiana</td>
</tr>
<tr>
<td>12</td>
<td>U.S.</td>
<td>Library Freedom Project at University of Indiana</td>
</tr>
<tr>
<td>100</td>
<td>U.S.</td>
<td>Library Freedom Project at Southern Illinois State</td>
</tr>
</tbody>
</table>
c. Number of USG-supported online tools developed or improved to maintain an open Internet:

Results:

- **Highlights for Pluggable Transport (PT):**
  - New PTs evaluations
    - obfs2
    - Scramble Suit
    - Flashproxy
    - FTE Transport
  - Improvements on 0.2.7.x Core Tor releases

- **Highlights for Testing improvements:**
  - Tor's tests are now launched from a unified testing framework that ships with the Tor source distribution, which integrates with external testing tools as well.
  - 0.2.7.3-rc is the most tested release of Tor to date (2015-09-25)
  - Unit tests coverage went from 37% to 39.4% at 0.2.7.3-rc release
  - Total coverage using stem and Chutney went from 62% to 64.49%

---

d. Number of individuals or organizations operating in Internet repressive countries that are provided with technical assistance to increase online security:

**Result:** 12 individuals operating in internet repressive countries were provided with technical assistance.

<table>
<thead>
<tr>
<th>Individuals trained</th>
<th>Country</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>China</td>
<td>Individuals</td>
</tr>
</tbody>
</table>

---

1. [https://blog.torproject.org/blog/tor-0273-rc-released](https://blog.torproject.org/blog/tor-0273-rc-released)
e. USG-assisted campaigns and programs to enhance public understanding, NGO support and media coverage of digital threats and promotion of an open Internet:

**Result:** We are focusing on four areas of outreach; below are some highlights of this work in each area:

- Direct work with organizations:
  - As part of our ongoing work supporting the efforts of the Library Freedom Project, we promoted their pilot project to install Tor relays in US public libraries, and publicly supported this project when it was threatened by law enforcement.
  - Partnership with Facebook in getting IETF and IANA to recognize the .onion suffix as a Special-Use Domain Name, which will allow onion services to request SSL certificates for the servers.

- Outreach materials
  - Storyboard for our animation explaining Pluggable Transports and Bridge Distribution
  - Sent 112 T-shirt to Tor supporters (relay operators or donors).

- Social Media:
  - Our social media account continues to grow in popularity and influence, with 3.9M impressions and 15K new followers (up from the 10K followers gained during the last quarter).
  - Effective social media engagement and response during significant events, such as the Hacking Team leaks, which earned 2K retweets of Tor press statements.

- Media Support:
  - Our fast-response list composed of researchers and developers rapidly worked through the leaked Hacking Team documents for any Tor exploit-related information, and submitted its analysis along with a statement which served as reference for media stories.

f. Number of times USG-supported analytic reports are cited by national and international media outlets:

**Result:** The metrics published by the Tor Project help illustrate stories about the impact of censorship circumvention tools. They also help provide educational information about the Tor network and services (i.e. Hidden Services, Pluggable Transports, etc.).
It is difficult to keep count of all the articles in which our metrics are cited, but we include here a selection of articles that highlight how the most-used metrics are cited in the media.

<table>
<thead>
<tr>
<th>Title</th>
<th>Media outlet</th>
<th>Metric cited</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Russia hits roadblock in fight against Tor, the anonymity software</td>
<td>The Washington Times</td>
<td>Users per country (Russia) and top 10 countries by number of users</td>
<td>9/24/2015</td>
</tr>
<tr>
<td>used to evade online censorship</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Why DDoS Attacks Have Doubled in the past Year</td>
<td>App developer magazine</td>
<td>Analysis of malicious requests coming from Tor (1 in every 380 - where 1 in every 11,500 non-Tor</td>
<td>8/22/2015</td>
</tr>
<tr>
<td></td>
<td></td>
<td>requests were malicious)</td>
<td></td>
</tr>
<tr>
<td>Crypto activists announce vision for Tor exit relay in every library</td>
<td>Ars Technica</td>
<td>Number of exit nodes</td>
<td>7/30/2015</td>
</tr>
</tbody>
</table>
<pre><code>                                                                                                                               |
</code></pre>

**g. Number of times USG-supported analytic reports are discussed in established social media sites:**

**Result:**

Our metrics are discussed on social media with direct links to our websites or stories published in media outlets about our metrics. With hundreds of millions of users, it is hard to measure the total reach of our metrics-related posts, but a search for keywords such as “#Tor, usage, metrics” on Twitter provides us with some examples of these conversations on social media during Q3 2015:

5. [https://twitter.com/search?q=tor%20usage%2C%20metrics%20%23Tor%20since%3A2015-07-01%20until%3A2015-09-30&src=typd](https://twitter.com/search?q=tor%20usage%2C%20metrics%20%23Tor%20since%3A2015-07-01%20until%3A2015-09-30&src=typd)
6. [https://twitter.com/OpenPrunus/status/644630298727219200](https://twitter.com/OpenPrunus/status/644630298727219200)
7. [https://twitter.com/kharashov/status/643778731455197184](https://twitter.com/kharashov/status/643778731455197184)
We also promote our blog posts about metrics we are adding, or new usage numbers, through our Twitter account.

Q3 Project Timeline (July 1, 2015 - September 30, 2015) - Activity Summary

**Pluggable transport integration**

**Project Objectives:**

The idea is to separate Tor's anonymity and privacy properties from its censorship-resistance properties: The core Tor software focuses on building Tor circuits and getting the multi-layer
encryption right, while the transport layer focuses on preventing an attacker from recognizing or blocking the client's connections to the rest of the Tor network. This modular approach lets us "plug in" new transports as needed—and since the transport layer is a separate program, it can be written in whatever rapid prototyping language is most convenient, allowing Tor to adapt much more quickly to a censor's new Deep Packet Inspection (DPI) tactics without needing to touch the core Tor program at all.

Outputs for the Quarter:

Task 1 (SponsorT, aka the work we did via the Internews contract): Write the initial evaluation (to be continually revised) of existing and soon to be deployed transports following the evaluation criteria set out in the proposal.

During the quarter we held extensive discussions around the criteria for the Pluggable Transports to be included in Tor software. ‘MUST’- and ‘SHOULD’-level priorities were listed to ensure the quality of new PT designs. This discussion helped us to draft the first guidelines for this process and to work on an updated version of the PT spec.

Based on these documents, we reviewed the evaluations of:

- **obfs3**
- **obfs4**

and carried out the following new evaluations:

- **obfs2**
  - This evaluation was done for “historical reference only”, since obfs2 “is considered trivially breakable by most adversaries and is deprecated”.
- **ScrambleSuit**
  - We would like to quote from the evaluation:

  *While unbroken, most if not all of the functionality is also present in the obfs4 protocol, and thus is considered deprecated and has been evaluated as a historical reference only.*

  The evaluation is available online, and indicates valuable features of this PT that can serve as reference points for developers. The project is documented to be active, with ~200 users/day.

---

8 https://trac.torproject.org/projects/tor/wiki/doc/PluggableTransports/GuidelinesForDeployingPTs
• **Flashproxy** - some highlights of the evaluation:
  ○ While the design is deployed in theory, in practice, the requirement that clients must be able to accept incoming connections appears to be a significant barrier to actual use (< 10 daily users).
  ○ During Tor’s Dev Meeting in Berlin, a discussion was held regarding whether to continue or terminate this project. The current plan is to remove it from an upcoming Tor Browser for now, and wait for a newer version of the design that has NAT piercing (e.g. via WebRTC support) by default.

• **FTE Transport** - below are some key points from the evaluation:
  ○ It is the only current "mimicry"-based Pluggable Transport in production use.
  ○ The current regexes have several identifying features that could be used by a DPI system to detect and censor FTE.
  ○ The implementation can be built deterministically and is currently integrated into Tor Browser’s build process.
  ○ The implementation is written in a mixture of Python and C++. The Python components are memory safe, and tests exist for both the underlying library and the proxy program.

---

<https://trac.torproject.org/projects/tor/wiki/org/meetings/2015SummerDevMeeting/PTMeeting#RelatedNotesfromthe
corresponding meeting>
<https://trac.torproject.org/projects/tor/wiki/doc/PluggableTransports/FteEvaluation>
Usage is very small, oscillating between ~50 to ~150 users/day

Task 2 (SponsorS, aka this direct contract): Maintain and extend obfsproxy, obfs4proxy, obfsclient and other Pluggable Transport codebases as needed, and assist developers and researchers who wish to use our frameworks to do relevant research.

We continued to maintain obfs4proxy as the main framework for deployed pluggable transports in Tor Browser. It is performing well, and hasn’t needed much attention this quarter, which allowed us to focus on the evaluations above.

We continued preparations to do a full pluggable transport specification overhaul in October / November (after meeting about it to finalize plans in the Berlin dev meeting).

Task 3 (SponsorS): Tor side pluggable transport related (and other) improvements.

Minor features related to pluggable transports that formed part of Tor 0.2.7.3 releases:

- When launching managed pluggable transports on Linux systems, we now attempt to have the kernel deliver a SIGTERM on tor exit if the pluggable transport process is still running. Resolves ticket 15471.
- When launching managed pluggable transports, setup a valid open stdin in the child process that can be used to detect if tor has terminated. The "TOR_PT_EXIT_ON_STDIN_CLOSE" environment variable can be used by implementations to detect this new behavior. Resolves ticket 15435.

Task 4 (SponsorS): Pluggable transport R&D (Catchall)
We continued helping Marc Juarez, a graduate student under Claudia Diaz at KU Leuven, to improve his pluggable transport that provides a website fingerprinting defense framework for research purposes. This framework has proven useful at exploring anonymity defenses, by transforming Tor traffic to reduce timing and volume signatures. We are looking into finding a research grant to fund Marc, plus professors we’re working with at UT Arlington, to further extend the framework.

We helped Serene Han start her OTF fellowship at Berkeley working on adding WebRTC support to Flashproxy. David Fifield is helping to mentor her. In parallel, we’re continuing to make progress at finding external funding to let Arlo Breault allocate some time to WebRTC in Flashproxy too. We’re optimistic that the two of them together will make great progress on this topic in the “end of 2015, beginning of 2016” timeframe.

Outcomes:

We continue to evaluate pluggable transports, and added 4 new evaluations during this quarter: FTE Transport, Flashproxy, Scramble Suit and obfs2.

Our investment on obfs4 development is proving back, it had gained some good user growth pace. We also improved the core Tor code in version 0.2.7.3 to improve behavior if Tor terminates.

Our collaboration with graduate students from Berkeley is bringing great improvements on how research and tests can be done for PTs.

Challenges:

Our main challenge right now is to increase our capacity to do more community outreach. We worked on making good documentation that can guide our community of developers, now we need to share it with them and onboard them to use it.

Successes:

We have extensively discussed the features that a PT should or must have in order to be deployable. Based on these discussions, we have created a set of evaluation criteria, and checked against these to produce new evaluations of pluggable transports.

During our dev meeting in Berlin, we dedicated a session to discussing the adoption requirements for deploying a PT, one result of which is a roadmap for developers to follow in order to build deployable transports.
Testing and network simulation improvements

Project Objectives:
Tor will improve the correctness and stability of the core Tor software by streamlining and automating the process of launching a complete test; designing and scripting an automated test suite to exercise and stress as much of Tor's functionality as possible; and extending Tor's controller interface to allow better monitoring.

Outputs for the Quarter:
Tor's tests are now launched from a unified testing framework that ships with the Tor source distribution, which integrates with external testing tools as well.\(^{15}\)

We're using “stem” and “chutney” to test Tor's controller suite and integration properties respectively, which raises the coverage to 64.5% (last quarter it was 62%). The unit tests cover 39.40% of the code (last quarter they were at 37%).

Major features in 0.2.7.3-rc (performance testing):

- The test-network.sh script now supports performance testing. Requires corresponding chutney performance testing changes.\(^{16}\)

Minor features (testing, authorities, documentation):

- New TestingDirAuthVote{Exit,Guard,HSDir}IsStrict flags to explicitly manage consensus flags in testing networks.\(^{17}\)

Testing improvements:

- Make "bridges+hs" the default test network. This tests almost all tor functionality during make test-network, while allowing tests to succeed on non-IPv6 systems. Requires chutney commit 396da92 in test-network-bridges-hs. Closes tickets 16945 (tor) and 16946 (chutney). Patches by "teor".
- Autodetect CHUTNEY_PATH if the chutney and Tor sources are side-by-side in the same parent directory. Closes ticket 16903. Patch by "teor".
- Use environment variables rather than autoconf substitutions to send variables from the build system to the test scripts. This change should be easier to maintain, and cause 'make distcheck' to work better than before. Fixes bug 17148.
- Add a new set of callgraph analysis scripts that use clang to produce a list of which Tor functions are reachable from which other Tor functions. We're planning to use these to help simplify our code structure by identifying illogical dependencies.

\(^{15}\) https://gitweb.torproject.org/tor.git/tree/doc/HACKING/WritingTests.txt
\(^{16}\) https://trac.torproject.org/projects/tor/ticket/14175
\(^{17}\) https://trac.torproject.org/projects/tor/ticket/14882
- Add new 'test-full' and 'test-full-online' targets to run all tests, including integration tests with stem and chutney.
- Make the test-workqueue test work on Windows by initializing the network before we begin.
- New make target (make test-network-all) to run multiple applicable chutney test cases. Patch from Teor; closes 16953.
- Unit test dns_resolve(), dns_clip_ttl() and dns_get_expiry_ttl() functions in dns.c. Implements a portion of ticket 16831.
- When building Tor with testing coverage enabled, run Chutney tests (if any) using the 'tor-cov' coverage binary.
- When running test-network or test-stem, check for the absence of stem/chutney before doing any build operations.

Outcomes:

The 0.2.7.3-rc stable release is the most-tested release of Tor to date. Not only that, but we have made various small improvements to the operation of our testing framework, in order to make it as smooth as possible for developers to use, as described above in more detail.

Unifying all the testing frameworks is a milestone for us: these new features in the core Tor code help developers to execute different types of tests, call external testing tools when necessary, and many other development requirements.

We also updated our developer-facing documentation giving guidance on how to write tests for their code. Including this information will help us maintain this high level of test coverage in a sustainable fashion.

Challenges:

As we develop our testing procedures and add new code, we’ve found that contributed test code tends to vary in quality. Most worryingly, it’s common for contributed tests to check that the code *does exactly what it does* rather than that the code *performs its functions* and *behaves well under corner cases*. For example, if we were implementing an encryption library, we would expect to test not only that the code behaves correctly with test vectors but also that it can cope with empty messages, malformed keys, and so forth. What’s more, we’d expect tests to check whether the library is in fact able to decrypt messages that it encrypts. Most volunteer-submitted code so far only checks for the most low-level definitions of “correctness”.

So, while our existing testing documentation has proved invaluable in soliciting volunteers, we need to improve it in order to better communicate what exactly a good test should contain. We

---

[18](https://blog.torproject.org/blog/tor-0273-rc-released)
should also audit our existing older tests and note where they fail to meet our current standards.

As we have been building out our design for a modularized Tor, we’ve found several key challenges. Most notably, our software’s structure has made it difficult to find and isolate natural modules, due to the high number of Tor components that are reachable from most other high-level Tor components. We call this set “the blob”. While we’ve made progress in reducing its size, we expect that the remaining functions in it will be the least tractable. And what’s more, we still need our blob-measurements to take function pointers into account.

Further, our modularization schema.

Successes:

We are very happy with the pace of this project. Test coverage of the core Tor code is more comprehensive than ever before, and the quality of the integration testing tools is also improving, helping developers cover a diversity of scenarios.

Another point of success is that this work will help us identify areas of improvement in the code. The implementation shipped with 0.2.7.3-rc is a good example:

- Add a new set of callgraph analysis scripts that use clang to produce a list of which Tor functions are reachable from which other Tor functions. We’re planning to use these to help simplify our code structure by identifying illogical dependencies.

Enhanced outreach

Project Objectives:

We will make more people aware of the benefits of Tor, especially when censorship circumvention needs to be combined with privacy and anonymity to extend the time that civil society members can work in Internet-repressive environments.

Outputs for the Quarter:

Direct work with organizations:

One of our most significant outputs this quarter relating to our direct work with organizations was the recognition of the .onion suffix by IETF and IANA as a Special-Use Domain Name. As we wrote in our blog post on the achievement19:

---

19 https://blog.torproject.org/blog/landmark-hidden-services-onion-names-reserved-ietf
“This standardization work for .onion is joint work between Facebook and the Tor Project amongst others in an effort to help secure users everywhere.”

This recognition means that the .onion suffix will not be available for uses other than in onion service addresses, avoiding potential technical problems in the future; it also means that SSL certificates can be created for onion services, increasing the security of their client-server communications. This is a significant victory, both in terms of the technical innovation it represents, and also as a symbol of the increasing recognition of onion services as an essential Internet technology.

Outreach materials

We mailed 112 t-shirts this quarter to supporters who are either running a relay or who donated to us.

Bridge and Pluggable Transports animation:

---

20. [https://www.facebook.com/notes/alec-muffett/rfc-7686-and-all-that/10153809113970962]
Following the success of our animation explaining the basic concepts and goals of Tor to users in various languages\textsuperscript{22}, another is in preparation that will introduce users to Tor’s advanced censorship-circumvention features, namely Pluggable Transports and Bridges.

We are happy to say that the initial planning process is complete and we have come up with a concept that covers the main points any user needs to know about how these tools work and the best way to use them.

Here are some screenshots of the storyboards:

\textsuperscript{22} https://blog.torproject.org/blog/releasing-tor-animation
What do you do when a website is blocked or censored?  
Do you use Tor?

But what if even Tor isn't working? / But what if even Tor is blocked?

Don't panic!!! It’s not the end of the world (yet) / Don’t panic!!! World hasn’t come to an end (yet)

Fortunately, there are several ways to connect to the Tor network ...
In fact, many of these methods are already built in Tor Browser.

Each of which aims to work in a different scenario.

No matter which one is working for you this week,
You need to understand the game.

This way, you can bridge (bypass?) the censors and confound the snoops,
trying to spy on your online activities.

These methods known as "Pluggable Transports" are constantly being developed,
there will be even more in the future!

To learn more about Tor and how it works, watch [this video].
Media Support:

Last quarter, we organized a new email list comprised of recognized researchers and developers (both inside and outside Tor) to help us respond quickly and accurately to media requests. This quarter, the team was plunged straight in at the deep end when emails from Hacking Team were published online\textsuperscript{23}. The team was able to quickly review the emails and study them for any technical information related to the security of the Tor network and software, resulting in an analysis\textsuperscript{24} that allowed the media to know our position about the topic as they were running their first news stories\textsuperscript{25}.

\textsuperscript{23} https://wikileaks.org/hackingteam/emails/
\textsuperscript{24} https://blog.torproject.org/blog/preliminary-analysis-hacking-teams-slides
\textsuperscript{25} http://www.ibtimes.com/hacking-team-tried-break-tor-anonymity-network-spy-company-joins-tors-long-list-2006135
Social Media:

During this quarter our Twitter account achieved 3.9 million views or “impressions” in total, and an average of 43,300 impressions and 128 retweets per day, which are significant numbers given the reduced user activity associated with summer. We gained 15k followers this quarter, a higher growth than we saw last quarter (10k followers).

The Tor Project's most-read social media engagement in this quarter was a statement following the widely-publicized data breach suffered by Hacking Team\[^{26}\], a surveillance software vendor that had suggested it knew of exploitable vulnerabilities in Tor software. When this proved not to be the case, the Tor Project issued a statement on Twitter informing users of this, and reaffirming its commitment to user safety and human rights. This statement gained 2000 retweets and almost half a million impressions.

\[^{26}\] [https://twitter.com/torproject/status/618303411071655936](https://twitter.com/torproject/status/618303411071655936)
Among Tor's other influential engagements on Twitter were in support of Kilton Library in Lebanon, New Hampshire, which was subjected to pressure by the Department of Homeland Security for running a Tor exit relay on the library’s computer system.
Crypto activists announce vision for #Tor exit relay in every library arstechnica.com/?p=716619 @libraryfreedom @mrphs

Live Free or Die--Congratulations, Kilton Library!

Alison Macrina @flexlibris

#KiltonLibrary WE'VE DONE IT. THE KILTON LIBRARY WILL TURN THEIR #TOR RELAY BACK ON!!!
A series of tweets directing users to an EFF campaign\textsuperscript{30} in support of the library, as well as a follow-up statement\textsuperscript{31} and a link to a write-up\textsuperscript{32} in the Christian Science Monitor after the DHS lifted their opposition, gained a combined total of 1299 retweets and 492,164 impressions.

\begin{itemize}
\item \textbf{Our statement on tonight's decision by the Kilton Public Library in Lebanon, #NH to reinstate its #Tor relay.}
\end{itemize}

\begin{quote}
The Tor Project is thrilled to stand with New Hampshire’s Kilton Library as it joins 7,000 volunteers worldwide to run the Tor Network. Tor offers people the freedom to read and write whatever they want without surveillance or censorship—values we share with librarians everywhere. We thank the library for standing firm in the face of pressure to take down their Tor relay.

Great thanks also to Nima Fatemi, a brave human rights activist who was instrumental in this effort, and of course to Alison Macrina, our great partner at the Library Freedom Project.

Finally, we stand in solidarity with the people of Lebanon New Hampshire, who saw what was at stake and came to the library tonight to defend free speech.

\textit{–The Tor Project}
\end{quote}

\begin{itemize}
\item [\textsuperscript{30}] https://act.eff.org/action/support-tor-and-intellectual-freedom-in-libraries
\item [\textsuperscript{31}] https://twitter.com/torproject/status/643995518201397248
\item [\textsuperscript{32}] https://twitter.com/torproject/status/644997695535497216
\end{itemize}
The Tor Project’s mission statement, developed in collaboration with former Wikimedia Executive Director Sue Gardner, was retweeted 757 times and gained 238,325 impressions.

33 https://twitter.com/torproject/status/635856569201246208
Another intervention, encouraging Australian users to download the Tor Browser\(^{34}\) following the adoption of stricter data retention laws by the Australian Parliament, gained 227 retweets and 38,459 impressions.

---

\(^{34}\) [https://twitter.com/torproject/status/638346887230152704](https://twitter.com/torproject/status/638346887230152704)
Our engagements on Twitter, of which these are only a few highlights, cover a diverse readership\(^{35}\): Links to stories with a general Internet freedom theme sit alongside technical release announcements and clarifications of misconceptions about Tor in the press or online.

Outcomes:

Great campaign for relays on Libraries in support of the Library Freedom Project work. Good fast response on the Hacking team leak, which helped set the tone for the news articles that came out of that.

Our social media work is continue to be a strong outreach tool, our followers and engagements continue to grow and we continue to see the influence power of our messages.

The great storyboard for our next animation is out and this definitely a milestone achieved for us.

Challenges:

Our main challenge has always to have fast response, not only on media requests but also on events that occur with our community like the development with the Library in New Hampshire.

The ability to have this fast response depend on the mobilization of a multidisciplinary group of volunteers (trainers, developers, researchers etc). Which is always a challenge.

Successes:

**Direct working with organizations**

Working with Facebook on the recognition of .onion domains represents an excellent precedent. Not only is our .onion domain now reserved for special use, but having a massive social network like Facebook state their support for our technology is immensely helpful in demystifying the idea of Tor and the people who might use it.

When asked why Facebook did it, Alec Muffett pointed to his email on our Tor-Talk list\(^{36}\):

> Beyond all these, though, I should quote the original posting* which we made on the matter, which explains a simpler and less technical point: people access Facebook over Tor, and they will continue to do so, and their doing so is entirely valid.

> The purpose of the Facebook Onion site, atop all the other security benefits which Tor affords, is simply to provide a better experience to these people.

---

\(^{35}\) [https://twitter.com/search?q=from%3Atorproject%20since%3A2015-07-01%20until%3A2015-09-30&src=typd](https://twitter.com/search?q=from%3Atorproject%20since%3A2015-07-01%20until%3A2015-09-30&src=typd)

The ongoing collaboration with the Library Freedom Project has helped them kick off our joint project of relays in libraries, not only by offering technical support but also developing media strategies during the campaign to help the relay stay online.

We hope to continue building relationships like this that bring Tor closer to more mainstream causes, letting audiences get to know our work and tools and how they can protect the privacy of all Internet users.

**Outreach materials**

After working on many versions of the storyboards for our video explaining Pluggable Transports and Bridges to users, we now have a simple narrative capable of explaining the main points behind this very sophisticated technology to bypass censorship. The material is not final, and still requires community review and feedback before we start editing the video.

**Social Media**

Formulating a quick response to events has proved to be the surest way to set the tone for media coverage, as demonstrated by our statement regarding the Hacking Team emails release. Our continued growth in followers demonstrates that our impact is positive on that social network. Twitter is about the moment, and our usage shows that we know how to best interpret that for Tor’s outreach.

We are developing a great channel for communicating with Tor users and supporters about our software releases, mission statement, news updates and of course, building support for campaigns like the effort to put Tor relays into libraries with the Library Freedom Project. Q3 showed how influential our account has become, which is a result of work done throughout this project year.

**Media Support**

**Press:**

<table>
<thead>
<tr>
<th>Date Published</th>
<th>Media Outlet</th>
<th>Article Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/18/2015</td>
<td>Wired</td>
<td>The Dark Web as You Know It Is a Myth</td>
</tr>
<tr>
<td>07/08/2015</td>
<td>Technically Philly</td>
<td>Inside Philly’s Growing Internet Privacy Community</td>
</tr>
<tr>
<td>07/16/2015</td>
<td>Technically Philly</td>
<td>How this West Philly activist became Tor’s first director of communications</td>
</tr>
<tr>
<td>07/24/2015</td>
<td>WHYY Radio</td>
<td>Security and Privacy on the Internet, with</td>
</tr>
<tr>
<td>Date</td>
<td>Source</td>
<td>Article Title</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>07/31/2015</td>
<td>SC Magazine</td>
<td>Tor Project, Library Freedom Project to establish Tor exit nodes in libraries</td>
</tr>
<tr>
<td>08/28/2015</td>
<td>SC Magazine</td>
<td>Dark website Agora closes over Tor vulnerability suspicions</td>
</tr>
<tr>
<td>08/29/2015</td>
<td>Sunday Paper</td>
<td>Tor and the Deep Web Going Mainstream</td>
</tr>
<tr>
<td>08/31/2015</td>
<td>Statesman</td>
<td>‘Tor’ is software for keeping things online anonymous</td>
</tr>
<tr>
<td>09/10/2015</td>
<td>Motherboard</td>
<td>Privacy by design, thanks to Tor’s Jacob Appelbaum and Facebook’s Alec Muffett</td>
</tr>
<tr>
<td>09/10/2015</td>
<td>The Register</td>
<td>Monsters defeated in quest to free .onion from clutches of DNS-snooping demons</td>
</tr>
<tr>
<td>09/10/2015</td>
<td>Propublica</td>
<td>First Library to Support Anonymous Internet Browsing Effort Stops After DHS Email</td>
</tr>
<tr>
<td>09/10/2015</td>
<td>SiliconANGLE</td>
<td>Tor anonymity network benefits from .onion added as special-use domain name</td>
</tr>
<tr>
<td>09/10/2015</td>
<td>Softpedia News</td>
<td>Tor Gets Its Own TLD Special-Use Domain at .onion</td>
</tr>
<tr>
<td>09/10/2015</td>
<td>Web Host Industry Review</td>
<td>IANA Designates .Onion as Special Use Domain to Boost Security</td>
</tr>
<tr>
<td>09/11/2015</td>
<td>Motherboard</td>
<td>The US Government Pressured a Small Local Library to Turn Off Its Tor Server</td>
</tr>
<tr>
<td>09/12/2015</td>
<td>Wired</td>
<td>Russia Tried and Failed to Hack the Tor Browser</td>
</tr>
<tr>
<td>09/14/2015</td>
<td>Wired</td>
<td>Mapping How Tor’s Anonymity Network Spread Around the World</td>
</tr>
<tr>
<td>09/16/2015</td>
<td>Motherboard</td>
<td>'Dissent,’ a New Type of Security Tool, Could Markedly Improve Online Anonymity</td>
</tr>
<tr>
<td>09/16/2015</td>
<td>NPR</td>
<td>N.H. Public Library Reconsiders Support For Anonymous Internet Network Tor</td>
</tr>
</tbody>
</table>
Next Quarter’s Planned Activities:

**Pluggable Transport Integration**

A major effort in Q4 will be to overhaul the pluggable transport specification, to make it more reusable by projects outside of Tor proper. We also plan to do some documentation work before, during, and after the December PT meeting that Internews is organizing.

Depending on Brandon Wiley’s progress on dust2, it will hopefully ready in Q4 for merging into obfs4proxy.

We also have been exploring a protocol improvement for obfs4: the current obfs4 design has a protocol flaw that can in theory allow distinguishing obfs4 flows from random bytes. We hope to begin writing a specification for a next-gen obfs protocol, which includes both this improvement and better traffic padding strategies.

We plan to implement our idea for “meek-lite” -- a new module inside obfs4proxy to do domain fronting without a browser. It won’t be as convincing as doing it with a browser, but it is way lower overhead and way less surface area. This approach will be especially useful on Android, since Orbot will gain domain fronting support (albeit slightly weaker) with very little overhead.

The next quarter should show the beginning of progress on WebRTC + Flashproxy development.

Roger and Nima plan to attend the Princeton censorship circumvention meeting, including meeting with several research groups that are aiming to track reachability of various transports from inside certain censoring countries. To that end, Roger plans to work with an anonymous graduate student researcher to deploy her "idle scan" bridge reachability tests to learn whether the default-configured bridges in Tor Browser are reachable from various censoring countries.

We would like to continue exploring the “pluggable transports and improvements against surveillance” avenue, but progress there will in large part be a function of how much time Marc Juarez (as an external researcher) has for this topic.

And lastly, we’re tracking the progress of (and assisting where we can) three different university research groups that are trying to write a comprehensive “systemization” of censorship circumvention tool designs. We expect they (and thus we) will have more concrete results to make public in the upcoming months.
Testing and network simulation improvements

Though these are subject to change, here's what we have planned now:

- Ticket #17271[^37] - Set up an IPv6 testing environment
- Ticket #17270[^38] - Identify best existing tor prototype for testing
- Ticket #17273[^39] - Module isolation design written
- Ticket #13802[^40] - Instrument tor to measure time spent in different crypto
- Ticket #17276[^41] - At least one authority script tested
- Ticket #17277[^42] - Prototype at least one bad server, at least one bad client

For more information about each planned item, see the associated ticket on trac.torproject.org

Enhanced Outreach

We are planning our first training with members of the government in Germany to teach them how to keep themselves and their correspondents safe online. In Q3 the German government gave Tor a grant for our Dev Meeting in Berlin, and we have had a good relationship with them since then, culminating in this training. We will train about 30 people, consisting of civil servants from various agencies.

A variety of activities relating to our crowdfunding campaign are in preparation. We hope that this campaign will help demystify what Tor is and who supports it. Our campaign has many “champions”, or prominent supporters of Tor who are preparing different ways to publicize their support.

Our outreach team is working hard to prepare materials in advance of this campaign. We are crafting content for social media, developing special web sites for our champions, helping them with their messages, preparing briefs for the media, and many other initiatives to ensure we have a successful campaign in support of Tor.

We are also aiming to launch our video about Pluggable Transports and Bridges by the end of the year, presenting it to the public for the first time, we hope, in one or more of our regular talks at the CCC conference in Germany. This is a difficult goal given the timeframe, but we will try.

[^37]: https://trac.torproject.org/projects/tor/ticket/17271
[^38]: https://trac.torproject.org/projects/tor/ticket/17270
[^39]: https://trac.torproject.org/projects/tor/ticket/17273
[^40]: https://trac.torproject.org/projects/tor/ticket/13802
[^41]: https://trac.torproject.org/projects/tor/ticket/17276
[^42]: https://trac.torproject.org/projects/tor/ticket/17277