BBC NEWS

TECHNOLOGY

21 August 2014 Last updated at 23:02 GMT

Tor Project's struggle to keep the dark net in the shadows

The BBC has interviewed Andrew Lewman, executive director of the Tor Project.

His US-based team creates software that lets people visit websites anonymously and access otherwise hidden parts of the internet.

An article based **on the interview can be found here**, which focuses on Mr Lewman's belief that cyberspies in the US and UK are leaking his team information, frustrating their colleagues' efforts to compromise Tor's special browser software.

The following is a transcript of his wider-ranging conversation with BBC News Online's technology desk editor, Leo Kelion.

How would you describe what the Tor Project is to someone unfamiliar with it?

We're a non-profit. We do research and development into online privacy, and our main product is called the Tor Browser, which is an anonymous browser that puts you in control of your data.

This browser to access the Tor network - how would you describe what that is?

It's actually a browser to access the full internet - you just do so anonymously, and it puts the user in control of if they want to deanonymise themselves, to log into places like Google and Facebook. The Tor Network is a network of about 6,000 relays. which are servers spread around 89 countries or so. And what we do is relay your traffic through three of these relays in sort of a random order, so that where you are in the world is different to where you appear to come from. So you know you are sitting here in the UK, you start up the Tor browser. You could pop out from Japan, Argentina, the United States.

Do you have any idea of how many people are now using the Tor Browser?

We do. We have some funding from the US National Science Foundation, and we believe within a factor of 10 that it's around 2.5 million daily users. We actually have a website that publishes everything we collect. So people and researchers can look into our data and find new things that we haven't discovered yet.

How is that spaced out across the world - are there particular countries where it is more popular than others?

Surprisingly, the majority of our users are in the US and Europe - people concerned about privacy. But we also have people in places like Russia, Iran, Vietnam and China as some of our top countries with users.

Bearing in mind the whole point of Tor is to protect anonymity, do you have any insight into the type of people using it?

Generally no. There is no registration. We do not collect any demographics about users or any information. Users will voluntarily say why they use Tor, and we have some samples on our main home page that list out typical users. But for the most part we have had 150 million downloads of Tor browser in the past year - so we don't really have any idea of who is using Tor on a daily basis. Nor do we want to know

After allegations made in the Edward Snowden leaks about the activities of NSA [US National Security Agency] and GCHQ [UK Government Communications Headquarters] cyberspies, there is concern among many members of the general public about surveillance on the net. Do you think we should all be using Tor now?

I think everyone should use Tor when they need to use it. I think that if your only adversary is the NSA or GCHQ you've probably already lost that battle, because they are multibillion-dollar agencies with fantastic capabilities, and a single tool... much like you cannot build a house with just a hammer, you need a whole toolbox and a whole set of practices to be able to defeat adversaries like that. However, the average person is mostly worried about spreading their information online, unscrupulous advertisers taking advantage of leaked data... and for the same reason that you close the door to go into your house, some people just don't want to leave a trail of data where they've been on the internet.

There's been a lot of reports about different groups wanting to overcome the anonymity that your provide. How big a threat to Tor is that?

It's a concern. It's something we hypothesised and are working against. In computer science it's called the perfect adversary, where there's total awareness of everything going on and everything you can do globally. We're not quite there yet and no tool is actually there yet. But that's one of our goals - to protect users from a global adversary, assuming you can take risks and steps and know what is going on.

A few years ago if we had talked about the dark net and Tor specifically, a lot of people would have been scratching their heads. Nowadays that has changed. Has being thrust into such prominence caused problems for the Tor Project?

It's been more challenging, because we now we sort of have many more eyes, looking at what we do, scrutinising everything we do. Constantly questioning, should we do this, should we do that? For the most part, though, we continue to work on the same core principles we have for the past 10 years. And, you know, we will continue to do so. At the core, we are researchers, and we do research. And our software is an example of what we would write if we were going to write software. And hundreds of millions of people are now relying on Tor - in some cases, in life-and-death situations - and that's what we pay attention to. We would be very sad if anyone was arrested, tortured and killed because of some software bug or because of some design decision we made that put them at risk.

But if you read about some of the reports and bounties being put up to overcome the protections you offer - is there concern that the project is a small group of people and there are huge amounts of effort being put against it?

We are around 30 people in total, and think of the NSA or GCHQ with their tens of thousands of employees and billions of pounds of budget. The odds there are obviously in their favour. With the bounties and things it's sort of funny because it also came out that GCHQ heavily relies on Tor working to be able to do a lot of their operations. So you can imagine one part of GCHQ is trying to break Tor, the other part is trying to make sure it's not broken because they're relying on it to do their work. So, it's typical within governments or even within large agencies that you have two halves of the same coin going after different parts of Tor. Some protect it, some try to attack it.

If you look at the funding, an awful lot seems to be coming from the US government at the same time people in the NSA are reportedly trying to compromise the anonymity offered. How would you describe your links with the US government?

They are pretty good. The people in the US government who fund us really want privacy and anonymity to exist. They heavily want to rely on Tor for censorship circumvention. So in less free countries where the internet is heavily censored, they want the average person to be able to use the internet as they see fit. We obviously don't have any funding from the NSA or the people who hate us, but that's fine because there's plenty of people who do love Tor and want to see it exist in the world. And that's why they keep funding us.

When you talk about the people who hate us, are you talking about people in the security world?

Right. So there's people in the security world who want to control everything, who want a magic button to be able to deanonymise anyone at will. And then there are plenty of other people that counter that and say: "No, that's not the kind of government I want. This is not the society I want to live in. And Tor needs to exist, so let's keep funding it."

Bearing in mind you are part-funded by the US government, what opportunity do you have for pushback? To say you can't both fund us and be out to destroy us?

The US government is not one entity, thankfully. It's many many factions within departments within agencies. And the people who fund us already understand - we don't need to convince them of anything. They already get it, they already understand why they want to fund Tor, and they understand what we do. One thing in our favour to stop any subterfuge is that everything we do is public. Our code is public. our designs are public, our project plans are public. Everything we do is transparent and public, including our finances. And this stops - we like to think it stops a lot of possible subterfuge and questionable actions because everyone knows that everything we do is going to be out there in public and open for scrutiny.

Do you think you can resist attacks on Tor indefinitely, or if they continue and are well funded will Tor inevitably break?

I think it's been interesting that since the Snowden exposures we've had a lot more people coming to help us, and a lot more people coming to sort of say, "You're a tiny little project and you're being picked on by huge bullies, let me help you, let me bolster your cause from advocacy, from code, from cryptography, from design - and, you know let us help you." So it's been great that sort of the crowds have come to help us take on this fight we didn't really ask for. But it's been good. I think that at some point there will always be attacks, there will always be software bugs - we are human, we will always make mistakes, but with many eyes trying to help us we seem to be getting better.

One of the other issues that you face is illegal activity on Tor. Buying and selling illegal drugs, paedophilic images and other illegal pornography, and a host of other unlawful activities. What are your concerns about Tor being used in that way?

We don't like it. This is why we work with law enforcement. I spend a lot of time working with many, many three, and four and five-letter agencies around the world. From Interpol to Soca in the UK - the Serious Organised Crime Agency - you know, the FBI, DHS [Department of Homeland Security] in America. There is a whole raft of organisations that we've spoken to to explain how Tor works, to explain what Tor does and does not do, and there are some very smart people there who understand what Tor can and cannot do. They are interested: one, to use it to catch criminals; two, because they use it themselves and they want to know what weaknesses the criminals can discover due to weaknesses in Tor, to protect their agents and let them do their jobs. On the more philosophical level, criminals are opportunists. They will use any technology, anything whatsoever to be able to do their crime. I work with a lot of victims of human trafficking and domestic violence, and in many cases the Apple iPhone is their nightmare device - but no-one ever goes after Apple for Facetime. You see Apple advertising Facetime for the travelling father talks back to his kid when he is in some foreign location. But at the same time for £1,000 an hour you can watch a live abuse session through Facetime and Apple works with the police just like we do to try and stop crime. And with the smart people in all these agencies, they seem to do be doing just fine with old-fashioned police work. Figure out a motive, they are out collecting suspects, start doing investigations. It doesn't matter which technology you use, smart officers will make the difference. As you've seen with all these paedophilia rings and online drug busts going on. It doesn't matter if it's Tor or not. A smart officer is a smart officer, and that's the asset.

But on a personal level. does it bother you that the work you are doing is being misused in this manner?

On some level, yes. On the other level, of all the activists and people who work on human rights that also rely on Tor, and those seem to vastly outnumber the actual criminals using Tor. Tor is spun out to be some big bogeyman to scare people into giving agencies more funding, and that's exactly what I'd expect agencies to do. This has been true of when it was horse and buggy, the trains came in the UK and the police wanted extra funding to handle all the criminals travelling by train, and then they want extra funding when the road system went in - you know, the highways and interstates. It's a typical thing that when new technology comes, police ask for more money to defeat it. And this is just par for the course. What we are encouraged about, what we keep working on, is the person who is in a dire situation, who heavily relies on Tor to make their life and the life of their countrymen better. So, that's what we focus on.

When the police come to your organisation for help, is it only advice that you can give or is there technical help you can provide?

In many cases because of our expertise in all things technology and privacy, we are advising them on, you know, so and so is

sending emails, so and so is using chat messaging, so and so is using video chat etc. Here are all the things to look at. And from the officer's perspective they have a crime to investigate and about a million technologies to understand. You know, we're not experts in everything, but we're pretty good at peer-to-peer, and Tor-related, security-related technologies. So we can help advise them, like, here are some other things to look at. No human is perfect. You know, when botnets, and criminals are using these stolen identities, proxy servers and all this other stuff, most criminals leave a lot of data because they are not much smarter than the less-than-average person. So it's generally - understanding... let's walk you through things you can think about and here are all the possible avenues of investigation. And then the officer goes back and says here are all these things I got from Tor. Just because someone is using Tor, there have been plenty of cases I've been involved in when someone uses Tor completely incorrectly and there are horrendous cases. Crimes have been committed and Tor is just one part. They'll steal identities, they will steal cars, it's a whole raft of things. But the officer has the idea, let me go ask the expert in each technology about what they can do to figure out who this person is.

Tor has become synonymous with the phrases dark net and dark web. Do those phrases bother you as they have meanings to people, and often they mean illegal or illicit activity?

So we may be called the dark net, we like to call it the deep web. What you see on the surface with Google and Bing search engines, the typical sites that everyone visits are the tip of the iceberg. What's under the iceberg is vast amounts of content, and the term dark net actually comes from a Google or Alta Vista - if you remember that search engine from 15 years ago - from a presentation they did about here's all the data that is locked behind paywalls, locked behind log-in screens, in corporate networks. And if your goal is to crawl all the world's information, what is dark to you is the things you can't crawl. And this includes your bank account, your email account and other things like your corporate file shares and all of this. The dark net term is sort of a misnomer, it's mostly dark because search engines can't see it. But the term seems to have stuck.

But is it an unhelpful phrase? It seems to have stuck - or does it not bother you that much?

We would like people to use deep web or hidden web, but you know, people seem to like the word dark web, and it's become the popular vernacular, and there's not much we can do about it.

Bearing in mind how much is reported about the illegal drug sales, the illegal images, does Tor have an image problem?

I think to the average person on the street they are ambivalent to Tor. I mean, what's nice is since the Snowden disclosures, when you talk about privacy people have an opinion. Over a year ago, before Snowden, people would say: "Privacy? I have nothing to hide, there's nothing to worry about." Now they have an opinion, they'll see it one way or the other. And that's a great sort of concept or meme to get out there. That people have it on top of their head, they have an opinion and they want to do something about it. I don't know that Tor necessarily has an image problem, because for every 10 people you ask, about 50% say: "Yeah, I've heard about Tor, you know I don't really care so much." But the other half will say: "I love Tor, I use it all the time, anyone who uses it should be protected and, you know. revered."

There are alternatives to Tor - I2P, Freenet and others. Is your sense that some of the potential terrorists or other illegal activity has moved away from Tor because there is so much scrutiny of it?

So the peer-to-peer, privacy and anonymity software market - if you include Freenet, I2P and VPNs and SSL proxies and things like that - has just grown tremendously. And interest in it has grown tremendously. So there is a sort of rising tide where all of us are benefiting from it. Tor seems to be the one taking the brunt of the press, and being the public face of this whole industry, which is fine. We're happy to do that. But that also means that we also get all the critics, and the commentaries have been about Tor. I think terrorists, much like criminals, will do the exact same thing and use whatever they can. And what has come out in a lot of research has been that, you know, terrorists are pretty brazen. If you are willing to die for your cause you don't want to hide your identity. You want to be out there in public and say, you know: "I am John Smith, here is what I am going to do, watch me do it." They want the attention. They don't want the secrecy and the privacy that comes with a lot of these tools.

We were recently expecting two researchers from Carnegie Mellon University [in Pittsburgh, Pennsylvania] to explain how they had compromised Tor's anonymity - but the talk was pulled. What's your thoughts on what went on?

So, we heard about it and Cert - which is the computer emergency response team - or task force gave us a little bit of a heads-up

and said: "You know we have this attack and blah blah blah." And then the Black Hat talk showed up, and it seemed really tied closely to the Cert team. And we sort of said: "Wait. We're the vendor, what are you sort of attacking us?" Then lawyers got involved, and that's never a good sign when you are having a conversation with the authors of a paper and suddenly lawyers jump in and say: "No comment." And it seems like the core question is that we don't have the details of the attack, whatever attack they claim to have done. And I think, really that there is a human research, human ethics component to this that. They did research on live people and possibly exposed and put people at risk. And any ethics review board, any university would generally stop that or put a lot of controls in place to say: "What are you doing?" Just as you can't experiment on humans off the street. Why can you do it on the internet? And in general, we'd still like to talk to the researchers. What generally happens is that researchers say: "Hey, I'm writing a paper and I found these following flaws, here is how we suggest you fix them. And we're still going to go public with our paper, but we wanted to give you a chance, we wanted to do responsible disclosure to give you a chance to fix your bugs first before we go public." In this case it seems like they wanted to go public first for the press attention and not actually give us the chance to fix anything, and not to take the users at risk and make them less at risk.*[Carnegie Mellon University has declined to comment on why the talk was cancelled]*

Bearing in mind they haven't passed on those details still, to what extent does that leave Tor exposed?

So we spent a lot of time from the hints that we had and from some other sources that may have anonymously leaked data to us, we've got a good idea of what we think they've done and we think we've fixed it. We've done a lot of simulations and a lot of testing, and on the whole, the whole general area of what they were attacking, we believe we have fixed it. But this is where we rely on a lot of academic researchers. There are a growing number of people who are getting their PhD or their master's on Tor and Tor-related technologies. And they find some good bugs and they find some good design decisions - that maybe you should think about X instead of Y, maybe you should think about A instead of B. And they back it up with data. So we think we have a pretty good idea as to what our exposure is, at least in that aspect. But with any software… this is why we say if Tor is your only tool in your toolbox you have already lost. If you are only relying on one tool, you need layers of security in order to be safe. And just like building a house, you don't build it with just a hammer. You need nails, you need screwdrivers, you need pliers, you need wrenches, you need wood - you need all of this stuff. You can't just have one tool and say: "All right, I'm going to conquer the world."

With the growth of the popularity of Tor, you need more servers to keep the service running. Are you facing a problem because of the controversy associated with some of the activities that people get up to that universities aren't as willing as they would have been otherwise to provide the facilities to you?

I think it's beyond universities. I think that since the Snowden disclosure many people want to help out. During the Arab Spring in North Africa and the Middle East there was a groundswell of support. And people said: "You know what, I'm going to run a relay because I want to help people in North Africa. I want to help Tunisians, I want to help Egyptians, I want to help Libyans." And for the same reason we get people who say: "I want to run a relay because I don't want a government that spies on me holistically. I want a relay because I know so-and-so and she was a domestic violence victim and I want to help protect her." So there is all sorts of reasons to run relays, people have lots of bandwidth at their home connections now and they are happy to give up some of it to run Tor. The scaling question though is - you know we have some large companies looking at Tor and wanting to say: "We want to roll Tor out on our premiere device to the scale of 70 million devices. Can you scale that far?" And right now the answer is no. Nobody has ever tried to scale a Tor network to tens of millions of devices and we're working with them on engineering questions on how we do this. These are fine problems to have, these are problems of growth, and you know I know that we will get there.

But is there a danger you fall victim to your own success? More people end up wanting to use Tor than you can support?

That's always been a danger. But so far with 2.5 million daily users and 6,000 relays we seem to be doing just fine. So long as we can sort of keep that ration of users to relays, we seem to be doing just great, and we can probably scale to 100,000 or even maybe one million relays easily before we have to do some serious hard work as to think about our - going from millions of relays to tens and hundreds of relays is a whole different ball game, and a ball game that we're happy to get into.

Back to the issue of the security services. Presumably from the NSA's point of view it would want to monitor Tor to head off potential terrorist threats. How concerned are you that your software could be used to help terrorism?

So anonymity loves company. The more users we have the better off everyone's anonymity and protection is. We're not that

concerned. Somehow we'll eventually learn what bugs, if there are bugs, that the NSA and GCHQ are using and we'll fix them. There are plenty of people in both organisations who can anonymously leak data to us to say maybe you should look here, maybe you should look at this to fix this. And they have.

You're saying there are people in the NSA and GCHQ who go behind their bosses' backs to give knowledge to you to fix potential flaws in Tor?

Right. We're one of the few open source projects that take anonymous bug requests - completely anonymous. We don't need your email, we let you log into our bug track anonymously - many people do it through Tor - and they report these fantastic bugs that if you think through, someone with a lot of experience and a lot of time has researched this bug and said: "Maybe you should look here, maybe you should fix X, Y and Z." Sometimes it includes a patch that says: "Here's my code fix." And we look through all this stuff very carefully, and we've been totally impressed by the quality of bug reports that we get both on the software side, which is a coding error - sometimes very, very subtle - or on the design side, where you know you guys made a design decision here and maybe you want to consider some other use cases

Are you 100% certain these people who are providing the information work for the security services, or is this a hunch?

It's a hunch. Obviously we are not going to ask for any details. Many people - you have to think about the type of people who would be able to do this and have the expertise and time to read Tor source code from scratch for hours, for weeks, for months and find and elucidate these super-subtle bugs or other things that they probably don't get to see in most commercial software. And the fact that we take a completely anonymous bug report allows them to report to us safely.

How often would you say it is that you receive reports from someone you think must come from one of the security agencies?

Probably monthly. People come around and say: "Can you explain what this is, can you explain what that is?" And we always have a grain of salt there where we think they are trying to figure out a bug to exploit or they are actually trying to leak to us that there is a sort of bug in the code and you should look hard at this.

Is it people who are undermining the work of their colleagues tasked with compromising Tor, and if that is the case why is this is going on?

So I've had conversations with William Binney, who is one of the NSA whistleblowers, and it's very sort of fascinating that he is in contact with many people in the NSA and he says, specifically to the NSA, that people are very upset that they are spying on Americans and doing lots of other sorts of stuff. There's a lot of groundswell of support as to what is going on, but at the same time there's the other half of the organisation that is: "You know what? People shouldn't have privacy," and "Let's go out and attack these things." So there is always a balance between those who protect our freedom and liberty and those who don't want you to have it.

Is there anything else you'd want to add that we have not covered already?

No. Tor exists for all the reasons of internet freedom and putting users in control of their data. And that's what we'll continue to do and we'll continue to research going further.

Some of the questions have been edited for the sake of clarity.

More Technology stories

NSA and GCHQ agents 'leak Tor bugs'
[/news/technology-28886462]
The Tor Project says it believes some NSA and GCHQ agents are surreptitiously leaking it information to protect anonymity on the net.
Social network cannot stop IS posts
[/news/technology-28882042]
Aircraft to have 'human-like skin'
[/news/technology-28881748]