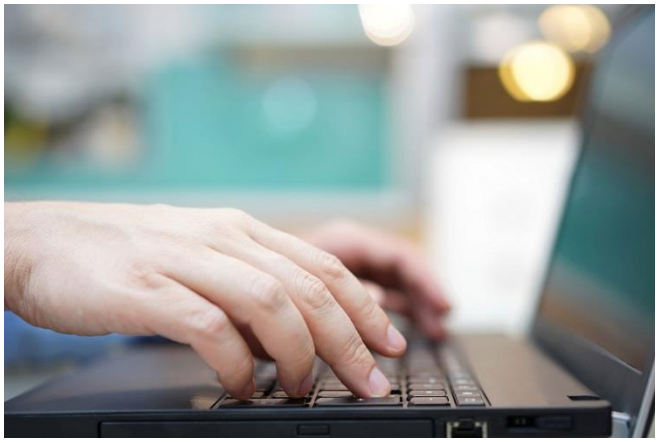
HOUSES OF PARLIAMENT
PARLIAMENTARY OFFICE OF SCIENCE & TECHNOLOGY

POSTNOTE

Number 488 March 2015

The darknet and online anonymity



Technologies that anonymise internet users have become increasingly popular in recent years. They help citizens to protect their security and privacy and to circumvent censorship. They also facilitate organised crime, such as the billion dollar drug market known as Silk Road. This POSTnote discusses the challenge of preventing such crimes without compromising the other uses of anonymity technologies.

Overview

- The term 'darknet' is used to refer to websites whose operators can conceal their identity with sophisticated anonymity systems.
- With an estimated 2.5 million daily users, Tor is by far the most popular anonymous internet communication system.
- It allows internet users to access the web and to create websites called Tor Hidden Services without revealing their identity.
- Tor is used for journalism, whistle-blowing, law enforcement investigations and the circumvention of internet censorship, as well as for drug dealing and other crimes.
- There have been several large law enforcement operations against criminal activities on Tor. It is not publicly known how law enforcement agencies de-anonymise criminal Tor users or the extent to which this involves surveillance of non-criminal users.

Background

The vast majority of web pages are invisible to most casual internet users. This part of the web is known as the deep web. In contrast to the open web, it consists of pages that cannot be found by popular search engines like Google. Most of these pages are standard personal or corporate pages such as intranet pages, administrative databases or personal photo collections. A very small proportion of websites in the deep web use sophisticated anonymity systems, which allow their operators to conceal their identity if they wish to. This part of the deep web is commonly referred to as the **darknet**, for example in recent media articles and parliamentary debate, and it is how the term is used in this POSTnote. Elsewhere, 'darknet' has been used to describe criminal content on the open web or private networks used for illegal file sharing. Darknet is also used interchangeably with the terms 'dark web' and 'dark net'.

Most internet users who wish to hide their identity take simple measures, such as using pseudonyms on social media sites or clearing the web browser history from their computer (Box 1).[1] A small proportion use sophisticated anonymity systems that offer stronger protection (see Box 2 for an overview of these systems). The most popular anonymity system is called 'Tor'. In 2014, Tor had an estimated 2.5 million daily users. A very small fraction of their activity was associated with hidden websites called Tor Hidden Services (THS) that various providers have set up. Most of the debate on the so-called 'darknet' is concentrated around THS. Tor is also the focus of a number of ongoing investigations by UK Law Enforcement Agencies (LEAs) and it is the main focus of this POSTnote, which explains:

- how Tor works, who develops it and what it is used for
- the measures that LEAs can take to de-anonymise users of Tor who are involved in crime
- future options to prevent criminal activities on Tor
- how concerns about online privacy may affect the future use of systems like Tor.

What is Tor

The development of Tor started as a research project in 1995 at the US Naval Research Laboratory.[2] The Tor Network (Box 2) became operational in 2003 and since 2006 it has been maintained and improved by Tor Project Inc., a US non-profit organisation with about 30 employees. In 2014, Tor Project Inc. received funding from the

Box 1. How is the identity of internet users revealed?
Without taking anonymity protecting measures, users of the open web reveal numerous items of information. These can be used in combination to track the online activities of a computer and help to reveal the identities of individual users.

- **Content**: Postings on public forums or social media sites may reveal the identity of internet users. Unless encryption is used (POSTnote 270), private information like the contents of emails can be monitored by anyone with access to the relevant network infrastructure although this is technically challenging.
- **IP address**: Every device requires an Internet Protocol (IP) address to be able to request and receive content from websites. The IP address can be recorded by the website operator. The IP address can sometimes be linked to an individual user (via their Internet Service Provider or ISP), but this can be difficult. For example, one IP address may be shared (for example within a household or company) and addresses are frequently re-allocated as users connect and disconnect from the internet. Sometimes it is not even possible to deduce a users' ISP from the IP address.
- **Cookies**: These are small text files that certain websites place on the computer of an internet user to store information about their activity. For example, Google uses cookies to remember a user's recent search terms and language settings. However, the information contained in cookies is sometimes passed on to third parties who may use it for targeted advertising.
- **Browser fingerprint**: Web browsers such as MS Internet Explorer or Mozilla Firefox have a 'fingerprint' that is made up of information on the user-specific browser version and configuration. Websites can use this fingerprint to recognise returning users, even without cookies.

Box 2. Online anonymity systems
Online anonymity systems can be categorised into systems of centralised and distributed trust. In centralised trust systems, for example Virtual Private Networks (POSTnote 436), a single entity (usually the provider of the service) can know the identities of all users and their communication partners. In contrast, distributed trust systems are designed so that no single entity (not even the designers or maintainers of the service) knows the users' online behaviour. For example,

- **Tor** is based on 'onion routing'.[4] It has two main parts: (1) approximately 6,000 computers provided by volunteers and forming a global network of nodes, called the Tor Network and (2) free software running on a user's computer and enabling access to the Tor Network. Users' data are encrypted in multiple layers and relayed through several (usually three) out of these 6,000 nodes before reaching their destination. At each node, one layer of encryption is removed (like the layers of an onion) before the data are passed on to the next node. Each node in the path knows its predecessor and successor, but not the other nodes in the path. This makes it difficult for any single part of the system to link communication partners.
- **The Invisible Internet Project (I2P)** is similar to Tor, but is designed for the use of hidden websites rather than the anonymous use of the open web. I2P is developed by anonymous volunteers. Compared to Tor, it is less well researched and has fewer users.
- **Freenet** is designed as a tool for sharing files anonymously and has been used to distribute censored information. Files shared by users are split into encrypted blocks and stored across the computers of other Freenet users.

Bureau of Democracy, Human Rights and Labour of the US Department of State, the Defence Advanced Research Projects Agency (DARPA) of the US Department of Defence, the National Science Foundation, as well as private organisations and donors.[3] Tor relays a user's data through the Tor Network (Box 2), which hides the user's Internet Protocol (IP) address and other identifiers (Box 1) from the websites they visit and disguises the user's online activities. This means that anyone monitoring internet communication will find it difficult to trace these activities back to a specific user. One of the main reasons for Tor's popularity is that users do not need to have a sophisticated knowledge of computers. The software enabling access to the Tor Network can be downloaded from the internet for free and is easy to install on a computer. It can also be used on mobile phones.

Tor allows users to do two distinct things:

- use the open web anonymously with the Tor Browser, which looks similar to common web browsers such as Microsoft Internet Explorer or Mozilla Firefox
- publish anonymous web services as Tor Hidden Services.

Anonymous use of the open web

There is little published research on how Tor is used. Tor Project Inc. states that most traffic (approximately 98.5%) on the Tor Network was from users accessing the open web; the remainder was to access THS. Tor Project Inc. and experts provide the following specific examples of why people use Tor to access the open web:

- **Circumventing censorship**: Researchers and journalists can use Tor to access information censored in their countries. For example, in China web services like Facebook, Twitter or the BBC News website are blocked by what is referred to as 'The Great Firewall of China'. During the Arab Spring in Egypt, the use of Tor in the Middle East increased as governments responded to uprisings by blocking websites and prosecuting activists.
- **Anonymous activism and journalism**: Tor enables journalists and dissidents to report without identifying themselves or to communicate securely with informants. The organisation Reporters Without Borders recommends Tor and offers training in its use.
- **Under-cover online surveillance**: LEAs can use Tor to access potentially criminal websites without revealing their Government-specific IP address to the website owner. Tor is regularly used by the Internet Watch Foundation, which detects and removes child sexual abuse material from the internet.
- **Protection from criminals**: Victims of digital abuse such as cyber-stalking have used Tor to protect their personal security and privacy.
- **Anonymous peer-to-peer file sharing**: The results of a study in 2010 suggest that, although only a small fraction of Tor users engage in peer-to-peer file sharing via the BitTorrent protocol, these users are responsible for more than 25% of the data exchanged on the Tor Network.[5] This is a similar picture to the use of BitTorrent on the open web. The authors of the study estimated that a large proportion of the shared material was copyright protected such as films and music files.

Anonymous websites via Tor Hidden Services

THS are websites only accessible via the Tor Network. THS addresses end with ".onion", instead of, for example, "co.uk" which is why they are referred to as 'onion addresses'.

The IP address of the server hosting these websites is protected by Tor, so its location is not easy to identify, unless the operator of the THS chooses to reveal identifying information. While it is relatively simply to use Tor to access the open web, access to THS is less straightforward. THS sites are not indexed by common search engines such as Google and Bing, and so can be difficult to find. There are, however, THS search engines emerging such as ahmia.fi, which allows users to identify THS related to specific content. Some THS can also be accessed from the open web by replacing "onion" with "tor2web.org".

Also, open web addresses typically indicate something about their owner or content, but THS typically do not. For example, https://3g2upl4pq6kufc4m.onion is the THS address of the search engine known as DuckDuckGo. There are exceptions, for example, https://facebookcorewwwi.onion is the address to access the social media site Facebook from within the Tor Network.

Contents of Tor Hidden Services

There is no central record of all existing THS and not all THS addresses are published. This makes it difficult to give an accurate overview of the contents of THS. Moreover, the landscape of THS changes quickly so that any analysis is merely a snapshot of THS available at a particular point in time. The few studies presenting THS metrics show that on average there are approximately 45,000 unique onion addresses present on each day.[6,7] A study in 2013 identified 39,824 onion addresses, 38,011 of which could not be analysed. Almost half of them were not accessible at the time of the analysis and about a third linked to sites generated automatically by computers infected with a botnet malware (POSTnote 389). Of the 1,813 addresses that could be analysed 44% linked to THS devoted to adult content, drugs, counterfeit products and weapons and 56% linked to THS devoted to politics, anonymity and other topics.[6] Of the 1,813 addresses, the most requested were those that linked to THS related to pornography. A separate, more recent study suggested that THS hosting child sexual abuse material are requested by far the most often.[7] However, there are several reasons to question how representative these and other studies may be. Tor Project Inc. is currently working to make THS more amenable to statistics gathering as part of a program by DARPA.

Examples for the contents and purposes of THS are:

- **Criminal markets**: Until September 2013, the most prominent hidden market place on the Tor Network was Silk Road. It allowed users to sell and buy illegal drugs and other commodities in a format similar to that of eBay. From its launch in February 2011 until July 2013, the site processed over $1.2 billion worth of sales between 4,000 vendors and 150,000 customers. Silk Road was taken offline by the US Federal Bureau of Investigation (FBI) in October 2013. Several other illegal markets rapidly took its place.
- **Indecent images of children**: The Child Exploitation and Online Protection Command (CEOP) of the UK National Crime Agency says that THS play only a minor role in the online viewing and distribution of indecent images of children. In 2013, the Internet Watch Foundation took action on 36 THS for containing such material, compared to 1,624 domains (POSTnote 279) on the open web. According to CEOP, Tor is less popular among offenders because it decreases the speed at which images can be downloaded.
- **Terrorism**: Some security experts suggest that terrorists use THS to share information without revealing their location to security agencies. Others are sceptical and emphasise that the open web offers numerous other covert communication channels that terrorists can use.
- **Whistle-blowing**: THS allow whistle-blowers to share information with the media and advocacy groups. For example, the New Yorker Strongbox is a THS that allows informants to share messages and files anonymously with reporters of the American magazine The New Yorker. Also, the THS MafiaLeaks was introduced to break through the code of silence that protects the Mafia by enabling citizens to submit information about Mafia activity anonymously.

Preventing crime on Tor Hidden Services

Preventing criminal activity on THS presents LEAs with a major challenge. Under the 2000 Regulation of Investigatory Powers Act (RIPA; POSTnote 436), LEAs may seek information about a user's online behaviour from Internet Service Providers (ISPs). However, Tor is designed so that no single entity (including ISPs and Tor Project Inc.) knows about a users' online behaviour, such as which websites they visited. Therefore, LEAs need to pursue more complex methods to find out about the online behaviour of a Tor user.

De-anonymising Tor users

While there have been occasions where LEAs have de-anonymised Tor users of specific sites (Box 3), it is not publicly known what the extent of their capability is and what methods they use. There are two possible approaches:

- **Exploiting technical limitations of Tor**: Tor Project Inc. notes that the design of Tor has made some trade-offs between security and usability which might make it possible to de-anonymise Tor users by exploiting technical limitations of Tor. However, this requires a high level of computer expertise and significant resources. In a leaked document from 2007, the US National Security Agency (NSA) stated that it "will never be able to de-anonymize all Tor users all the time", but with "manual analysis" a "very small fraction of Tor users" can be de-anonymised.[8]
- **Exploiting user mistakes**: People may make mistakes in the use of Tor. For example, Tor users sometimes choose the same pseudonyms or make distinct comments on both hidden services and the open web that allow them to be identified by non-technical means (Box 3).

Future options

Identifying criminals using Tor is time consuming and it requires a high degree of skill. LEAs are unable to disclose full details while an operation is still ongoing, which fuels speculation over the extent to which such operations involve surveillance of non-criminal Tor users. Proponents of privacy protection have voiced concerns that uncertainty over the extent of online surveillance could itself affect the public's online behaviour. They say there is a need for legislation that clarifies the legal pathways LEAs can take to identify internet users. They also emphasise the importance of privacy considerations being factored into the authorisation, on-going scrutiny and oversight of such investigations.

Tor without Tor Hidden Services

There is widespread agreement that banning online anonymity systems altogether is not seen as an acceptable policy option in the UK. Even if it were, there would be technical challenges. For example, when the Chinese government attempted to block access to Tor, Tor Project Inc. introduced secret entrance nodes to the Tor Network, called 'bridges', which are very difficult to block.

Some argue for a Tor without hidden services, because of the criminal content on some THS.[9] However, THS also benefit non-criminal Tor users because they may add a further layer of user security. If a user accesses a THS the communication never leaves the Tor Network and the communication is encrypted from origin to destination. Therefore, sites requiring strong security, like whistle-blowing platforms are offered as THS. Also, computer experts argue that any legislative attempt to preclude THS from being available in the UK over Tor would be technologically infeasible.

Collaboration with Tor Project Inc.

Tor Project Inc. has supported a large number of LEAs in the US and Europe by explaining how to use Tor for LEA operations and how criminals may use it, as well as by developing tools and documentation that can assist LEA operations. However, they would not be willing to specifically advise LEAs on ways to exploit limitations in the Tor software. The Executive Director of Tor Project Inc., Andrew Lewman, says he would like to intensify collaborations with LEAs and policy makers in the UK.

Future development of anonymity systems

There is a longstanding debate over the extent to which citizens have a right to be anonymous online. Proponents of privacy protection see anonymity as an important aspect of freedom of speech, but opponents say that anonymity reduces accountability and leads to unethical and criminal behaviour.

Effects of Tor Hidden Services on crime

THS may create criminal communities, where immoral behaviour and crimes are discussed openly. This can re-affirm offenders in their belief and amplify the extent of their criminal behaviour.[9] On the other hand, it has been argued that online drug markets like Silk Road transfer parts of the drug dealing business from the streets to the internet and may shorten the supply chain from drug producers to consumers. Some say this can reduce the number of drug-related crimes like robbery and shoplifting, and thus lower the social and economic costs of drug misuse.[10]

Future Tor use

Tor Project Inc. plans to make Tor faster, easier to use and to increase its capacity. In response to public concerns about privacy, more people may start to use strong anonymity protection systems like Tor. Also, organisations involved in providing browser and operating system software are increasing the level of privacy and anonymity they offer to their users. For example, the non-profit organisation Mozilla Foundation, which offers the popular Firefox internet browser, has recently announced its collaboration with Tor Project Inc. on a project evaluating the use of Tor with Firefox on a larger scale.

Box 3. Investigations against criminal Tor Hidden Services

Malicious software attacks

In August 2013, computers of people accessing THS hosted by servers of the company Freedom Host, were infected by malicious software. This software exploited a security flaw in Mozilla Firefox, which the Tor Browser is based on. It caused the IP address and other identifiers of infected computers to be sent to a central server in Virginia, US. Among the affected THS were child pornography websites, but also legal services. Before the attack, the FBI had taken control over Freedom Host, which has led some computer experts to suggest that the FBI was behind the attack.

Silk Road shutdown

In October 2013, the FBI arrested the alleged operator of the illegal market place Silk Road, which was operated as a THS. In the criminal complaint, the FBI describes that the suspect was identified as the Silk Road operator based on his activities on the open web, including posts about Silk Road on discussion forums, where he registered using his real name and email address. However, it is not publicly known how the FBI identified the IP address of the server hosting the Silk Road.

Operation Onymous

About a month after Silk Road had been taken offline, the THS Silk Road 2.0 was launched to continue the criminal market activities. On 6 November 2014, the international operation Onymous, which involved LEAs of 16 European countries and the US, led to the shutdown of more than 400 addresses linking to 27 distinct THS, including Silk Road 2.0. It is not publicly known whether the servers hosting these sites were located by an attack against the Tor Network as a whole or because of mistakes by the people operating the THS. LEAs stressed that the operation showed that cyber-criminals were not safe from prosecution even if using Tor Hidden Services.

Endnotes

1 Pew Research Center, 2013, http://goo.gl/59aYcp
2 Syverson, 2011, ACSAC '11, 123-135
3 Tor Project Inc., 2014, http://goo.gl/3hsB0e
4 Dingledine *et al*, 2014, http://goo.gl/tNVEWt
5 Chaabane *et al*, 2010, NSS '10, 167-174
6 Biryukov *et al*, 2013, arXiv preprint arXiv:1308.6768
7 Owen, 2014, 31C3, http://goo.gl/1dF7m7
8 The Guardian, 2013, http://goo.gl/0q0b3s
9 Guitton, 2013, Comput Hum Behav, 29, 6, 2805-2815
10 Bartlett, 2014, *The Dark Net*, William Heinemann, London

POST is an office of both Houses of Parliament, charged with providing independent and balanced analysis of policy issues that have a basis in science and technology. POST is grateful to Thomas Kriechbaumer for researching this briefing, to the Engineering and Physical Sciences Council for funding his parliamentary fellowship, and to all contributors and reviewers. For further information, please contact the co-author, Dr Chandrika Nath.