CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Emin Çalışkan, Tomáš Minárik, Anna-Maria Osula

Technical and Legal Overview of the Tor Anonymity Network

Tallinn 2015

www.ccdcoe.org
publications@ccdcoe.org

Technical and Legal Overview of the Tor Anonymity Network

1. Introduction

The Tor anonymity network keeps making the headlines. The notorious Tor Stinks presentation,[1] as well as the Freedom Hosting[2] and Silk Road 2.0[3] cases, are just a few examples of the use (and abuse) of this software that was initially built to help its users anonymise their location and that of their websites and other services.[4] Judging from recent developments, and much to the dismay of several governments,[5] the use of anonymisation technologies such as Tor will continue to thrive.

Despite the attention that Tor has received worldwide, the technical and legal questions surrounding it remain relatively unexplored. One of the reasons for this is that most Tor users, relay providers, and cyber security researchers have a limited knowledge of the possible legal implications surrounding the use of Tor. At the same time, most legal researchers may not be familiar with Tor's technical aspects or have not fully grasped the demand for anonymisation solutions being echoed by different layers of modern surveillance societies.

We find these underexplored questions fascinating. Does Tor grant its users 100% anonymity? How can public authorities detect, investigate and prevent crimes committed with the help of Tor? Can they use Tor themselves in their activities? What is the role of the exit node operators? Would it not be easier to simply ban the use of Tor altogether? And who needs Tor anyway?

Aiming to fill this gap in the discussions about Tor, this study will look at these questions from both a technical and legal perspective. By so doing, we aim to contribute to the exchange of information between the technical and legal members of the cyber security community who are dealing with controversial multidisciplinary issues related to anonymising technologies. In order to cater to the interests of policy-makers, governmental bodies and researchers in various domains, who are all looking for a comprehensive overview of these technical and legal issues, the nature of this study is introductory and therefore does not necessarily require previous technical or legal knowledge. Hopefully, this study will serve as a starting point for numerous future research projects that will tackle in greater detail some of the issues introduced here.

We start with a technical overview of privacy-preserving Internet technologies and censorship circumvention methods, such as proxies, Virtual Private Networks (VPN) and Domain Name System (DNS) based bypassing mechanisms. Then, the concept of onion routing is explained with a special focus on Tor. The underlying technical structure of Tor, and the access to the network, its relays, and exit nodes are elaborated on afterwards. We conclude the technical part by discussing the weaknesses of the Tor network, popular attacks, defence mechanisms and other indirect issues which affect the efficacy of this anonymity network.

---

[1] The Guardian, '"Tor Stinks" presentation – read the full document', http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document.
[2] Kevin Poulsen, 'FBI Admits It Controlled Tor Servers Behind Mass Malware Attack', http://www.wired.com/2013/09/freedom-hosting-fbi/.
[3] Joe Mullin, 'Silk Road 2.0, infiltrated from the start, sold $8M per month in drugs', http://arstechnica.com/tech-policy/2014/11/silk-road-2-0-infiltrated-from-the-start-sold-8m-per-month-in-drugs/.
[4] Tor Project, 'Overview', https://www.torproject.org/about/overview.html.en.
[5] See section 3.1.

Understanding the technical foundation of Tor is necessary for further elaborating on the legal issues. In the legal part, we explore government activities with respect to Tor, focusing on open source intelligence, personal data protection, and the collection of evidence. We go on to discuss the importance of Tor in the exercise and protection of human rights, and we briefly illustrate the content liability of exit node operators in the context of European law. We conclude by describing the legal limits on traffic monitoring.

2. Tor and Internet Filtering Circumvention

Tor is one of the most prominent and famous tools among other internet privacy and anonymity solutions. There are other similar applications, so called *privacy enhancing technologies*, which help internet users to stay anonymous in the cyber world.[6] Categorisation of such techniques can appear in different forms, but they are mainly listed under: proxies; tunnelling and Virtual Private Networks (VPN); Domain Name System (DNS) based bypassing; and onion routing.[7] Tor, which is maybe the most successful and common implementation, is a type of onion routing mechanism.[8]

2.1. Technical Methods

This section discusses different types of privacy enhancing technologies. The complexity, technical superiority and accessibility of these solutions vary, but their main goal is to help internet users to hide their own IP addresses, which can be used as an identifier of personal information.

2.1.1. Proxy

A proxy is a type of computer service which collects access requests from clients and forwards them to the destination on behalf of the requestors. After receiving replies, the proxy sends back the information to the requestor. It works like an intermediary service between sources and destinations. Although the idea was first presented almost 30 years ago as a means of structuring a powerful framework for distributed computing systems,[9] it is now commonly used for monitoring and filtering internet communications. There are also different types of proxies such as *reverse proxies* which focus on distributing server load, accelerating TLS/SSL, or optimising content by compressing it in order to speed up loading times.

Proxies can be used both for internet filtering and bypassing such internet filtering attempts. Schools, governmental agencies and most private companies use proxy solutions to limit users' access to specific websites or internet services. If users want to bypass those limitations, they can try to connect to a different proxy server outside the perimeters from which they connect to the internet.

---

[6] I. Goldberg, 'Privacy Enhancing Technologies for the Internet III: Ten Years Later', in *Alessandro Acquisti, Stefanos Gritzalis, Costas Lambrinoudakis & Sabrina De Capitani di Vimercati, ed., Digital Privacy: Theory, Technologies and Practices*, New York, London: Auerbach Publications (2007), pp. 3-18.

[7] Cormac Callanan, Hein Dries-Ziekenheiner, Alberto Escudero-Pascual, and Robert Guerra, 'Leaping Over the Firewall: A Review of Censorship Circumvention Tools', p. 22, Freedom House, April 2011, http://www.freedomhouse.org/sites/default/files/inline_images/Censorship.pdf.

[8] R. Dingledine, N. Mathewson, P. Syverson, 'Tor: The Second-Generation Onion Router', in *Proceedings of the 13th Usenix Security Symposium*, (2004).

[9] Marc Shapiro, 'Structure and Encapsulation' in *Distributed Systems: the Proxy Principle*. icdcs, Dec 1985, Cambridge, MA, United States. pp. 198-204.

If this channel to the proxy cannot be detected and blocked within the perimeter, they would be able to circumvent the limitations and bypass the restrictions.

There are different types of proxy solutions available in the context of circumvention techniques, such as web proxies, Hyper Text Transfer Protocol (HTTP) proxies and Socket Secure (SOCKS)[10] proxies.

In order to benefit from web proxies, it would be enough to know the Unified Resource Locator (URL) of the proxy web site's address. Visiting that website will allow the user to use the service.[11] HTTP proxies require the user or a piece of software to modify the browser settings. This type of proxy is very common in corporate environments and it only works for web content. SOCKS proxies are similar to HTTP proxies, but they also allow other internet applications like e-mail, IM tools and DNS to be tunnelled over them.

2.1.2. Tunnelling/Virtual Private Networks

A Virtual Private Network (VPN), which is the most common solution for network tunnelling, is a way to channel all or in some cases part of the network traffic via a different middle node. Technically, it is a private network and provides inter-connectivity to exchange information between various entities that belong to the VPN.[12]

In most cases, VPNs are used to access internal networks such as a company's intranet resources. Since VPN traffic is encrypted and can be used like a proxy, it is another way to bypass internet censorship. Using VPN to connect to a computer which does not reside within a restricted environment, and then accessing desired resources on internet circumvents the censorship.

A VPN has some advantages over the proxy solutions. It uses Internet Protocol Security (IPSec) or SSL, which provides secure communication. Confidentiality, integrity and authentication tenants of security are available in a VPN so that, even if the network traffic is sniffed, attackers would only see encrypted data and not the plain text. Integrity of communication is also provided, so that any sort of tampering would be detected and discarded from the network.

Although the content of the network channel cannot be observed under normal circumstances, using a VPN to circumvent internet censorship has a downside. If the IP address of the VPN server can be detected, and simply blocking that IP address is enough to prevent the circumvention. It is also easy to profile people if they run a VPN connection back to their offices from public internet spots. Although VPNs are mostly used as a mechanism for accessing corporate environments, they are also widely used for bypassing censorship.

2.1.3. Domain Name System based bypassing

Before discussing Domain Name System (DNS) based bypassing, we will briefly describe the fundamentals of DNS as that will make it easier to grasp the filtering mechanism. Basically, DNS is a translation mechanism which converts domain names to IP addresses. Since memorising names is much easier than memorising IP addresses, which are long strings of numbers, accessing internet resources is easier using DNS. In order to visit a web site, all we need to know is the address of that

[10] Socket Secure (SOCKS) is an internet protocol that routes network packets between a client and server through a proxy server.
[11] An sample list of web proxies can be found at http://proxy.org/cgi_proxies.shtml.
[12] R. Venkateswaran, 'Virtual Private Networks,' IEEE Potentials, Mar. 2001.

web site, not its IP address. DNS does the rest of the operation, resolving the IP address for that domain name and forwarding the request to the server.

When it comes to filtering, DNS is another option for enforcing censorship. Since the initial step is to learn the IP address of the target service, a DNS server can be configured to block access to that service. If a specific domain name is black-listed, DNS would simply block access to that web site by not answering the DNS request. It is also possible to configure DNS to return a different IP address for a specific query, which would result ending up on a totally different web site.

Bypassing DNS filters is not complicated. If the resource itself or the target website is not blocked, merely changing the DNS server to a different and untampered one would be enough. Alternatively, if the IP address of the web server is known, it may also be possible to access it directly via its IP address. However, many web sites operate on virtual hosting servers with shared IP addresses where direct IP access rarely works.[13] As an example of such censorship attempts, during March 2014, this type of DNS filtering was enforced for the Twitter website by the Turkish government, claiming that Twitter had failed to comply with court orders in Turkey.[14] According to news agencies[15] and cyber security researchers,[16] many citizens simply reconfigured their DNS settings and used Google's Open DNS service, thus bypassing the censorship.

2.1.4. Onion Routing

Onion routing is a networking mechanism which not only ensures that the contents are encrypted during network transmission to the exit node, but also hides who is communicating with whom during the process. It is a general purpose infrastructure for private communications over a public network.[17] It provides anonymous connections that are strongly resistant to both eavesdropping and traffic analysis between the relays of the network, although exit nodes can monitor the traffic since they transmit the network packets to their destinations.

Onion routing is quite different from the other methods mentioned above. In basic terms, the connection from source A to destination B takes a detour along an encrypted chain, which is called an *onion*. The network communication within the onion is also encrypted and each node, known as a *relay*, only has the information about the adjacent nodes (the immediate sender and the next recipient), so that the complete picture of the communication chain is hidden, at least theoretically.[18]

Censorship circumvention efforts mostly focus on what is observable by authorities in a network channel, with the aim of bypassing them. Encrypted channels, which are created between each relay

[13] Cormac Callanan, Hein Dries-Ziekenheiner, Alberto Escudero-Pascual, and Robert Guerra, 'Leaping Over the Firewall: A Review of Censorship Circumvention Tools', p. 22, Freedom House, April 2011, http://www.freedomhouse.org/sites/default/files/inline_images/Censorship.pdf.

[14] 'Turkey blocks use of Twitter after prime minister attacks social media site', *The Guardian* http://www.theguardian.com/world/2014/mar/21/turkey-blocks-twitter-prime-minister.

[15] 'Turkish citizens fight back against Twitter ban', http://www.cnet.com/news/turkish-citizens-fight-back-against-twitter-ban/

[16] 'Turkey bans Twitter, citizens tweet more', https://nakedsecurity.sophos.com/2014/03/24/turkey-bans-twitter-citizens-tweet-more/

[17] M. Reed, P. Syverson, and D. Goldschlag, 'Anonymous Connections and Onion Routing', IEEE Journal on Selected Areas in Communications, vol. 16 no. 4, May 1998, pp. 482, 494.

[18] There are various types of attacks against this architecture. Traffic correlation is one of them, which tries to identify network flow and the details about each relay. For more information, please take a look at Tor Project Blog. https://blog.torproject.org/category/tags/attacks

in onion routing, are therefore very effective. When the number of nodes increases, so does the complexity and number of encrypted channels. Compared to other circumvention methods like proxy or VPN, this is one of the reasons behind the popularity of onion routing solutions. Tor is the prominent example of onion routing network implementation[19], but it is not the only one. I2P[20] is a strong competitor for Tor, though not as popular. Freenet[21] is another example. Using Tor together with proxies and VPNs makes it even more resistant.

2.2. Technical background of Tor

Tor is defined as a third-generation onion routing system[22] which addresses limitations in the original design by adding forward secrecy, congestion control, directory servers, integrity checking, configurable exit policies, and a practical design for location-hidden services via rendezvous points.[23] It is one of the pioneers in anonymous network communications solutions today, and is also a way to bypass circumvention.

Tor allows people to access information safely and anonymously.[24] The architecture relies on the computers of volunteers and sponsors, since they share internet connections used by others. When users join the Tor network, they can contribute to the community by becoming *relay* or a *bridge* in the system. These terms will be described in the following section.

2.2.1. How does it work?

Tor is a low-latency communication service, meaning that the delays in the network sessions are minor for most users. The system provides a reasonable trade-off between anonymity, usability and efficiency.[25] The latency is due to the mode of operation. Regular internet connections follow the shortest, fastest and most efficient route when transferring network packages, depending on the algorithm.[26] Internet users do not have to worry about this, since Internet Service Providers (ISPs) deal with delivering the internet packets in the most effective way.

A Tor network follows a different approach. It creates a private network pathway, a *circuit*. Starting with the end user, the network packets follow different hops, called *relays*, until the final hop of the circuit, the *exit relay*. Exit relays will then transmit the request to the destination (e.g. the web site which the user wants to browse). All connections between the first relay and the exit relay are encrypted, and each relay along the way knows only the previous and the next hop. No one knows the complete pathway in this architecture, except attacks which reveal some of them.[27]

The following figures visualise this process for clarity.

---

[19] *Ibid*.
[20] I2P, The Invisible Internet Project. https://geti2p.net/en/
[21] Freenet, The Free Network. https://freenetproject.org/index.html
[22] In the early stages of Tor, the implementation was defined as a second-generation onion routing technique, but now it is accepted as the third-generation.
[23] *Ibid*.
[24] 'Building Bridges', https://media.torproject.org/video/2012-03-04-BuildingBridges-HD-english.ogv.
[25] *Ibid*.
[26] B. Halabi, *Internet Routing Architectures*, 135, Cisco Press: Indianapolis, IN, 1997.
[27] There are various types of attacks which are targeting to expose the relays in a Tor circuit, and some of them are successful. As an example: 'Deanonymizing Tor', https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-evans-grothoff.pdf.
This topic is elaborated in the next sections.

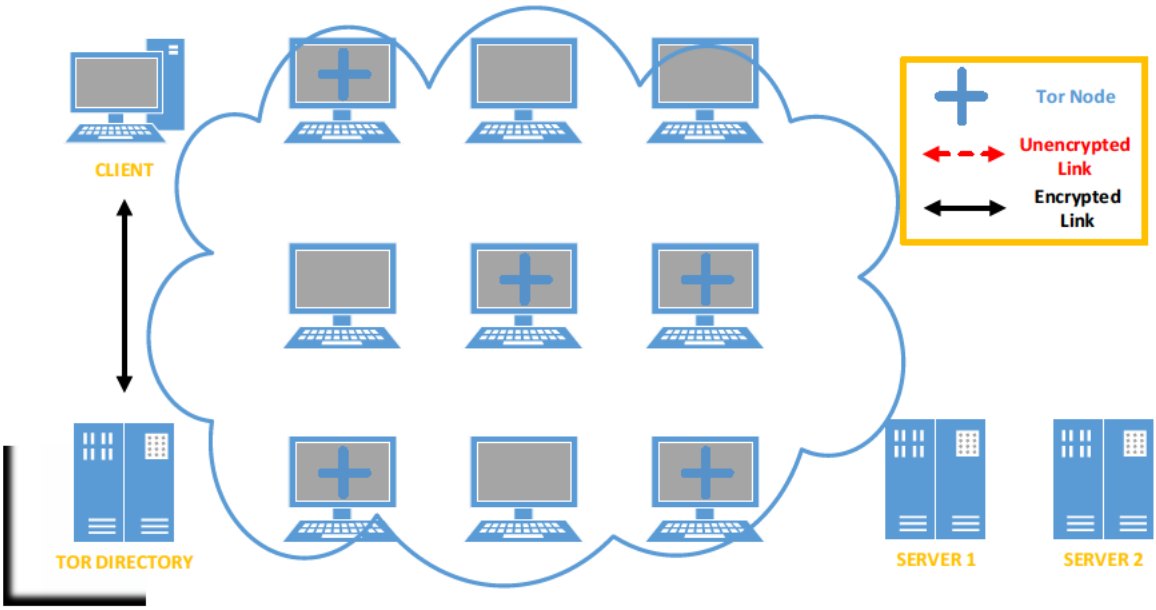

Figure 1 How Tor Works: Step 1

In the Figure 1, a simple Tor network layout is represented. The target servers are on the right hand side, the Tor nodes (relays) are in the middle, and the client and Tor Directory are on the left. [28] In the first step, a client who wants to join the Tor network sends an encrypted request to the Tor Directory to get a list of available Tor nodes. Once he receives the list, the client is ready to initiate connections with those relays in the internet cloud.

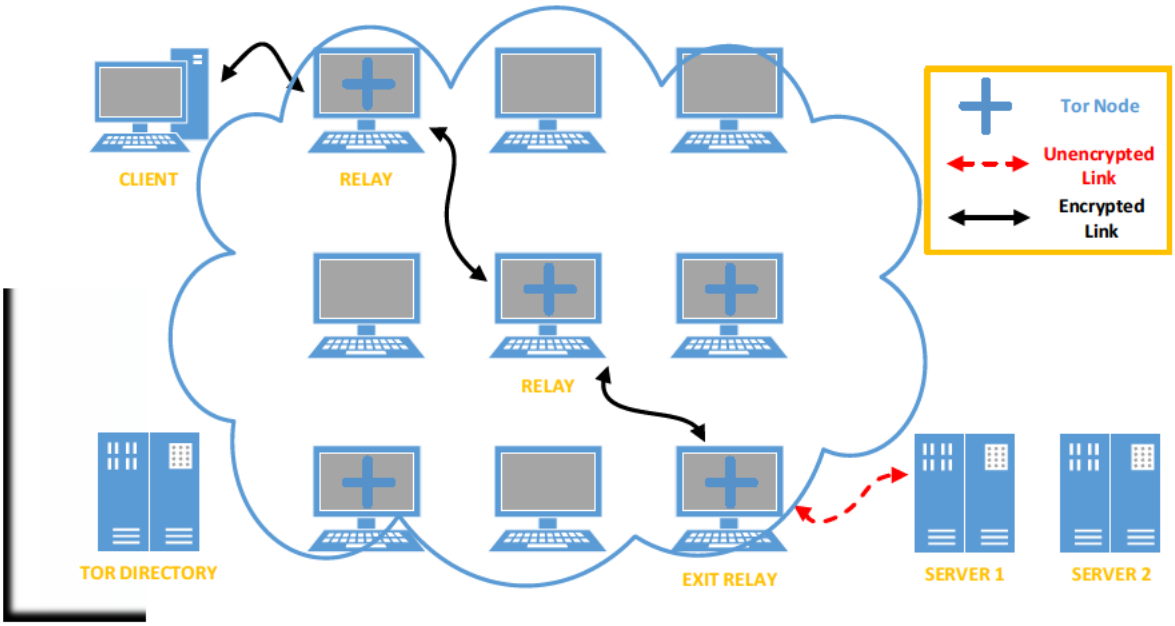

Figure 2 How Tor Works: Step 2

[28] More detailed descriptions can be found at https://www.torproject.org/about/overview.

In the second step (Figure 2) the client picks a random path to the destination, Server 1 in this example. Note that all network connections between the client and the last relay (exit node) are encrypted, except the one between the Exit Relay and Server 1. This happens when the client wants to connect to unencrypted services such as HTTP web sites. If the client sends a request to a HTTPS website, like *https://ccdcoe.org/*, then the entire chain would be encrypted. However, encrypted connections can also leak sensitive information, depending on the implementation of the web service. This topic will be elaborated on later.

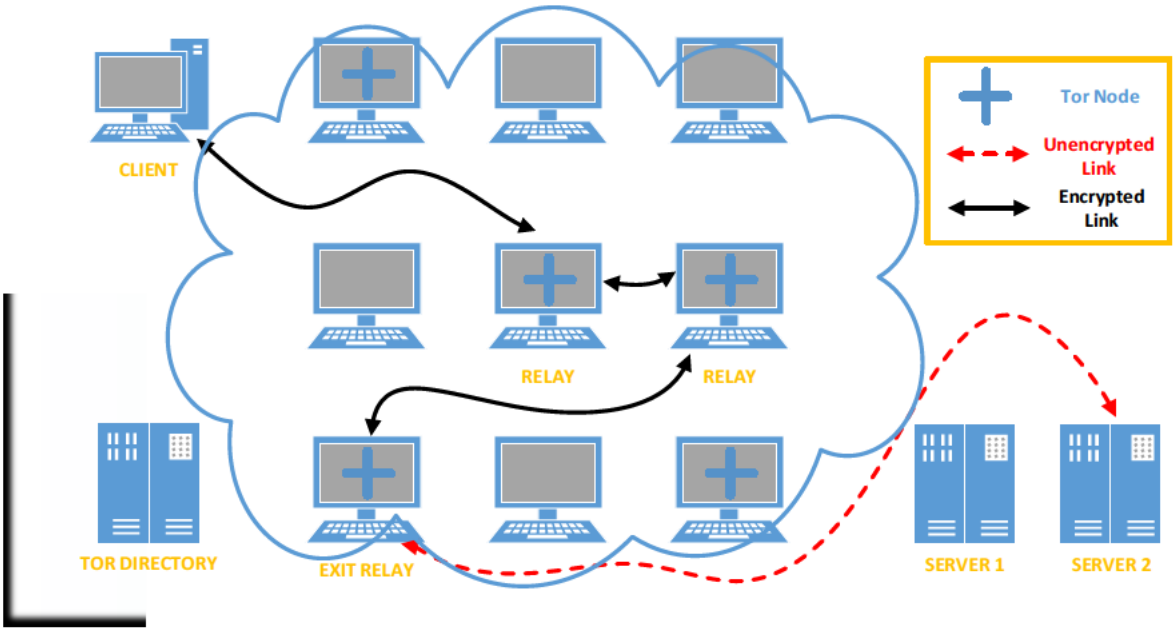

Figure 3 How Tor Works: Step 3

In another example (Figure 3), the client wants to establish a new connection to a different server, Server 2. In this case, Tor provides a different route to the destination in order to prevent potential correlation attacks.[29] Different attack vectors are discussed in detail below.

There are other ways to benefit from Tor as well, such as Hidden Services. In Hidden Services, the traffic does not go out from Tor relays, but stays inside. A detailed explanation is given in section 2.2.4.

2.2.2. Joining the Network

There are different types of active involvement options in Tor such as downloading the Tor browser application and running it as a client,[30] running a relay[31] or using a bridge.[32] Most users prefer the first option, and connect to the Tor network for their own use. According to the statistics today, there are around 2 million direct connections each day.[33] The top 5 countries of use and their

[29] Y. Zhu, X. Fu, B. Graham, R. Bettati and W. Zhao, 'Correlation-Based Traffic Analysis Attacks on Anonymity Networks', *IEEE Trans. Parallel Distrib. Syst.*, 21(7), pp.954-967, 2010.
[30] 'Tor Browser for Windows', https://www.torproject.org/download/download-easy.html.
[31] 'Configuring a Tor relay', https://www.torproject.org/docs/tor-doc-relay.html
[32] 'Tor: Bridges', https://www.torproject.org/docs/bridges.html.
[33] 'Tor Metrics', https://metrics.torproject.org/userstats-relay-country.html.

percentages are: United States (15.64 %), Germany (8.90 %), France (6.27 %), Russia (6.14 %) and Brazil (4.68 %).[34]

The second option is running a relay. Tor is not only technical but also a social network of volunteers who share network bandwidth with others. Running a regular relay, not an exit node, is a straightforward process. Debian/Ubuntu distributions of Linux have the necessary packages in Tor repositories.[35] A Vidalia Relay Bundle does the same thing in Windows environments.[36]

Third option is running a bridge. Tor clients need to get a list of active relays in the network to start creating the circuit. Once established, the network flow will start from the first relay. But what if that relay, or even all relays in the circuit, are inaccessible to the user? This would simply make it impossible to join the network. This is a common technique for ISPs in Tor blocking countries.[37,38]

Bridge relays, known as *bridges* in short, come into play at this stage. Bridges are unlisted, hidden relays which users can leverage as a first step to accessing Tor. Even if an ISP is blocking all the relays, users can still connect to Tor with the help of bridges. There are different ways of learning a bridge's IP address, such as sending an email to *bridges@bridges.torproject.org* with the line 'get bridges' in the email body. An automatic reply will send 3 IP addresses to the sender, instantly.[39]

2.2.3. Exit Relays

Running an exit relay is a bit different and a controversial topic. There are various reasons behind this, but from the technical and legal point of view, one of them stands out: exit relays are the interface of the Tor network with the internet. Whatever the Tor users do, wherever they connect, be it legal or illegal, exit relays carry those messages to the final destination.

For the Tor software itself, running a Tor exit relay requires some configuration changes in the Tor software bundle, such as Vidalia. The main issues do not arise from the Tor application itself, rather from the surrounding environment. In a proper configuration, adjusting server settings for rate limiting and reduced exit policies, managing ISP relations, getting a separate IP for the node and setting a recognisable DNS name are just a few of the issues.[40]

Finding an appropriate place for hosting and informing ISPs about potential issues which might arise in the future is among the first advice from the Tor community.[41] Since Tor is not being used only for innocent reasons,[42] the activities of spammers, Torrent file uploaders and abusers all look like they come from Tor exit relays.[43] If the Tor exit relay operators runs the services via a hosting company, which is a better option than running it at home, those hosting companies and the ISPs would receive

[34] 'Tor Metrics: Top-10 countries by directly connecting users', https://metrics.torproject.org/userstats-relay-table.html.
[35] 'Configuring a Tor relay on Debian/Ubuntu', https://www.torproject.org/docs/tor-relay-debian.html.
[36] 'Configuring a Tor relay', https://www.torproject.org/docs/tor-doc-relay.html.
[37] 'Tor partially blocked in China', https://blog.torproject.org/blog/tor-partially-blocked-china.
[38] Phillip Winter and Stefan Lindskog. 'How the Great Firewall of China is Blocking Tor', *FOCI. USENIX Association* (2012).
[39] 'Finding more Bridges in Tor', https://www.torproject.org/docs/bridges.html#FindingMore.
[40] 'Tips for Running an Exit Node with Minimal Harassment', https://blog.torproject.org/blog/tips-running-exit-node-minimal-harassment.
[41] 'Tor Exit Guidelines', https://trac.torproject.org/projects/tor/wiki//doc/TorExitGuidelines.
[42] 'Tor users', https://www.torproject.org/about/torusers.html.
[43] B. Li, E. Erdin, M. Gunes, G. Bebis, & T. Shipley, 'An overview of anonymity technology usage', *Computer Communications 36 (12)* (2013), pp.1269-1283.

many abuse complaints from other users.[44] Although there are some workarounds to decrease the numbers of complaints, it is more likely to happen eventually. The Tor community provides a list of ISPs from different countries, and rates their response if someone runs a bridge, relay or exit node in their infrastructure.[45] Reading previous experiences collected on Wiki pages is one of the first things for those considering running an exit node on their own.[46]

2.2.4. Hidden Services

One of the main goals of the Tor architecture is to protect the identity of users. But what if someone wants to protect a destination on the internet as well, such as a web service? Tor also provides a solution for that, which is called *Hidden Service*.[47]

The technical explanation of hidden services is complex, but the logic behind relies on distributing *rendezvous points* on the Tor network. Instead of using a destination server address and directly connecting to the server, clients use an identifier to find the server. That identifier is a 16 character name derived from the service's public key (such as *xyz.onion*).[48] Once found, client and server meet at a rendezvous point, without knowing each other's real location. This provides privacy for both parties, client and server.[49] The main goals behind hidden services are access-control protection, robustness of servers and hiding the true identities of hidden service administrators.[50]

From the security perspective, there is one more detail about Tor hidden services. While accessing regular web services, Tor traffic leaves the Tor network at exit nodes. With hidden services, Tor traffic stays inside and does not leave. This might prevent security issues like traffic monitoring using exit nodes.

2.3. Analysis of the technology

Anonymity technologies on the internet are a controversial topic from technical point of view, because of the common failures or design problems of such solutions. As new problems emerge, there are new challenges for technical experts and academics who are working in this domain. This section presents discussions about the strengths, weaknesses, and direct and indirect issues which affect the Tor network.

---

[44] 'Tor Exit Guidelines', https://trac.torproject.org/projects/tor/wiki//doc/TorExitGuidelines.
[45] 'Good-Bad ISPs', https://trac.torproject.org/projects/tor/wiki/doc/GoodBadISPs.
[46] As an example of consequences for running a Tor exit node which happened before: 'An Open Letter: Is copyright trolling a thing in Finland now?', http://semantics.sebastianmaki.fi/2014/08/an-open-letter-is-copyright-trolling.html.
[47] 'Tor: Hidden Service Protocol', https://www.torproject.org/docs/hidden-services.html.
[48] An infamous example of such services is SilkRoad. The address of Silkroad was https://silkroadvb5piz3r.onion before its seizure by FBI. The site shows a banner about this operation now. Further discussion on this subject is carried out in this research.
[49] There is a service called tor2web, located in https://tor2web.org/ which provides easy access to Hidden Services without using Tor directly. Although it does not provide full functionality of Tor, it can be useful to check out hidden services quickly. For example, you can check out https://silkroadvb5piz3r.tor2web.org address to see FBI's banner on the server.
[50] *Ibid.*

2.3.1. Academic and Technical Research

As the motto goes, 'the Tor community of software and services aims to make the internet experience safer and better'.[51] In order to achieve that, many people around the world support Tor, ideologically or actively participate in the projects. There are other motivations as well, such as attacking Tor to learn more about the users and their real identities. No matter which approach someone follows, there is one common discussion: what are the weaknesses of the system and how do we exploit them?

There are many researchers studying Tor design and its potential vulnerabilities around the world. Many of them focus on what is going on in the network, how to collect and analyse Tor data, how improve its design, and so forth.[52]

The main source for Tor related research would be the 'Tor Research Home' webpage run by the Tor community.[53] Since there is a lot of overlap in research topics, such as collecting Tor related data, measuring current Tor statistics or running analysis based on these findings, sharing what others have achieved so far or meeting with other researchers in the community makes a lot sense. For these reasons, Tor Research Home also has a list of 'Tech Reports' giving background information.

Tor is not a very old solution, and the first paper on the idea was published only 10 years ago.[54] However the discussions related to anonymity and privacy-preserving network communications go back to the 1980s.[55] Thus, there is a lot of background information to cover, especially for academia. As an example, there is a very structured list of anonymity related academic publications at Freehaven.net.[56]

Along with the academic research and technical analysis in the field of anonymity studies and Tor, there are more practical efforts within the Tor ecosystem as well. Bundle software development, browser add-ons, simulators, libraries, client services, backend services and utilities are some them.[57] A more detailed list of projects can be found on the community web page.[58] The idea behind all these applications is to support the Tor community in every possible way, be it end-user, developer or researcher. If there is an issue with Tor, there is probably a solution, a workaround or at least a discussion on that very topic within the Tor community.

2.3.2. Anonymity and Tor

Providing comprehensive and error-free anonymity to Tor users is in the centre of academic research and technical discussion. From the technical point of view, the design of Tor architecture might look like it can achieve this goal, however, there are many issues which makes the system susceptible to failure. Some are related to user mistakes, some are onion routing issues, and some are indirect issues which affect the success rate of the system. (Due to the nature of the mechanism, Tor related attacks refer to success rates which could be achieved. Not every user can be de-anonymised every

[51] 'Software & Services', https://www.torproject.org/projects/projects.html.
[52] 'Research groups', https://research.torproject.org/groups.html.
[53] 'Tor Research Home', https://research.torproject.org.
[54] *Ibid*.
[55] D. Chaum, (1981), 'Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms', *Commun*. ACM 24 (2), 84-88.
[56] 'Selected Papers in Anonymity', http://freehaven.net/anonbib.
[57] 'Tor Ecosystem', https://www.torproject.org/getinvolved/volunteer.html.
[58] 'Software & Services', https://www.torproject.org/projects/projects.

time, but some users might be de-anonymised at some point of time.)Types of attacks are covered in the next part in detail.

Leaving aside all non-Tor-related issues, the main subject of the anonymity research comes from the results of monitoring the data which is transmitted on Tor. Then, the degree of anonymity could be measured via different models such as probability, similarity, entropy and evidence theory based on the analysed data.[59] Since all network flow is encrypted between Tor relays with the help of these models, it might be possible to correlate the traffic and disclose the real IP addresses of the users.[60]

Collecting data for traffic analysis, which is mostly encrypted, is the crucial step and of the utmost importance. There are previous studies which have focused on analysing the network,[61] collecting URL of HTTP traffic[62] and so forth. A Tor exit relay creates another possibility here, because anyone can operate an exit relay and the relay transmits the internet packages in an unencrypted format to the destination if the client used HTTP instead of HTTPS (see section 2.2.3). There were some researchers who focused on this possibility,[63,64] and some also used DPI[65] to take a closer look on the data transmitting over the exit relay.[66,67]

2.3.3. Attacking Tor

There is a huge amount of effort behind Tor, however, the results of the studies indicate that there are some possible ways to uncover the real identities of some Tor users. Some of these techniques are easy to leverage, especially the ones arising from user mistakes. Others need advanced technical capabilities and lots of time. Some of these attacks might reveal IP addresses, while others might show what Tor users are doing at some point of time, and require deductions and estimations to find the person. These threats are categorised under three sections: user mistakes, Tor issues, and indirect problems.

[59] *Ibid*.
[60] Aaron Johnson, *et al*. 'Users get routed: Traffic correlation on tor by realistic adversaries', in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013.
[61] M. Mulazzani, M. Huber, E. Weippl, 'Anonymity and monitoring: How to monitor the infrastructure of an anonymity system', *IEEE Transactions on Systems, Man, and Cybernetics. Part C: Applications and Reviews* 40 (5) (September 2010) pp. 539-546.
[62] B. Li, E. Erdin, M. Gunes, G. Bebis, & T. Shipley, 'An analysis of anonymity technology usage', in *Proceedings of the Third International Conference on Traffic Monitoring and Analysis,* TMA'11, Springer-Verlag: Berlin, Heidelberg, 2011, pp. 108-121.
[63] P. Manils, C. Abdelberi, S. Le-Blond, M.A. Kafar, C. Castelluccia, A. Legout, W.Dabbous, 'Compromising tor anonymity exploiting P2P information leakage', CoRR, abs/1004.1461, 2010.
[64] D. McCoy, K. Bauer, D. Grunwald, T. Kohno, D. Sicker, 'Shining light in dark places: understanding the tor network', in *Proceedings of the Eighth International Symposium on Privacy Enhancing Technologies,* PETS '08, Springer-Verlag, Berlin, Heidelberg, 2008, pp. 63-76.
[65] DPI is complete packet inspection technique which analyses data and header parts of a packet.
[66] A. Chaabane, P. Manils, M. Kaafar, 'Digging into anonymous traffic: a deep analysis of the Tor anonymizing network', in *2010 Fourth International Conference on Network and System Security (NSS)*, September 2010, pp. 167-174.
[67] *Ibid*.

User Mistakes

Tor provides a different browsing experience. In order to get the most out of it and make the system work properly, there are couple of issues which need special attention.[68] The first important issue is the Tor browser, although there are other solutions to use Tor with a complete Operating System[69] as well.

It is very common to view a document, open a Flash Object or use an add-on in a regular internet browsers. In the Tor browser, such attempts can disrupt the mechanism of the system and might reveal the real IP address of a user. The reason behind this is simple. Tor is meant to communicate only with other relays before the exit node. However some objects or embedded executables in documents can force to break this chain and lead to a leakage. These baits might also be a part of attacking campaign against some users to learn their true IP addresses.[70]

Using Torrent over Tor is not advised, because the logic is similar to the threats mentioned above. Torrent file sharing applications might ignore the proxy settings of the Tor browser, and can create direct connections to other users.

As an example for Tor related attacks against anonymity, it is being claimed that anonymous payment can be made with crypto currencies like Bitcoin.[71] Using Bitcoin over Tor was believed to improve this even more.[72] However in October 2014, researchers at the University of Luxemburg showed that combining them enables man-in-the-middle (MitM) attacks to gain full control of information flows between users using Bitcoin over Tor.[73]

One last example is using HTTP web sites instead of HTTPS. Tor exit nodes can view the internet packages flowing through them. If Tor clients use HTTP, this would simply make the system prone to wiretapping.[74]

Human nature is always susceptible to errors in the world of cyber. If a user can be tricked into taking an extraordinary action while using Tor, his or her true identity might be revealed.

Tor issues

The Tor community works on new features, additional security mechanisms, tools and applications to make the system better. Nevertheless, according to some studies there are issues with the Tor environment by design, which might leak critical information regarding users' privacy.[75]

Redirecting users to special servers[76] via telecoms operators can constitute a man-in-the-middle attack, as an example. It can be done by intercepting the traffic between a Tor user and the

[68] 'Want Tor to really work?', https://www.torproject.org/download/download.
[69] 'Tails, Privacy for anyone anywhere', https://tails.boum.org.
[70] Active Defense Harbinger Distribution, which is a Linux distribution has compiled a list of applications which can be used for such attacks. http://sourceforge.net/projects/adhd.
[71] 'Bitcoin, Anonymity', https://en.bitcoin.it/wiki/Anonymity
[72] 'Bitcoin, Tor', https://en.bitcoin.it/wiki/Tor
[73] Alex Biryukov, and Ivan Pusto, 'Bitcoin over Tor isn't a good idea', arXiv preprint arXiv:1410.6079, 2014.
[74] 'Security expert used Tor to collect government e-mail passwords', http://arstechnica.com/security/2007/09/security-expert-used-tor-to-collect-government-e-mail-passwords.
[75] Famous presentation 'Tor Stinks' which was leaked last year also discusses exploitation techniques such as QUANTUM attacks. http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document.
[76] NSA's FoxAcid servers could be an example, according to the Snowden leaks.

legitimate server, although it has been argued that only the US National Security Agency (NSA) has this sort of capability.[77]

In academic research, it has been shown that if someone takes control of one or more of the autonomous systems (ASes) and Internet Exchange Points (IXPs), he or she can de-anonymise any given user within three months of regular Tor use with over 50% probability, and within six months with over 80% probability.[78] This is an example of correlation attacks for the encrypted data in the Tor environment.

There is another famous exploitation technique for large scale peer-to-peer networks, called the Sybil attack, which was presented in 2002.[79] According to the study, it is possible to subvert reputation systems of peer-to-peer networks like the Tor environment by forging identities. However, there are also prevention techniques to protect anonymisation networks from Sybil.[80,81]

Accessing Tor bridges is an important first step to circumvent censorship if Tor is being blocked in an environment. In such cases, if the connection between the client and the Tor bridge cannot be detected and blocked, the connection to Tor would be established successfully. Because of this importance, Tor has some additional tools to hide this connection which are known as *Pluggable Transports*.[82] Pluggable transports transform the Tor traffic flow between the client and the bridge. This way, traffic between the client and the bridge will see only innocent-looking transformed traffic, like a Skype conversation, instead of the actual Tor network flow. SkypeMorph,[83] Stegotorus[84] and CensorSpoofer[85] are some of the examples in this approach. Nevertheless, recent studies have shown that such solutions fail to provide privacy all the time because of the success rate of passive and active attacks against the mechanisms of the tools.[86]

Indirect problems

Encrypted connections between randomly chosen relays, updating these relay circuits in every 10-15 minutes, and providing hidden bridges to reach Tor networks are only some of the features Tor

[77] 'Attacking Tor: how the NSA targets users' online anonymity', http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity.
[78] Aaron Johnson, *et al*. "Users get routed: Traffic correlation on tor by realistic adversaries." *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013.
[79] J.R. Douceur, 'The sybil attack', *Peer-to-peer Systems*. Springer: Berlin, Heidelberg, 2002, pp. 251-260.
[80] S.D. Chandhana, 'Defending Against Sybil Attacks in Anonymizing Networks', 2012.
[81] A.P. Chamarti, Rajasekhar, 'Securing Anonymizing Networks from Sybil Attacks', *Arunasri Chamarti et al., Int.J.Computer Technology & Applications, Vol 3 (6)*, 2012, pp. 2046-2052.
[82] 'Tor: Pluggable transports', https://www.torproject.org/docs/pluggable-transports.html.
[83] H. Moghaddam, B. Li, M. Derakhshani, and I. Goldberg. 'SkypeMorph: Protocol Obfuscation for Tor Bridges' in *CCS '12 Proceedings of the 2012 ACM conference on Computer and communications security*, ACM New York, NY, USA ©2012, pp. 97-108.
[84] Z. Weinberg, J. Wang, V. Yegneswaran, L. Briesemeister, S. Cheung, F. Wang, and D. Boneh, 'StegoTorus: A Camouflage Proxy for the Tor Anonymity System' in *CCS '12 Proceedings of the 2012 ACM conference on Computer and communications security*, ACM New York, NY, USA ©2012, pp. 109-120.
[85] Q. Wang, X. Gong, G. Nguyen, A. Houmansadr, and N. Borisov, 'CensorSpoofer: Asymmetric Communication Using IP Spoofing for Censorship-Resistant Web Browsing', in *CCS '12 Proceedings of the 2012 ACM conference on Computer and communications security*, ACM New York, NY, USA ©2012, pp.121-132.
[86] Houmansadr, A.; Brubaker, C. & Shmatikov, V., 'The Parrot Is Dead: Observing Unobservable Network Communications', in *IEEE Symposium on Security and Privacy*, IEEE Computer Society, 2013, pp. 65-79.

provides to its users. There are also some indirect problems which affect the privacy of users in Tor, such as browser vulnerabilities.[87]

The Tor browser bundle might be a gate for privacy enabled internet communication, but it is still a browser. As many applications have exploitable vulnerabilities, so does the Tor browser. Essentially, the Tor browser is based on Firefox with some specific configurations, and it has been discovered that some versions have a critical vulnerability.[88] As a result, Tor users are at risk from the exploitation of that vulnerability.[89] This is not directly a Tor architectural issue, but leveraging this attack might allow arbitrary code execution on the victim's computer. Not only the privacy features, but the computer itself can be compromised with these sorts of attacks.

Another recent development in information security world was the infamous Heartbleed bug, which was a serious vulnerability in the popular OpenSSL cryptographic software library.[90] Exploiting this vulnerability led to the exfiltration of secret keys used for X.509 certificates, usernames, passwords and many other critical pieces of data from services which use OpenSSL. Many HTTPS sites also suffered from the vulnerability, just like Tor. Some of the Tor relays, Tor applications like Orbot and Tor clients were open to this vulnerability as they were using vulnerable version of OpenSSL.[91] It was not possible to solve the situation by just patching the client applications which had vulnerable OpenSSL. There were other problems as well: the bug also affected the Tor relay capacity by up to 12% because the relays, which are the backbones of the architecture, were also vulnerable.[92] The havoc which Heartbleed caused affected Tor and its users, providing a solid example how indirect problems can lead to serious privacy issues for Tor users.

We shall now move on to discuss a number of legal issues connected to the use and abuse of Tor.

3. Selected legal challenges regarding Tor

From the legal perspective, Tor is a very interesting phenomenon. Be it Tor or some other network, anonymity will be part of cyberspace as long as the Internet remains 'global and open'.[93] However, anonymity can be a mixed blessing, and Tor also raises many legal questions. Due to the limited extent of this paper, we will tackle only some of these challenges, namely the activities of governments with respect to Tor, human rights aspects of the use of Tor, content liability of Tor exit node operators, and exit node monitoring.

---

[87] 'NSA tried and failed to compromise Tor, but browser vulnerabilities gave some users away', http://www.theverge.com/2013/10/4/4802512/nsa-failed-to-compromise-tor-network-but-exploited-browser-vulnerabilities.

[88] Execution of unmapped memory through onreadystatechange event, https://www.mozilla.org/en-US/security/advisories/mfsa2013-53.

[89] 'Tor security advisory: Old Tor Browser Bundles vulnerable', https://blog.torproject.org/blog/tor-security-advisory-old-tor-browser-bundles-vulnerable.

[90] 'The Heartbleed Bug', http://heartbleed.com.

[91] 'Heartbleed and TOR in practice', http://www.digitalassurance.com/blog/heartbleed-and-tor-practice.

[92] 'Tor may be forced to cut back capacity after Heartbleed bug', http://www.theguardian.com/technology/2014/apr/17/tor-heartbleed-bug-vulnerable-servers.

[93] United Nations General Assembly, Resolution A/RES/68/167, 'The right to privacy in the digital age', 18 December 2013, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167.

3.1. Governments and Tor

The use of Tor has been subject to diverse reactions from governments. The relationship between Tor and governments is especially complex due to the fact that Tor is being used not only by private citizens seeking more privacy, but also by other entities, ranging from states to organised crime groups.

It is a well-known fact that the Tor Project non-profit organisation is being supported by several private and public entities as well as by governments.[94] In fact, Tor was originally designed, implemented, and deployed as a third-generation onion routing project of the Naval Research Laboratory.[95] It was originally developed with the U.S. Navy in mind with the principal goal of protecting government communications, and is even today used by a wide variety of state entities such as the military and law enforcement.[96] Even today there have been suggestions that government officials help to develop the network by informing Tor about possible bugs or other aspects in Tor which need to be fixed.[97]

Government support is also evident in terms of funding Tor. Active sponsors in 2013 included the U.S. Department of State and U.S. Department of Defense, with federal awards amounting to $1.8 million.[98] While in 2012 the part of the income that was US Government based amounted to 60%,[99] the Tor project has publicly called for additional contributions to diversify the source of sponsorship[100] and insisted on not having a back door to Tor.[101]

At the same time there are examples of countries that openly suppress Tor. For instance, China has outlawed the use of Tor and has blocked access to Tor entrance nodes, and Saudi Arabia and United Arab Emirates are both blocking Tor's website,[102] as is Iraq.[103]

Other countries go further than that. Although not officially confirmed, the NSA has been reported to have made repeated attempts to develop attacks against individuals using Tor.[104] In 2013, it was suggested that while leaked documents confirm that the NSA does indeed operate and collect traffic from some nodes in the Tor network, there is no further information as to how many nodes are

---

[94] 'Tor Sponsors', https://www.Torproject.org/about/sponsors.html.en.

[95] 'Tor Users', https://www.torproject.org/about/torusers.html.en#military; 'Onion Routing', http://www.onion-router.net/.

[96] 'Tor Users', https://www.torproject.org/about/torusers.html.en.

[97] James Cook, 'Tor Director Claims Some Government Agents Are Secretly Helping Him, Undermining Intelligence Operations', *Business Insider*, 22 August 2014, http://www.businessinsider.com/tor-director-says-intelligence-agents-tips-him-off-2014-8.

[98] Moody, Famiglietti & Andronico, *Tor Project Financial Statement 2013 and 2012* https://www.Torproject.org/about/findoc/2013-TorProject-FinancialStatements.pdf.

[99] *Tor Annual Report 2012*, https://www.Torproject.org/about/findoc/2012-TorProject-Annual-Report.pdf.

[100] Roger Dingledine and Jacob Appelbaum, 'C3TV - The Tor Network: We're Living in Interesting Times', 2013 http://media.ccc.de/browse/congress/2013/30C3_-_5423_-_en_-_saal_1_-_201312272030_-_the_tor_network_-_jacob_-_arma.html.

[101] 'Tor Project FAQ', https://www.torproject.org/docs/faq#Backdoor.

[102] Keith Watson, 'The Tor Network: A Global Inquiry into the Legal Status of Anonymity Networks', *Washington University Global Studies Law Review*, 11 (2012), 715–37.

[103] 'Iraq Crisis: Government Blocks Access to Tor Project Following Isis Insurgency', *International Business Times*, 2014.

[104] James Ball, Bruce Schneier and Glenn Greenwald, 'NSA and GCHQ Target Tor Network That Protects Anonymity of Web Users', *The Guardian*, 4 October 2013, section World news http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.

being controlled, and whether the proposed de-anonymisation technique was ever implemented.[105] Some sources claim that the 'NSA tracks users who are believed to live outside the US and who request Tor bridge information via e-mail or who search for or download Tor or the TAILS live operating system'.[106] Some leaked documents argue that it would be 'counterproductive' to 'scare' the critical mass of targets that are using Tor away from it.[107] Other commentators believe that US efforts to target or undermine Tor would raise legal concerns for national intelligence agencies, especially concerning whether 'the NSA has acted, deliberately or inadvertently, against internet users in the US when attacking Tor'.[108]

Other countries have also proposed measures to challenge the anonymity enabled by Tor. An example is Russia which, with the aim 'to ensure the country's defence and security', has openly offered an award of $110,000 to anyone able to crack the identities of users of the Tor network.[109]

In a recent development, EUROPOL announced in 2014 the takedown of 'more than 410 hidden services',[110] the numbers later being corrected to 27 websites.[111] There is little information how law enforcement managed to 'break Tor' and identify the users behind these hidden services, other than that the methods were not revealed because they were 'sensitive' and the servers located in a foreign country were accessed and 'imaged'.[112] The Tor project speculates that the number of takedowns and the seizure of Tor relays could mean that the Tor network was attacked with the purpose to reveal the location of those hidden services,[113] as has been attempted before when a group of Tor relays were 'actively trying to break the anonymity of users by making changes to the Tor protocol headers associated with their traffic over the network'.[114] While some of the servers that were taken down were clearly related to illegal activities such as selling drugs, they allegedly also included several that were acting as infrastructure for Tor's anonymising network.[115] The unanswered question of how these services were located will hopefully be answered in court when prosecuting the arrested suspects.[116] Needless to say, illegally obtained evidence may be found inadmissible in court.

In the context of international law, if a state is accessing servers located on foreign territory and taking them down, it requires either the consent of the other state or other grounds under international law such as convention or customary law. Additional legal issues may arise if the

[105] Ball, Schneier and Greenwald, *op cit*.
[106] Pierluigi Paganini, 'Hacking Tor and Online Anonymity' (InfoSec Institute) http://resources.infosecinstitute.com/hacking-tor-online-anonymity/.
[107] '"Tor Stinks" Presentation', *The Guardian*, 4 October 2013, http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document.
[108] Ball, Schneier and Greenwald, *op cit*.
[109] BBC News, 'Russia Offers $110,000 Tor Bounty', http://www.bbc.com/news/technology-28526021.
[110] EUROPOL, 'Press Release: Global Action Against Dark Markets on Tor Network', https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network.
[111] Tor Project, 'Thoughts and Concerns about Operation Onymous', https://blog.torproject.org/blog/thoughts-and-concerns-about-operation-onymous.
[112] Kashmir Hill, 'How Did The FBI Break Tor?', *Forbes*, http://www.forbes.com/sites/kashmirhill/2014/11/07/how-did-law-enforcement-break-tor/.
[113] 'Thoughts and Concerns about Operation Onymous'.
[114] Sean Gallagher, 'Law Enforcement Seized Tor Nodes and May Have Run Some of Its Own', *ArsTechnica*, http://arstechnica.com/security/2014/11/law-enforcement-seized-tor-nodes-and-may-have-run-some-of-its-own/.
[115] Gallagher, *op cit*.
[116] 'Thoughts and Concerns about Operation Onymous'.

targeted servers are those of innocent bystanders that are not connected with the investigation at all. Such activities may also be criminal under the law of the state on whose territory the servers were located.

3.1.1. Law enforcement using Tor in criminal investigations

Today, Tor is a common tool for national law enforcement.[117] The Tor project summarises three main activities for law enforcement's use:

> - *'Online surveillance: Tor allows officials to surf questionable web sites and services without leaving tell-tale tracks. If the system administrator of an illegal gambling site, for example, were to see multiple connections from government or law enforcement IP addresses in usage logs, investigations may be hampered.*
> - *Sting operations: Similarly, anonymity allows law officers to engage in online "undercover" operations. Regardless of how good an undercover officer's "street cred" may be, if the communications include IP ranges from police addresses, the cover is blown.*
> - *Truly anonymous tip lines: While online anonymous tip lines are popular, without anonymity software, they are far less useful. Sophisticated sources understand that although a name or email address is not attached to information, server logs can identify them very quickly. As a result, tip line web sites that do not encourage anonymity are limiting the sources of their tips.'*[118]

In addition, Tor is used as an environment for general investigation, intelligence collection and infiltration, such as can be seen in the recent takedown of Silk Road 2.0 that operated on the Tor network.[119]

National law enforcement and their use of Tor raises a number of interesting legal issues such as whether there are any limitations for law enforcement for using Tor for collecting evidence, and, if we consider information available via Tor or within Tor as publicly available data, whether there are any restrictions for law enforcement in processing them.

The legal boundaries for law enforcement's activities that are generally being set in national law can differ greatly from one country to another. This is especially true in the context of collecting digital evidence that raises challenges for domestic procedural law. Use of Tor for collecting evidence may touch upon many of these challenges. For example, in some legal systems, the fact that the agency which is using Tor for collecting evidence is anonymised, may raise concerns regarding 'deception' in criminal procedure,[120] or otherwise hinder the use of such evidence in court.

---

[117] According to one of the principle inventor of Tor, Roger Dingledine, Tor trainings and talk have been delivered to e.g. Dutch, German, Norwegian law enforcement as well as FBI and United States Department of Justice, many of them declaring the use of Tor; Roger Dingledine, 'Trip Report: Tor Trainings for the Dutch and Belgian Police', *Tor Project*, https://blog.torproject.org/blog/trip-report-tor-trainings-dutch-and-belgian-police.
[118] 'Tor Users', https://www.torproject.org/about/torusers.html.en.
[119] 'Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court, FBI Press release', http://www.fbi.gov/newyork/press-releases/2014/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court.
[120] Bert-Jaap Koops, Colette Cuijpers and Maurice Schellekens, 'Analysis of the Legal and Ethical Framework in Open Source Intelligence' (EU FP7, 2011), p. 20.

Since Tor is to be viewed in the context of criminal procedure as any other source for Open Source Intelligence (OSINT),[121] it must also be verified whether there are concerns related to the possible processing of personal data. Even though Tor is used for the anonymisation of its users, and their IP addresses are veiled behind the known addresses of exit nodes, and therefore the users' personal data should not be available at all, this does not preclude the presence of personal data in the databases exhibited as part of Tor's hidden services such as names, addresses, phone numbers, credit card data, personal security numbers, such that are exhibited in a Tor hidden service called Doxbin.[122]

3.1.1.1. Tor and Open Source Intelligence

Although not raising specific legal concerns in relation to Tor, there are a few interesting arguments that have been raised. The most significant of them is related to the Council of Europe's Convention on Cybercrime.[123] Article 32(a) of the Convention regulates trans-border access to stored computer data where 'publicly available (open source) stored computer data, regardless of where the data is located geographically'[124]. Unless domestic law states otherwise,[125] law enforcement may access the same data that is generally accessible to the public and, if needed for this purpose, subscribe to or register for services available to the public.[126] According to some commentators, access to open source material for criminal investigation purposes has become generally accepted practice.[127] As Tor is a service freely available for the public, this provision should also apply to law enforcement's activities that involve employing Tor for collecting evidence.

However, there is a minority view arguing that the mere fact that certain information is publicly available does not imply an absence of restrictions to processing such data.[128] Such restrictions may derive from the means and volume of data collected. Bert-Jaap Koops asserts that the current

[121] Bert-Jaap Koops a, Jaap-Henk Hoepman b,c, Ronald Leenes, 'Open-source intelligence and privacy by design', Computer Law & Security Review 29 (2013), pp. 676-688.
[122] Gallagher, *op cit*.
[123] The Convention was adopted in 2001 and has been signed by 53 and ratified by 44 states. Council of Europe, *Convention on Cybercrime*, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. 'Council of Europe Convention on Cybercrime, List of Signatories and Ratifications', http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.
[124] Council of Europe, *Convention on Cybercrime*, Art. 32 para (a).
[125] In many cases, however, open-source data gathering is not explicitly mentioned in national legislation. An example of this is the Criminal Procedure Code (CPC) is Estonia. CPC does not mention open source data and access to it, but includes an obligation that 'If technical equipment is used in collecting evidence, this must be communicated in advance to the parties involved in the procedure and they will be explained the purposes of using such technical means'. This provision may raise an additional set of questions. The latter condition is not being further explained in official explanatory material, but in a narrow sense appears to be highly challenging to follow in all instances of collecting of evidence, especially when it is being done using technology such as the Internet to access public source information. Estonia, *Code of Criminal Procedure*, *Passed 12.02.2003 RT I 2003, 27, 166 Entry into force 01.07.2004*, para. 64 (3) https://www.riigiteataja.ee/en/eli/527022014001/consolide.
[126] Cybercrime Convention Committee (T - CY) Ad - hoc Subgroup on Transborder Access and Jurisdiction Council of Europe, 'T-CY Guidance Note #3: Transborder Access to Data (Article 32), Draft for Discussion', 2013.
[127] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, February 2013, p. 133 http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf .
[128] Bert-Jaap Koops, 'Police Investigations in Internet Open Sources: Procedural-Law Issues', *Computer Law & Security Review*, 29 (2013), 654–65, http://dx.doi.org/10.1016/j.clsr.2013.09.004.

investigative powers that focus on physical space investigations may need to be revised in order to fit with the particularities of open-source investigations, especially those that offer extensive automated large-scale search capabilities such as entity recognition, image-to-text conversion and automated translation.[129] This is based on the assumption that automated open-source investigations may affect the right to privacy and thereby require a legally codified base to inform the citizens about such a possibility.[130] Should such automated means of data processing be used via Tor or be targeting, for example, Tor hidden services, legal regulation of such large scale search capabilities might need to be considered by the legislature.

3.1.1.2. Tor and personal data

As can be seen from evidence of recent take-downs of hidden services, Tor users may not be granted 100% anonymity, thereby resulting in the possible situation of law enforcement processing personal data not necessary for the original scope of the investigation. It is also possible that Tor is used to access personal data stored in, for example, some of Tor's hidden services. This is why the use of Tor by law enforcement for criminal investigations may entail processing personal data, and may thus be limited by data protection legislation.

Concerns about the possible processing of personal data during an investigation are certainly not specific to Tor. However, EU data protection reform will have a significant effect on the work of law enforcement, including possible investigative activities carried out via Tor when the data to be processed is personal data. This means that even if law enforcement uses Tor to anonymously access certain websites or services, the requirements and legal remedies deriving from the data protection regulation would nevertheless be applicable.

Despite the criminal procedure aspects traditionally not being subject to detailed EU regulation, the EU's approach is changing. The Lisbon treaty puts forward the principle according to which data protection applies to the police and to judicial cooperation in criminal matters. The proposal for reforming the EU data protection landscape (the *General Data Protection Regulation*)[131] is supplemented by a proposal for the *Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.*[132] This proposal aims to harmonise the rules relating to the processing of personal data by competent authorities such as law enforcement, applying also to domestic processing. The proposal addresses the challenges raised by *Framework Decision 2008/977/JHA*, characterising the latter as an instrument of 'limited scope and various other gaps**,** often leading to

[129] Examples include Platforms such as VIRTUOSO middleware and infrastructures such as iColumbo, Koops, p. 655. Read more on Versatile InfoRmation Toolkit for end-Users oriented Open-Sources explOitations (VIRTUOSO) at: 'Versatile InfoRmation Toolkit for End-Users Oriented Open-Sources explOitations (VIRTUOSO)' http://www.virtuoso.eu/.

[130] Koops, *op cit*, p. 665.

[131] *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52012PC0010.

[132] European Union, *Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data* http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52012PC0010.

legal uncertainty for individuals and law enforcement authorities, as well as to practical difficulties of implementation'.[133] After being adopted, the (now draft) Directive will be the principal instrument regulating the personal data processing by law enforcement.

These reforms are particularly noteworthy given the wide definition of 'personal data' in the EU. According to the *Data Protection Directive 95/46/EC*, personal data can be any information 'relating to an identified or identifiable natural person', and an identifiable person 'is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.[134] Whereas until now, law enforcement's activities have been exempt from the EU data protection rules, the adoption of the proposed Directive will raise interpretative questions regarding specific type of data that need to be processed, such as the IP address.[135]

There are also other issues that may arise during the implementation of the proposed Directive and the use of Tor. While still in its draft version, and thus subject to further changes, the proposal states, *inter alia*, that personal data must be 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes' (Art 4(2)), and 'kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which the personal data are processed' (Art 4(e)). The proposal also calls for the need for 'distinction between different categories of data subjects' (Art 5) so that Member States should ensure, as far as possible, that the controller makes a clear distinction between personal data of different categories of data subjects. There is no indication that law enforcement would be restricted from using anonymising software during its investigations, but the actual collection of data while using Tor or its hidden services must enable following these rules in the Directive. Practical implementation of these rules when collecting evidence via or within Tor may become challenging for national law enforcement. For example, it may not always be even possible to determine fully which parts of the data to be processed entail personal data (especially with data of a more technical nature such as IP addresses), and therefore whether personal data regulation applies to the processing of such data, and if so, to what extent. Neither is it clear what providing 'clear distinction between personal data of different categories of data subjects' would look like in practice when applied to, for example, large data sets published by Tor hidden services.

---

[133] European Union, *Impact Assessment Accompanying the Document Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data*, p. 31 http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf.

[134] European Union, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*. Article 2 (a).

[135] Notorious debates about whether an IP address is personal data or not in the EU. '/…/ IP addresses should be considered as personal data in many but not necessarily in all cases. The context of a particular case remains important, especially if "all the means likely reasonably to be used for identification, either by the controller or by any other person" should be evaluated', Peter Hustinx, 'Protection of Personal Data On-Line: The Issue of IP Addresses', *Revue Légicom*, 2009 https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2009/09-04-15_adresses_IP_EN.pdf.

3.1.1.3. *Use of Tor exit nodes for collecting evidence*

Another interesting issue related to Tor is using its exit nodes for collecting evidence. There have been reports claiming that some governments have control over and are running the exit nodes themselves.[136] While there is no concrete evidence to support the claim, the legal basis for such hypothetical surveillance should nevertheless be analysed.

Despite the differences between legal systems in different countries, surveillance can be broadly divided into two categories: targeted surveillance (usually 'interception' or similar in national law) that is carried out by or under the authority of law enforcement and is subject to a distinct regulatory regime, and non-targeted surveillance ('monitoring' or 'filtering') that is carried out by the law enforcement or private entities as a more general security measure and is not governed by such clear set of rules.[137] In both cases, the legal basis and specific conditions for authorising interceptions[138] must be outlined in domestic law and need to be in conformity with Article 8 of the European Convention on Human Rights.[139] Without authorisation, statutory defence or immunity from prosecution, these activities may be illegal and the evidence gained inadmissible in court.[140]

From the perspective of law enforcement, it would be difficult if not impossible to determine that the data that needs to be intercepted would be going through a particular exit node because Tor changes its path on average every 10 minutes,[141] and it would therefore be challenging to determine the scope and details of the warrant needed for accessing such data. Therefore targeted surveillance would be difficult to carry out in terms of practical implementation when running the Tor exit node. Should law enforcement nevertheless be in the position to monitor the data going through the exit nodes, or in any other way carrying out surveillance over Tor traffic, legal limits to surveillance need to be taken into account.

Unlike interception, monitoring of traffic does not target specific individuals or data but rather more general types of undesirable content for overall 'security' purposes, and may be effective only in certain types of environments.[142] If such monitoring does take place, it needs to have legal foundation and be in accordance with human rights law, especially because such monitoring would equally target users and their personal data whose activities are not illegal and do not pose any threat to the 'security' in question. In the context of Tor, such monitoring may be useful for tracking down illegal content but tracing the initiator of the traffic or taking firm action against the source of the traffic is challenging if not impossible.

---

[136] Sean Gallagher, 'Law enforcement seized Tor nodes and may have run some of its own', Arstechnica, http://arstechnica.com/security/2014/11/law-enforcement-seized-tor-nodes-and-may-have-run-some-of-its-own/.

[137] Ian Walden, *Computer Crimes and Digital Investigations*, Oxford University Press, 2007, p. 215.

[138] E.g. 'Member States may provide for lawful interception by the State where necessary to protect national security, the prevention and detection of crime and related circumstances (art. 15(1)); as well as by data controllers in the course of a "lawful business practice" (Art. 5(2))', Directive 2002/58/EC of the European Parliament and of the Council concerning 'the processing of personal data and the protection of privacy in the electronic communications sector' (Communication Privacy Directive) OJ L 201/37, 31.7.2002, in Ian Walden, 'Privacy and Data Protection', *Computer Law: The Law and Regulation of Information Technology*, Editors: Reed, C, Angel, J, 7th Edition, Oxford University Press (Oxford), 2011, para. 10.4

[139] European Court of Human Rights, European Convention of Human Rights, http://www.echr.coe.int/Documents/Convention_ENG.pdf.

[140] Ian Walden, *Computer Crimes and Digital Investigations*, Oxford University Press, 2007, p. 219.

[141] Tor FAQ, https://www.torproject.org/docs/faq.html.en#ChangePaths.

[142] Ian Walden, *Computer Crimes and Digital Investigations*, Oxford University Press, 2007, pp. 224-229.

Besides the activities described above, law enforcement agencies may also be interested in Tor exit nodes when assuming that their IP addresses may be connected with malicious content or activities. Hence, Tor exit node operators may receive subpoenas or other information requests from law enforcement or any other entity that may not be aware that, without having a legal precedent claiming otherwise, Tor exit node operators do not bear responsibility for the content running through their node. The Tor project suggests ignoring such requests or making use of the pre-prepared response templates.[143]

3.2. Tor and human rights

Tor is one of the best known tools for providing online anonymity and can be used for both legal and illegal purposes. In the previous subsection, we explored the activities of governments that try to fight crime enabled or facilitated by the use of Tor. In this subsection, we turn to introducing the legal uses of Tor: those that enable Tor users to protect and exercise their human rights.

3.2.1. Anonymity

Anonymity (from the Greek ἀνωνυμία), or namelessness, is the unidentifiability of a person in a given context. Related to anonymity is pseudonymity, which entails a repeatable identification of a person but avoids that person's real name. Anonymity and pseudonymity are beneficial or even necessary for people in many situations, such as lottery winners, victims of abuse, voters, people seeking medical or psychological aid, whistle-blowers, witnesses to serious crimes whose lives are threatened, and authors of controversial publications, as well as investigators, intelligence officers and other government agents.

Tor helps to improve one's level of online anonymity. Online anonymity itself is acknowledged by international documents, such as the Council of Europe's 'Declaration on freedom of communication on the Internet'[144] or the United Nations' 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression'.[145] The legality of the mere use of Tor is therefore well established.

---

[143] 'Abuse FAQ', https://www.torproject.org/docs/faq-abuse.html.en.

[144] Council of Europe, 'Declaration on freedom of communication on the Internet (Adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies)', Principle 7: Anonymity:

> *In order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity. This does not prevent member states from taking measures and co-operating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the fields of justice and the police.*

https://wcd.coe.int/ViewDoc.jsp?id=37031

[145] United Nations General Assembly, A/HRC/23/40, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue', section 23, 47-49 and others:

> *In order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous.*
> *[...]*
> *Restrictions on anonymity facilitate State communications surveillance by simplifying the identification of individuals accessing or disseminating prohibited content, making such individuals more vulnerable to other forms of State surveillance.*

http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

Even though anonymity is recognised and protected by law, it would be misleading to describe it as a separate right. That is because anonymity is context-dependent. Simply put, if something is legal, then doing it anonymously should also be legal; if something is illegal, then it does not become legal when done anonymously.[146] Instead, it is better to treat anonymity as an integral element in multiple human rights, such as the right to freedom of expression, the right to privacy, the right to freedom of assembly, the right to freedom of association, and the right to vote (whose exercise is actually compulsorily anonymous).

Tor has the potential to improve online anonymity in the exercise of the right to freedom of expression and in the protection of the right to privacy, which are discussed below.

3.2.2. Right to freedom of expression

The right to freedom of expression is set down in Article 19 paragraph 2 of the International Covenant on Civil and Political Rights (ICCPR).[147] However, some governments do not honour this right, and they orchestrate widespread online censorship. Tor is a way to bypass that censorship by misinforming the firewall about the source and nature of particular traffic. China, for example, bottlenecks all Internet traffic through government-controlled systems and subjects it to thorough inspection and filtering.[148] Here, improving the Tor infrastructure by upgrading the obfuscation protocol and increasing the number of bridges with pluggable transports allows the users of Tor to get past the 'Great Firewall'.[149]

The right to freedom of expression is limited.[150] In practice, the generally accepted reasons include, but are not limited to, defamation, hate speech, illicit pornography, copyright violations, or aiding or abetting a crime. Inasmuch as certain states engage in excessive online censorship, they interpret the limitation too broadly by international standards. Banning or indiscriminately suppressing Tor would mean an interference with the right to freedom of expression for which it would be difficult to imagine an appropriate justification.

---

[146] Compare the statement '*People are permitted to interact pseudonymously and anonymously with each other so long as those acts are not in violation of the law.'* in Columbia Insurance Company, Plaintiff, v. Seescandy.com, Sees Candys, Web Service Provider, No. C-99-0745 DLJ, United States District Court for the Northern District of California, 185 F.R.D. 573; 1999 U.S. Dist. LEXIS 12652; 51 U.S.P.Q.2D (BNA) 1130, March 8, 1999, Decided, http://cyber.law.harvard.edu/property00/domain/Sees.html

[147] International Covenant on Civil and Political Rights, New York, 16 December 1966. Article 19 paragraph 2:

> *Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.*

[148] Keith D. Watson, 'The Tor Network: A Global Inquiry into the Legal Status of Anonymity Networks', 1 Wash. U. Glob. Stud. L. Rev. 715 (2012), http://digitalcommons.law.wustl.edu/globalstudies/vol11/iss3/6

[149] Tor Project website, 'How to read our China usage graphs', https://blog.torproject.org/category/tags/china

[150] Article 19 paragraph 3 of the ICCPR:

> *The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:*
> *(a) For respect of the rights or reputations of others;*
> *(b) For the protection of national security or of public order (ordre public), or of public health or morals.*

http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

3.2.3. Right to privacy

Right to privacy is provided for in Article 17 of the ICCPR.[151] Even countries that are perceived to uphold the freedom of expression have engaged in activities highly intrusive in people's privacy. There are several recent examples about alleged surveillance activities undertaken by different State entities. For example, in October 2013, after the German Chancellor *'angrily condemned America's "unacceptable" behaviour after "firm suspicions" emerged that United States intelligence agencies had monitored her personal mobile telephone for almost four years'*, questions were raised about the acceptability of ubiquitous digital surveillance.[152] At the same time, *Der Spiegel* reported in August 2014 that *'Germany's foreign intelligence collection agency was spying on Turkey. It also reported, based on anonymous sources, that calls made by Secretary of State John Kerry and former Secretary of State Hillary Clinton were accidentally recorded.'* [153] Unlawful interference with privacy has also been underlined by the United Nations High Commissioner for Human Rights who noted in her report of 30 June 2014 that *'[p]ractices in many States have [...] revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy.'*[154] In such an environment, it is natural that both individuals and public entities would pay more attention to protecting their privacy, even if they feel that their freedom of expression is not imperilled.

However, even though the ICCPR does not contain any explicit limitation on the right to privacy, it is obvious that this right is not boundless. The European Convention on Human Rights, which defines the right in similar words, provides a list of exceptions.[155] For example, certain measures during a criminal investigation can legally interfere with the right to privacy. Nevertheless, the alleged ubiquity of mass surveillance raises concerns about the proportionality between the results of such surveillance and the interference with people's privacy.[156]

---

[151] Article 17 of the ICCPR:

> *1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
> *2. Everyone has the right to the protection of the law against such interference or attacks.*

http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

[152] The Telegraph, 'Angela Merkel: spying between friends is unacceptable', http://www.telegraph.co.uk/news/worldnews/europe/germany/10403437/Angela-Merkel-spying-between-friends-is-unacceptable.html

[153] David Francis, 'Spies Like Us: Germany Spies on Allies, Too', http://thecable.foreignpolicy.com/posts/2014/08/18/spies_like_us_germany_spies_on_allies_too

[154] Report of the Office of the United Nations High Commissioner for Human Rights, 'The right to privacy in the digital age', http://www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a.hrc.27.37_en.pdf

[155] Article 8 of the ECHR:

> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

http://www.echr.coe.int/Documents/Convention_ENG.pdf

[156] Report of the Office of the United Nations High Commissioner for Human Rights, 'The right to privacy in the digital age', page 16, http://www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a.hrc.27.37_en.pdf

3.3. Content liability of Tor exit node operators

Content liability is perhaps the first legal issue that comes to mind when analysing the use and abuse of Tor. A recent example dates back to 2012, when Austrian police raided the flat of William Weber in Graz, and seized the computer hardware located there, which he had used to control Tor exit nodes physically located abroad.[157] Some unknown users of Tor had used his exit nodes for downloading child pornography, and the authorities suspected Weber of doing the downloading himself, presumably because they were not aware that the exit nodes were not the final destination of the files. Weber was ultimately convicted on 30 June 2014 to a three-month jail term suspended for a three-year supervision period for aiding and abetting the distribution of child pornography.[158] Although this was only the verdict of a lower court, Weber decided not to appeal it, citing financial and personal reasons,[159] so the case will not undergo a further juridical scrutiny.

In Austria, intent is a necessary element of criminal responsibility for aiding and abetting. In the judgment, the regional criminal court in Graz accepted several quotations by the defendant from a chat saying *'you can host child porn on our servers'* and *'if you want to host child porn ... I would use Tor'* as the proof of the defendant's indirect intention to aid an unknown perpetrator in the distribution of child pornography, despite Weber's claims that these quotations were taken out of context. The court's decision *'highly depended on the special circumstances of the case [and] cannot be seen as a general ruling against Tor services'*, said Maximilian Schubert, general secretary of the Austrian association of Internet Service Providers.[160]

The *Weber* case thus highlighted but left unanswered a very interesting legal question with an EU-wide significance: is the Tor exit node operator protected from civil and criminal liability by the clause on 'mere conduit' from Article 12 of the E-Commerce Directive?[161]

A Tor exit node operator easily fulfils the conditions listed under Article 12 paragraph 1(a) to (c) of the E-Commerce Directive, because in a standard situation the node acts as a true relay and the operator does not interfere with the transmission. However, we must examine two additional conditions from paragraph 1: is the Tor exit node operator a 'service provider'? And is the provision of a Tor exit node an 'information society service'?

Article 2 of the Directive defines 'service provider' as 'any natural or legal person providing an information society service' and 'information society services' by reference to Article 1 paragraph 2 of Directive 98/34/EC[162] as amended by Directive 98/48/EC as *'any service normally provided for*

---

[157] BBC News, 'Austrian police raid privacy network over child porn', http://www.bbc.com/news/technology-20554788 ; Patrick Howell O'Neill, 'The darkest net', http://kernelmag.dailydot.com/issue-sections/features-issue-sections/10407/history-child-pornography/

[158] Loek Essers, 'Tor exit node operator convicted of abetting spread of child porn', http://www.pcworld.idg.com.au/article/549645/tor_exit_node_operator_convicted_abetting_spread_child_porn/

[159] William Weber's blog, 2 July 2014, https://rdns.im/court-official-statement-part-1

[160] Essers, *op cit*.

[161] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32000L0031

[162] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1998L0034:20070101:EN:PDF

remuneration, at a distance, by electronic means and at the individual request of a recipient of services...'.

The definition provides a detailed interpretation of three of its conditions, which are easy for a Tor exit node to fulfil, but the wording 'normally provided for remuneration' remains difficult to interpret with respect to Tor, which is by its nature a free service. In a judgment from 11 September 2014 (C-291/13), the Court of Justice of the European Union (CJEU) provided only a limited interpretation by stating that *'the concept of "information society services", within the meaning of that provision, covers the provision of online information services for which the service provider is remunerated, not by the recipient, but by income generated by advertisements posted on a website.'*[163] This explanation is fully in line with previous European Commission statements,[164] but it does not help to determine the legal status of Tor exit nodes.

In an ongoing case, the CJEU (7 O 14719/12)[165] has been requested to assess what is meant by 'service normally provided for remuneration'. The judgment of the CJEU is hard to predict but it will certainly have an effect on how Tor is seen as a service provider. If the CJEU decides that mere conduit cannot be applied to free services, even by analogy, then a question arises about the viability of free services, whose providers would then be responsible for the transmitted data. This would put the EU in an awkward position by comparison to the US, where safe harbour rules for all ISPs are well-established.[166] As a possible solution, a study commissioned by the European Commission's Information Society and Media Directorate-General recommends adopting a different criterion if the ambiguity would not be resolved by case law.[167] However, this would require changing the Treaty on the Functioning of the European Union, which contains a cross-cutting definition of 'service' in Article 57,[168] so it may yet take considerable time.

3.4. Legal limits on traffic monitoring

Tor may be used for carrying out various activities illegal in domestic legislation, such as selling and buying illegal goods, or disseminating child pornography. All these are generally criminalised under national criminal legal framework. However, it should not be overlooked that the monitoring of the traffic going via Tor may also be illegal under national law.

Little legal analysis has been undertaken regarding the activities of a Tor exit node operator. There is no concrete evidence to claim that running the Tor exit node is illegal as such. However, it should not

---

163 http://curia.europa.eu/juris/document/document.jsf?text=&docid=157524&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=13299

164 http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2009-0969&language=EN; http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2009-4374&language=EN

165 Martin Husovec, 'Munich Court Asks CJEU About Injunctions Against Operators of Open WiFis', http://www.husovec.eu/2014/10/munich-court-asks-cjeu-about.html

166 See for example Daniel A. Tysver, 'ISP Liability', http://www.bitlaw.com/internet/isp.html, and Jack Scheckter, 'The DMCA Safe Harbor Remains Intact After Viacom v. YouTube', http://sunsteinlaw.com/the-dmca-safe-harbor-remains-intact-after-viacom-v-youtube/

167 'Legal analysis of a Single Market for the Information Society (SMART 2007/0037)', Chapter 06. Liability, page 39, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=835

168 Consolidated version of the Treaty on the Functioning of the European Union, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:12012E/TXT

be disregarded that the Tor exit node operators have access to the traffic going through their exit nodes. Tor anonymises the origin of the traffic, and ensures encryption inside the Tor network, but it 'does not magically encrypt all traffic throughout the Internet'.[169] Or in other words, Tor does not offer 100% anonymity since the exit node is in a position to capture any traffic passing through it.[170] For example, the Tor exit node operator can intercept private e-mail messages (unless there is end-to-end encryption) as well as get access to user names and passwords.[171] In 2014, researchers identified over twenty 'spoiled onions' (Tor exit nodes) that were run to sabotage Tor traffic.[172]

Even if such access to data and interception is done 'in good faith' such as when a researcher wants to find out what type of data is transferred by Tor for the purposes of improving the service for legitimate users**,** and identifies and blocks traffic which is in contradiction with law (for example, child pornography, hacking attempts, and most torrent traffic), such monitoring would be illegal in most legal systems.

Due to the differences in national legislation, countries may have various approaches to criminalising activities that could be undertaken using Tor. For the sake of clarity, the following analysis will be based on the Council of Europe's Convention on Cybercrime.[173] Traffic monitoring could be categorised under various articles (such as Article 2 'Illegal access'), but foremost it should be analysed in the context of Article 3 that obligates the Parties to criminalise 'illegal interception':

> ***Article 3 – Illegal interception***
>
> *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.*[174]

[169] Tor project, FAQ, https://www.torproject.org/docs/faq.html.en#CanExitNodesEavesdrop

[170] Tails, Warning, https://tails.boum.org/doc/about/warning/index.en.html#index1h1

[171] E.g. a case where a security researcher intercepted thousands of private e-mail messages sent by foreign embassies and human rights groups around the world and posted the user names and passwords for 100 e-mail accounts used by the victims. Read more, Kim Zetter, 'Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise', Wired, 9 October 2007.

[172] Dan Goodin, Arstechnica, 22 January 2014, 'Scientists detect "spoiled onions" trying to sabotage Tor privacy network', http://arstechnica.com/security/2014/01/scientists-detect-spoiled-onions-trying-to-sabotage-tor-privacy-network/

[173] The Convention on Cybercrime has been ratified by all NATO member states except Canada, Greece and Poland; however, even these states have signed it. See http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG; Nevertheless, Greece and Poland have to implement the *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*, which forces the EU Member States to implement provisions very similar to those of Articles 2 to 6 of the Convention on Cybercrime in their domestic law. See http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1401259123247&uri=CELEX:32013L0040

[174] Convention on Cybercrime, Budapest, 23.XI.2001, http://conventions.coe.int/Treaty/en/Treaties/html/185.htm

The Explanatory Report[175] to the Convention on Cybercrime puts Article 3 into connection with Article 8 of the European Convention on Human Rights, which protects private life and correspondence.[176] Even though the primary aim of human rights treaties is to protect individuals from the abuse of state power, the Convention on Cybercrime requires its Parties to criminalise illegal interception by anyone, including law enforcement and individuals. Interception by 'technical means' is understood to mean 'listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices.'[177] To give rise to criminal liability, the illegal interception must be committed 'intentionally', and 'without right'; the latter suggesting that domestic laws may also offer legal justifications of such activities.[178] One such justification would be the consent of the participants of the transmission, or if surveillance is lawfully authorised in the interests of national security or the detection of offences by investigating authorities.[179] Other examples may include monitoring employees during working hours;[180] using cookies on the system of a website visitor;[181] and criminal investigation or information collection by an intelligence agency.

This is also applicable to monitoring a Tor exit node for research purposes. Unless there are explicit justifications in national law allowing for such monitoring, the exit node operators should assess their decision to undertake such research with care. The Tor website also advises Tor exit node operators not to 'snoop on the plain text traffic that exits through [their] Tor relay'.[182] If Tor exit node operators aim to limit the amount of torrent traffic passing through their node, the operators can block certain ports used by torrent clients, and consequently reduce the number of takedown notices submitted to them by collective copyrights management organisations.[183] Nevertheless, researchers and other private entities will find it difficult, if not impossible, to identify legal grounds for monitoring Tor traffic by intercepting Tor exit nodes.

---

[175] Explanatory Report to the Convention on Cybercrime, paragraph 51, http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm

[176] European Convention on Human Rights as amended by Protocols Nos. 11 and 14 [and] supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 13, http://www.echr.coe.int/Documents/Convention_ENG.pdf; corresponding provisions are also in Article 7 of the Charter of Fundamental Rights of the European Union, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF, and Article 17 of the International Covenant on Civil and Political Rights, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

[177] Explanatory Report to the Convention on Cybercrime, paragraph 53, http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm

[178] Explanatory Report to the Convention on Cybercrime, paragraph 55, http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm

[179] Explanatory Report to the Convention on Cybercrime, paragraph 55, http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm

[180] *Copland v. The United Kingdom*, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-79996#{"itemid":["001-79996"]}.

[181] Explanatory Report to the Convention on Cybercrime, paragraph 58, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

[182] Electronic Frontier Foundation, 'The Legal FAQ for Tor Relay Operators', https://www.torproject.org/eff/tor-legal-faq.html.en

[183] Tor Project, 'Reduced Exit Policy', https://trac.torproject.org/projects/tor/wiki/doc/ReducedExitPolicy.

4. Conclusion

In this paper, we presented an overview of the Tor anonymisation network from the technical perspective and introduced several legal issues related to its use.

The technical part started with an overview of Internet privacy tools and censorship circumvention methods. Tor, which is a third-generation onion routing system, was seen to be the most common and popular tool. However, there are various issues which hinder the effectiveness of Tor. Some of them arise from the properties of Tor, although others are related to user mistakes or indirect matters which affect the system. Due to these weaknesses, technical assessments show that providing 100% privacy is not possible at this stage. However, the use of Tor, especially in combination with other technical solutions like VPN, significantly improves the level of anonymity of the users.

The legal section presented selected legal challenges related to the use of Tor. We first discussed the relationship between governments and Tor, and focused on the use of Tor by law enforcement. We identified a number of legal issues that should be subject to further analysis, such as the use of Tor for collecting evidence. For example, open source intelligence of Tor resources is considered to be uncontroversial, but this may change with the advance in technical capabilities. Also, the data protection reform in the EU may lead to complications in criminal investigations involving Tor. Additionally, we noted that the collection of evidence at the exit nodes is problematic due to the inability to target the collection precisely enough.

We then turned to discussing human rights and Tor. We reiterated that anonymity is an integral part of established human rights, and therefore a complete ban of Tor or its indiscriminate monitoring would constitute an undue interference with these rights. For the same reason, any legal interception involving the Tor network is subject to the same requirements as the interception of other Internet traffic.

Finally, we found that in the EU, Tor exit node operators are generally protected from liability for the content passing through the exit node, but this protection is far from absolute, and they should clearly distance themselves from any illegal activities involving the exit node in order to avoid possible complications.

It can therefore be concluded that there are many under-researched issues related to the Tor network that need to be taken into account both by its users and by governments designing national policies and reviewing national legal frameworks.