Risk assessment for I2P with an enhanced outproxy design.

Dolf Smits

January 2018

Master thesis

Supervisor: dr. ir. Pieter Burghouwt

Second reader: prof.dr. ir. Jan van den Berg

Cyber Security Academy, The Hague

“I don’t know why people are so keen to put the details of their private life in public; they forget that invisibility is a superpower.”

Banksy

Abstract

The Internet has become a vital way of communication in the human society. However, the communication of users on the Internet is becoming more and more interesting to third parties. There is an increasing awareness that the Internet and privacy do not fit well together. This has resulted in the development of several anonymity networks, such as The onion routing network (Tor) and the invisible Internet project (I2P).

While the Tor network has been adopted at a rather large scale, the low capabilities of using I2P for communication to the public Internet, seem to hinder the acceptance of this anonymity network by a broad audience. Therefore, we asked ourselves the question: “Can I2P be enhanced so that it has better capabilities for communication with the public Internet, and what will be the risks when this enhancement is implemented?”

We first inventoried the users and other stakeholders of anonymity networks and their requirements. Based on these requirements, and the current design of I2P, we propose a design enhancement. We defined a new classification for all the threats, based on the goals and vulnerabilities that are abused. This includes a complete new group of non-technical attacks on anonymity networks that are formed by legislation measures and are a threat to anonymity networks.

We then made an inventory of all the threats and risks as given by the I2P website and by a literature search. This results in a new overview of all known attack scenario’s.

Based on this information a risk assessment is made. A standard cyber risk assessment approach is extended with the criteria Simplicity and Effectivity, which together are used to give an estimation of the likelihood that an attack will lead to an incident. This gives us 7 high risks, the majority of these risks are present in the current implementation of I2P. For each of these risks we suggest several mitigation measures to lower the risks.

We conclude by observing that that our enhancement will not lead to higher risks for the users, and that some of our enhancements will even lower the existing risks that are in I2P. If this is combined with our suggestions for mitigating measures, we argue that I2P can become a more versatile and robust anonymity network needed for widespread adoption.

Acknowledgment

The author would like to acknowledge the contribution and support of several people during this master study.

First of all, my family who has missed me on many weekends and evenings when I locked myself up in my room. Then off course, the staff and teachers of the CSA, their drive to launch a new executive master study on the field of cybersecurity, has made this study possible. Also, my fellow students for the support and discussions on the broad field of cybersecurity. My employer, who made this study possible for me. And last but not least, Jan and Pieter, for your support, discussions and critical remarks on my thesis. I couldn't have written this thesis without you.

Table of Contents

1. introduction

1.1. The need for privacy

The use of the Internet for communication has earned a vital position in the human society. It has become the preferred communication medium for people. But the backside of this development is, that this (private) communication has become interesting to other parties. Now, an increasing number of people realise that privacy and the current Internet do not work well together. The first "demand" for anonymity was the well-known paper by David Chaum [1], published in 1981, already 12 years after Oct. 29, 1969, the day that the first message was sent over Internet. But also 7 years before the emergence of the famous Internet worm, being the first widespread security incident[2].
Several initiatives have been started to redesign the Internet from a clean slate, [3][4][5][6], which all name privacy as an important factor to consider.
Privacy of the Internet users can be enhanced in two fundamentally different ways.
One way is to ensure that all organisations that collect privacy sensitive data will not abuse the collected data, and ensure the protection of the data in an appropriate way. This is the privacy protection as pursued by law such as the General Data Protection Regulation (GDPR).
The second way is to ensure anonymity on the Internet, to make it impossible to link the collected privacy sensitive data to a natural person.

Although the new GDPR will become effective in Europe this year, many people are not convinced that their privacy will be better protected by law or governmental organisations. Indeed, the new laws that are accepted by the parliaments in Europe, for example the "Sleepnetwet" in the Netherlands [7] [8] [9], suggest that even the governments of the member states of the EU do not always fully respect the privacy of their inhabitants.
A growing number of organisations raise concern about the privacy risks that result from laws that expand the possibilities of wiretapping and data retention by authorities. For Europe these organisations formed an association called "European Digital Rights" (EDRI) [10] which has members in most countries. For the Netherlands, Bits of Freedom, is a well-known organisation. For the USA, the Electronic Frontier foundation (EFF) [11] is the most well-known.
Considering this, it is believed that protecting privacy by anonymity is becoming the utmost importance to protect the freedom of speech.

1.2. Dark side of anonymity

Although there is a definite need for privacy on the Internet, there is also a negative aspect of anonymity. Not only sincere people are attracted by anonymity, but anonymity can also be used to hide criminal and terroristic activities. Where cryptography can hide what is communicated between people, anonymity can also hide who is communicating. It is clear that cryptography and anonymity sometimes hinders the work of law enforcement. And these arguments can be used by legislative powers to define laws that threaten the privacy of their citizens, such as the previous mentioned "Sleepnetwet".

1.3. History

After the first article of David Chaum, it lasts until 1995 before the first design work is done on “onion routing” and the first official publications are in 1996. Since 1997 until 2004, funding from the Tor projected is attributed by the “Defence Advanced Research Projects Agency” (DARPA) and the Naval Research Laboratory (NRL)[12]. Goal is to build a network which hides all routing information. This generation-0 network has run until 2000, the same year that JAP[13] goes live. Also in 2000 the famous article about Freenet was published. [14]
It states as design goals: “

- Anonymity for both producers and consumers of information
- Deniability for storers of information
- Resistance to attempts by third parties to deny access to information
- Efficient dynamic storage and routing of information
- Decentralization of all network functions”

It still takes until 2001 before development starts again, and in 2003 the Tor network as it runs today is brought live again, with a dozen nodes.
In 2003, the Invisible Internet Project (I2P) is started, as a spin-off development from Freenet.[15]

The current widespread concern about privacy and anonymity on the Internet has contributed to a growing deployment of these aforementioned anonymity networks, like Tor[16], Freenet[17] and I2P[15] to address the mentioned concerns.
Other anonymity solutions are in use as well, like the Java Anonymous proxy (JAP, AKA JonDoNym)[13], GNUnet [18], TAHOE-lafs[19] and SAFE Network[20]).

But still all these solutions have not widely spread under the Internet users of today. Also, all these solutions have their advantages, as well as their disadvantages.
In many cases, deployment by an inexperienced Internet user is not trivial, some basic knowledge is required and often the application does not completely meet the user requirements.
For example, the Tor network can only reliably be used with a specially prepared Internet browser and then it only works for HTTP network connections via that browser. It does not always work for other Internet protocols, such as e-mail traffic via the SNMP protocol as this is always sharing the IP-address of the client with the server. The Tor network is depending on a fixed infrastructure where the entry-points and exit-points are fixed. Therefore, it has a higher chance of being blocked or taken down by a government then a more distributed overlay network. Despite this, Tor is probably the most well-known and mostly used anonymity network under the Internet users with 2 to 2,5 million users per day [21].
In contrast to Tor, the I2P network is mainly designed for communicating anonymous with designated partners, and is less usable when a public site is visited. It has a more flexible and fluid infrastructure then TOR, because all nodes joining the network are used as part of the infrastructure for other nodes. This creates a highly-distributed infrastructure.
The Freenet is also a self-contained network, and can only be used for Internet traffic in the Freenet, and not for visiting public Internet sites. It also uses a flexible and fluid infrastructure.

Although Tor is the most widely used network, comparisons between Tor and I2P show that the I2P network is a more resilient network which guarantees a high level of anonymity. [22] However, I2P is not the best choice when users want to visit public Internet sites, as the outproxy functionality, which gives access from the Invisible Internet to the Public Internet, is not of major importance for the design, as the website states: “Remember: I2P was not designed for creating proxies to the outer Internet. Instead, it is meant to be used as an internal network”. [23]
Because of this concentration on internal communication within I2P, only a few instances of outproxies exist, the connection between the I2P network and the public Internet is not working very well and it is relatively vulnerable for Denial-of-Service attacks.
Enhancements on this outproxy functionality could make I2P a better anonymity choice for many Internet users.

1.4. Definition of Internet anonymity and Internet privacy

The Merriam-Webster dictionary describes anonymity[24] as: “the quality or state of being anonymous” and it defines anonymous as: “not named or identified”.

Based on this, we define Internet anonymity as: “The state of an Internet user of being not identified and not being identifiable”.

The same Merriam-Webster dictionary describes privacy as “the quality or state of being apart from company or observation”. For our research, the part “being apart from observation” is important.
Merriam-Webster learners dictionary describes observation[25] as “the activity of paying close attention to someone or something in order to get information”.
When we combine this, Internet privacy can be defined as: “The state of the Internet user of being free from information gathering by others about himself”

However, an Internet user having privacy, and although no one is paying close attention to him to collect information, he is still leaving information behind and is not anonymous. This means that it is relatively simple to start collecting information about that user afterwards, and thus violate his privacy.

So, for Internet users the definition of privacy is too weak, it just defines a momentary state, but it has no influence on any future state.
Therefore, we redefine the definition of Internet privacy as:

“Internet privacy is the state of an Internet user where it is impossible to collect information about the user, about his actions on the Internet and about the natural person or organisation behind that Internet user”

This definition will be valid over time, it is changed form a passive state (not under observation) to an active state (impossible to collect) and adds “actions” instead of only “information”. Also added is the notion that it is not possible to know who is behind the actions the Internet user is performing.
So, there is a difference between anonymity and privacy; Where anonymity is concentrating on being unidentified, privacy concentrates on being free from information gathering.

Anonymity is stronger than privacy as there is no possibility to collect information about an unidentifiable user. So, an anonymous user always has privacy.

We use this definition of Internet anonymity throughout this thesis.

1.5. Goal of this thesis.

Assuming that I2P will be enhanced to add outproxy functionality to all nodes, in the way as described in this thesis, what are the risks for the anonymity and privacy of the users?

To define the answer to this question, we will answer the following sub-questions:

1. How is the current I2P software functioning?
2. Which stakeholders can be identified for this research?
3. What are the legal consequences of the assigned exit-role to all participating nodes? (from the perspective of the different stakeholders)
4. What requirements can be defined for the proposed enhancement?
5. How can the exit-role functionality be incorporated in the design?
6. To what extent is it possible to route all the node network traffic through the I2P overlay network, thus using the I2P software as a virtual entry-point for the node?
7. What existing vulnerabilities exist in I2P?
8. To what extent will the abundant presence of exit-point and virtual entry-point functionality in I2P influence existing vulnerabilities and existing attack scenario's?
9. Which new threats to security or anonymity will arise from the newly assigned exit-point role to all nodes?
10. Assess the risks from the existing I2P configuration and the risks when the proposed enhancements would be implemented.
11. How can the existing threats and the new threats be mitigated? And what are the risks that remain?

1.6. Guidance

In this chapter, we started with an introduction, containing a general description about the need for anonymity and the threats to the Internet users. A short history of anonymity on the Internet was given, followed by a definition of Internet anonymity and Internet privacy. After that, the research goal was explained. Now we will explain how we reached the goal. (see

)

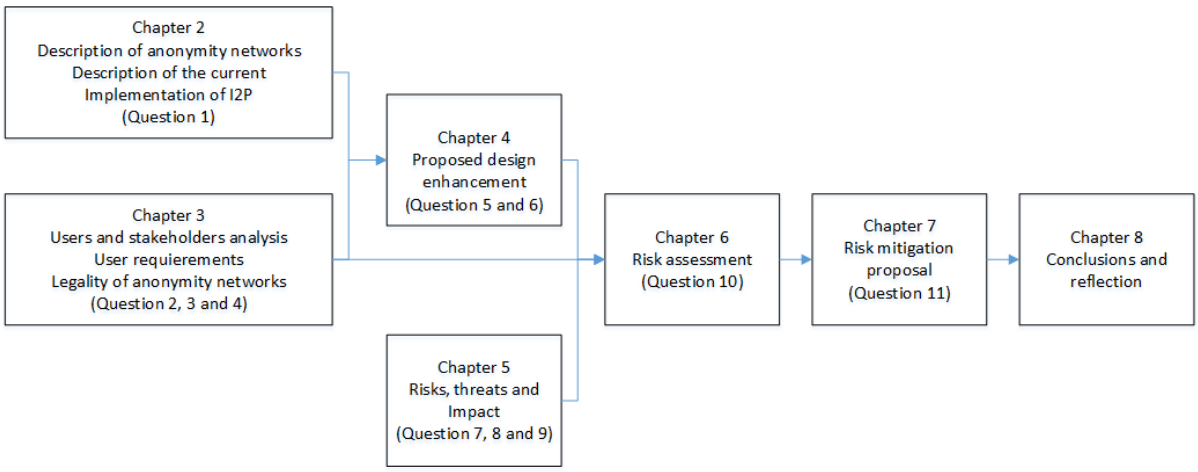

Figure 1 Guidance through the thesis

In chapter 2, we give a short description of general anonymity solutions, an extensive description of I2P, including an explanation of I2P as overlay network on the Internet and a short comparison with Tor. This is based on literature search and the public information on I2P.

In chapter 3 we perform a stakeholder analysis and user requirements.
This chapter contains an inventory and description of users, their activities and their requirements, which will be used as input for the design enhancement.
It also contains an inventory of other stakeholders that might influence the environment and threats to I2P and thus might be used in the risk assessment. We will also present a short overview of the legal aspects of running anonymity software. This is also based on literature and consultation with a legal specialist.

The results from chapter 2 and 3 are combined in chapter 4 where we describe the proposed enhancement, this solution will be used for the risk assessment.

Chapter 5 will then highlight the threats, risks and impact. We describe the current known technical threats and their risks. This includes the newly introduced threats that are caused by our design proposal. But we will also describe other (non-technical) threats to anonymity networks.

Now that the proposed enhancement is defined, the users and other stakeholders have been inventoried and the threats and risks are clear, the risk assessment can be made and is presented in chapter 6.
We present a risk assessment for all the threats to I2P in a qualitative way. We end this chapter with an overview of the results and the highest risks.

In chapter 7 we will reflect on the risk assessment results and define some possible mitigation measures. We also make some remarks about I2P and the Tor network and the influence of the number of users on the anonymity.

We end this thesis in chapter 8 with conclusions and a reflection on our work, which gives some suggestions for further research.

2. Description of anonymity networks

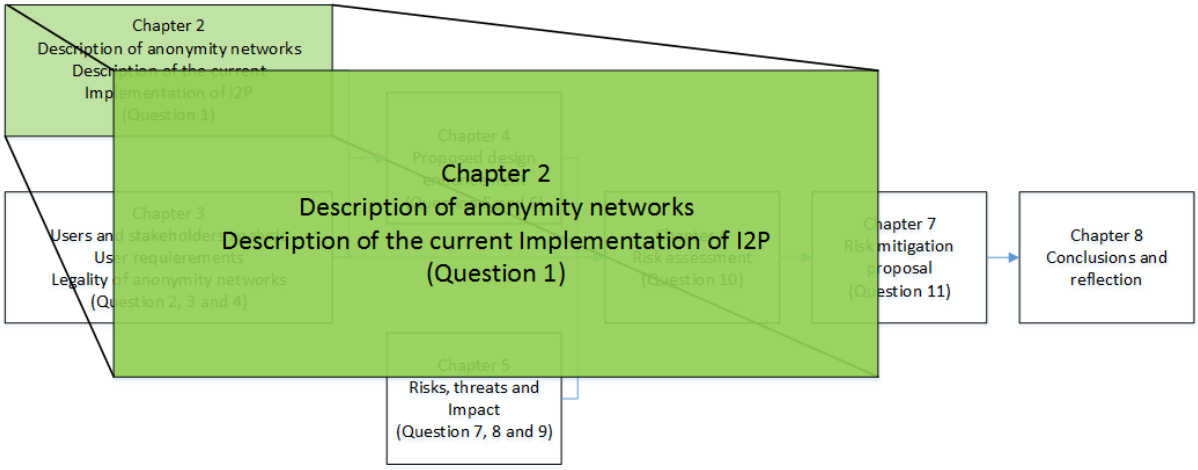

Figure 2 Guidance for chapter 2.

In this chapter, we will start with a short introduction into anonymity networks to give more understanding about the possible anonymity solutions that are available. This will be followed by an extensive description about the current implementation of the Invisible Internet Project (I2P). This is divided in three parts; one part about a node joining the network, one part about the actual usage of the network, and finally a part about the connection to the public Internet. We conclude this chapter with a short comparison to Tor, which is, at this moment, the most widely used anonymity network.

2.1. Introduction into anonymity networks

There are different kinds of solutions to ensure anonymity on the Internet.
Marques and Zuquete [26] make a distinction of 4 different types of anonymity solutions. These are:

- Anonymizers (e.g. [27])
  - These are services to which a user can connect. The service will, on behalf of the connected user, access the Internet. Thus, the visited service only sees the access by the anonymizer. Thus, anonymity relies completely on the owner of the anonymizer and the trust the user has in the anonymizer service. Sometimes a virtual private network (VPN) is used as an anonymizer service.
- Distributed File sharing
  - A distributed file-sharing mechanism stores files on the network nodes from the participants, which can then be retrieved by the users using a key. One example is Freenet[17].
- Crowds
  - A solution where a crowd of people issue requests on each other's behalf. Any member can either submit the request directly to the end server or forward it to another randomly chosen member, example is Crowds[28].
- Mix networks[1]
  - The idea originates from the paper of David Chaum[1]. He was the first to introduce the concept of mixes, where a "mix computer" forwards the mail,

but with a different return address, thus ensuring that the receiver does not know who sent the mail. Several mix computers can be cascaded to raise the anonymity. When returning a mail to this different return address, the mix computer retranslates it to the original return address and send the mail through. In this way two people can communicate with each other anonymously.

- This idea was extended by Tor, but then for HTTP and other network traffic. It was then extended by the concept of onion routing. With onion routing, a message is encrypted several times, ensuring that only the receiver can remove the layers of encryption. This guarantees that the message is not altered or read during its travel through the several mix nodes.
- This idea was again extended with the introduction of Garlic routing[29] (chapter 8.1.1.), which is used by I2P. Now several messages are combined into one new message which is encrypted and sent through, latter on, this message is decrypted, split in the original messages and these are again sent on, each to their own destination. This feature makes traffic analysis harder.

A common denominator in all these solutions is the fact that they are all run as an overlay on the existing Internet infrastructure. Each network relies on the existing Internet protocol and the TCP/IP (or UDP/IP) stack. This has the advantage that all these solutions can be used on the existing, worldwide present, Internet. The disadvantage is that each packet that is sent through the network can be seen, together with its metadata, like source address, destination address and timestamps. This can be used in several methods to de-anonymize the user who sent the packages.

2.2. Description of I2P network

I2P [15] is an overlay mix network. Development started in 2003, it has about 50.000 concurrent users each day. As shown by Figure 3[30]

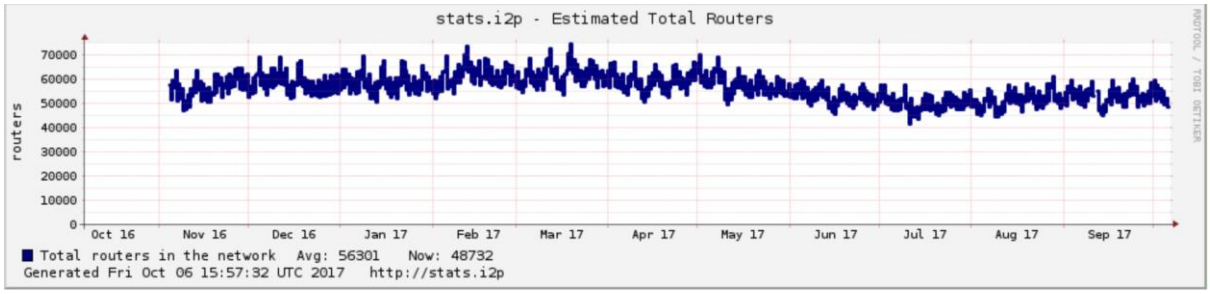

Figure 3 Estimated total number of routers on I2P

2.2.1. General overview of the working of I2P.

We give a short description of the way I2P currently works. This is based on [31], [22] and [15]. These sources give a more detailed description.

Figure 4 is an example of the basic I2P layout. The blue computers are all different nodes on the I2P network, and can communicate with each other over the Internet.

The four red computers are also I2P nodes, but these have a special function and are called the floodfill routers. This is a special node in the I2P network that contains a part of the I2P distributed hash table (DHT). This DHT is called the netDB and contains two types of information, the RouterInfo and the LeaseSet's.
RouterInfo is stored for every running I2P node, and it contains the information about how to contact that node. It contains information like IP-address, port number, I2P version and information about the transport capabilities.
A LeaseSet is stored when a I2P node is building an inbound tunnel on the I2P network, it contains information on how to contact the offered service. This information specifies a set of entry points to tunnels leading to the service.
I2P has two types of tunnels, client tunnels and exploratory tunnels, where the client tunnels are used for sensitive operations, and exploratory tunnels for other operations, like contact to the netDB.

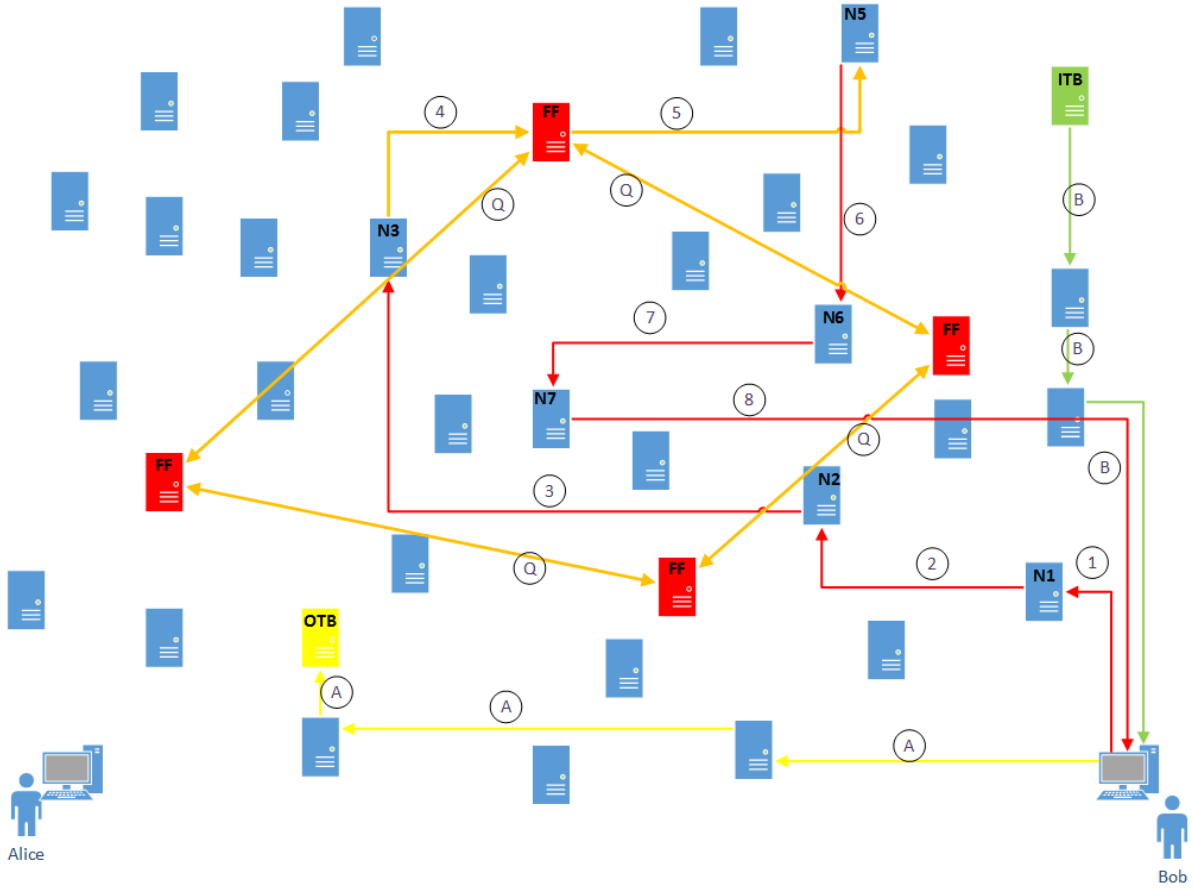

Figure 4 Basic I2P layout, bootstrapping a node

We will explain what happens when Bob starts his computer and connects to the I2P network. We assume that the other nodes in the picture are already up and running and are fully integrated in the I2P network.

1 When the I2P software is started, it first builds up the exploratory tunnels, by asking some nodes to join his tunnels. These requests are sent to the Nodes N1, N2, N3 for the outbound exploratory tunnel and to the nodes N5, N6 and N7 for the inbound exploratory tunnel.

2 Via the exploratory outbound tunnel (red, 1, 2, 3) connects to the floodfill router (orange, 4).
3 It publishes the own RouterInfo, so that the node of Bob can be used by others for creating tunnels.
4 It also asks for RouterInfo from other routers which is then sent from the floodfill to the exploratory inbound tunnel (orange, 5)
5 The RouterInfo is received through the exploratory inbound tunnel (red 6, 7, 8) by Bob's node.
6 Bob starts building the client inbound tunnels (B) and client outbound tunnels (A) by sending tunnel request to the nodes. Every node connecting to the I2P network starts at least two client tunnels, one inbound tunnel and one outbound tunnel. All tunnels are uni-directional. Tunnel length is normally three nodes long, but the length is a trade-off between anonymity and performance [32].
Tunnels are short-lived, they only last for about ten minutes and then new tunnels are created, this to prevent traffic analysis attacks[33].
7 So, the node of Bob builds one client outbound tunnel (the yellow arrows, A) which ends on the yellow I2P node, (Outbound Tunnel Bob, OTB).
8 It also builds a client inbound tunnel (green arrows, B) where the entry point is the green I2P node, (Inbound Tunnel Bob, ITB)
9 It then connects to the floodfill router again, to publish the LeaseSet for his node, which contains the information about the entry point of his inbound tunnel.
10 The floodfill router distributes this info to other floodfill routers (orange arrows, Q).

Now the computer of Bob is a fully integrated node in the I2P network. This is also represented in the flow diagram from Figure 5.

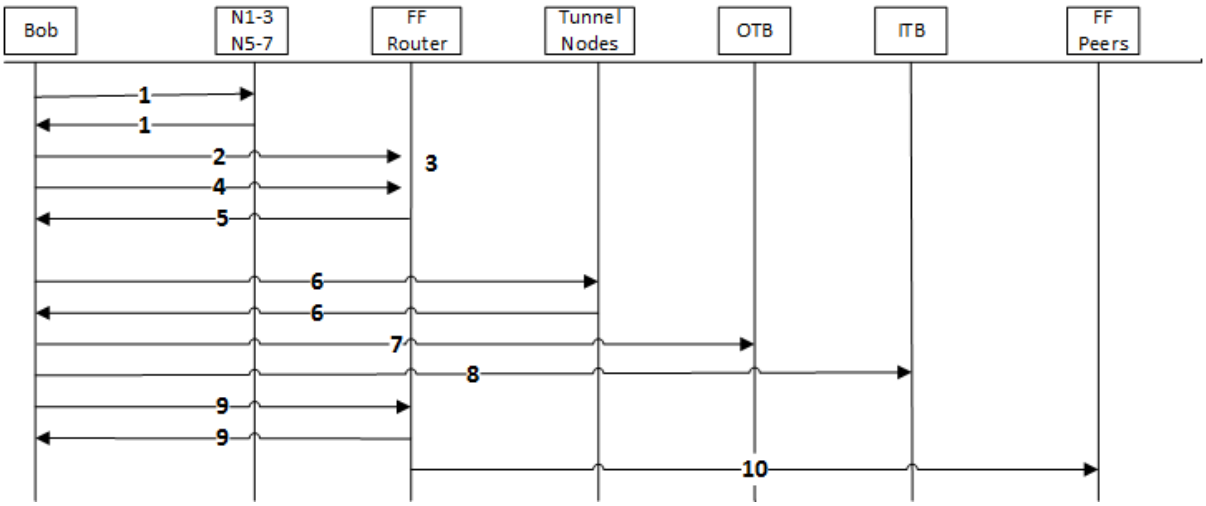

Figure 5 protocol flow diagram of booting an I2P node

The next step for Bob will be to start communicating, in this example with Alice.
This explanation is based on Figure 6.

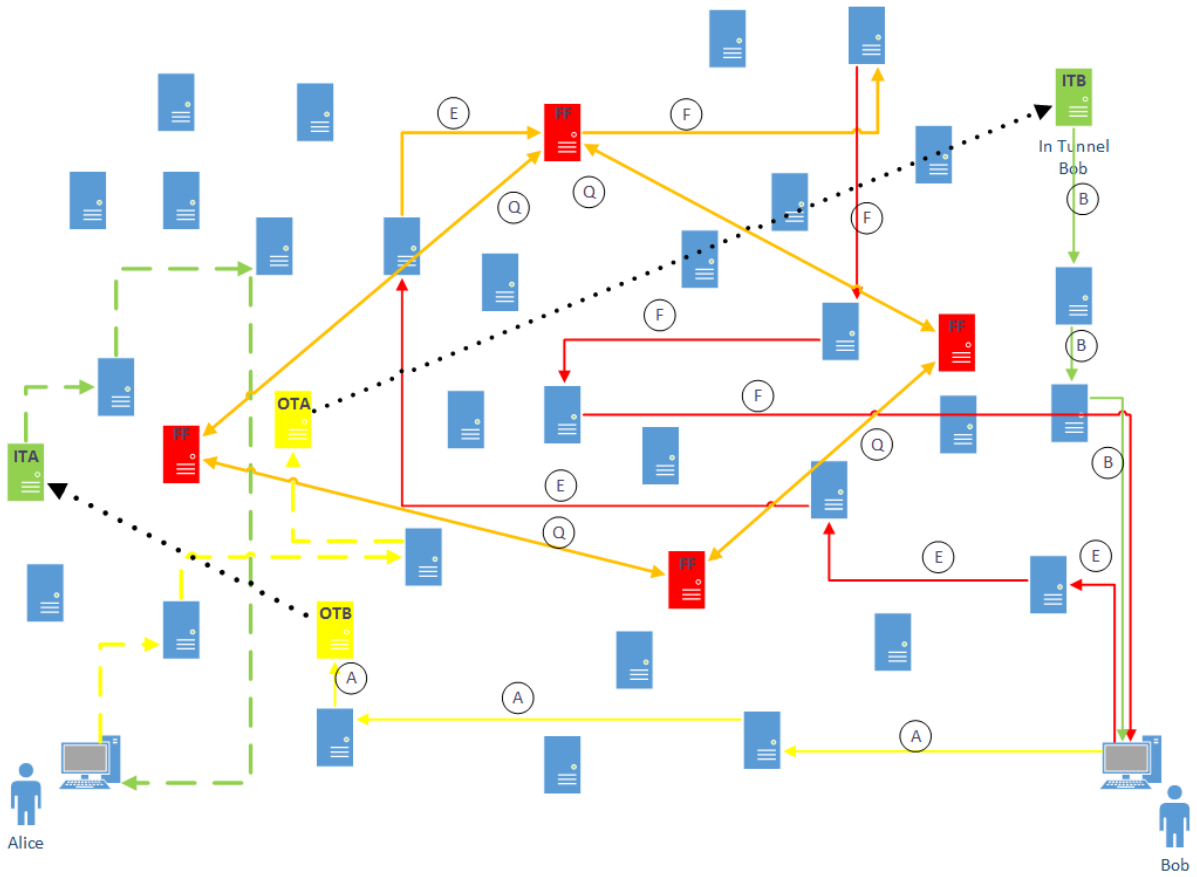

Figure 6 Basic I2P layout, starting communication between 2 nodes

When Bob wants to connect to Alice, she must have published a LeaseSet to the netDB. This LeaseSet contains the entry point from Alice's inbound tunnels. Bob must already know the destination he wants to connect to. This destination is a 516-byte crypto key and refers uniquely to Alice.

1 Bob contacts the netDB via his exploratory tunnel E, and he asks for the LeaseSet of the destination.

2 When the floodfill router does not have this information, it will redirect the searches to other floodfill peer routers (orange arrows Q).

3 When the LeaseSet is found, this information is returned to Bob through his exploratory tunnel F. The LeaseSet from Alice contains information about Alice's inbound tunnel (Inbound Tunnel Alice, ITA), the green I2P node name ITA.

4 The complete message is encrypted with the public key from the destination, in this case from Alice.

5 Bob will multiple encrypt the message with the keys from the nodes in his outbound tunnel.

6 The message that Bob sends is Garlic encrypted in such a way that only the endpoint of Bob's outbound tunnel knows that it must forward the message to the endpoint of Alice's inbound tunnel.

7 Each node in the tunnel removes one layer of encryption and so the endpoint has only the encrypted message and the entry-point (Inbound Tunnel from Alice, ITA) where to send it (the black dotted arrow).

8 The message is delivered from the outbound tunnel from Bob to the inbound tunnel from Alice.

9 Each node in the inbound tunnel from Alice adds a layer of encryption in such a way that only Alice can decrypt the message.
10 When the message is finally delivered to Alice, she can remove all the layers of encryption from her inbound tunnel nodes and then decrypt the message from Bob.
11 When a return message is needed, it goes by a complete different route through the nodes. Bob can add the entry-point of his inbound tunnels in the message, so that Alice can use that as a destination when she sends a return message through her own outbound tunnel.

This is also represented in the protocol flow diagram of Figure 7.

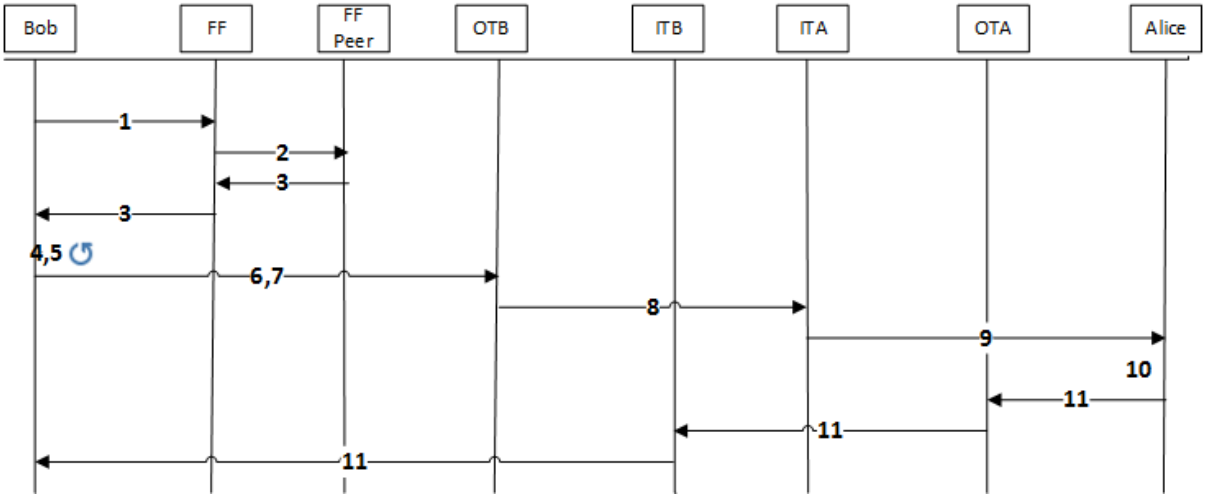

Figure 7 Protocol flow diagram of communication in I2P

Figure 8 is a simplified picture, depicting only the peer-to-peer communication between Alice and Bob. The tunnels are depicted as blocks, which consist of several nodes. When the communication has started, there is no need to contact the floodfill routers, so these are left out for simplicity. In reality, the tunnels are short-lived, so the nodes of Bob and Alice are regularly contacting the netDB for information about other nodes to build new tunnels. The simplified picture will be used as the basis for the explanation of how I2P can connect to the public internet, and during the presentation of our design enhancements.

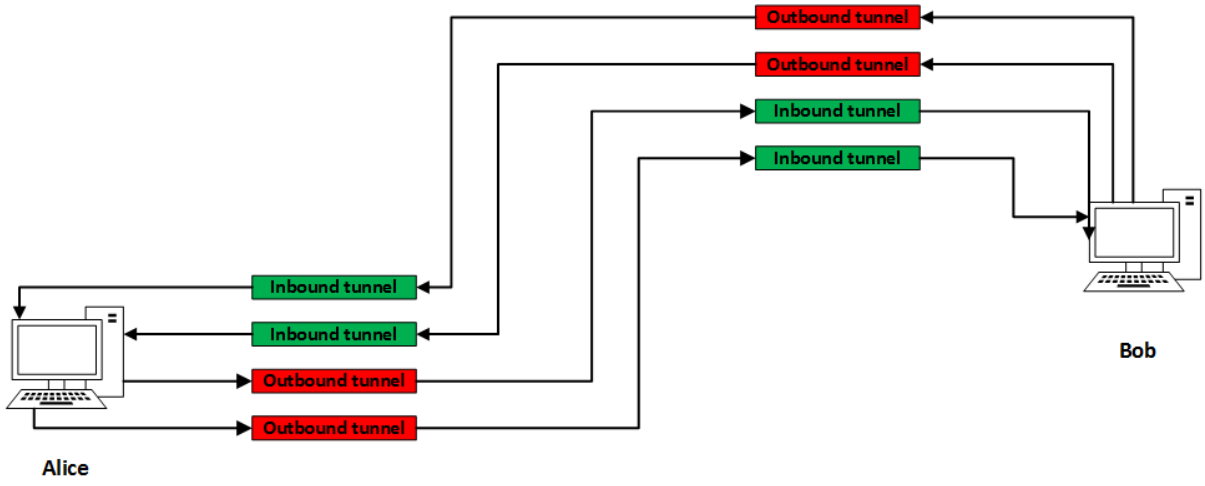

Figure 8 Simplified picture of I2P

2.2.2. I2P and access to the public Internet.

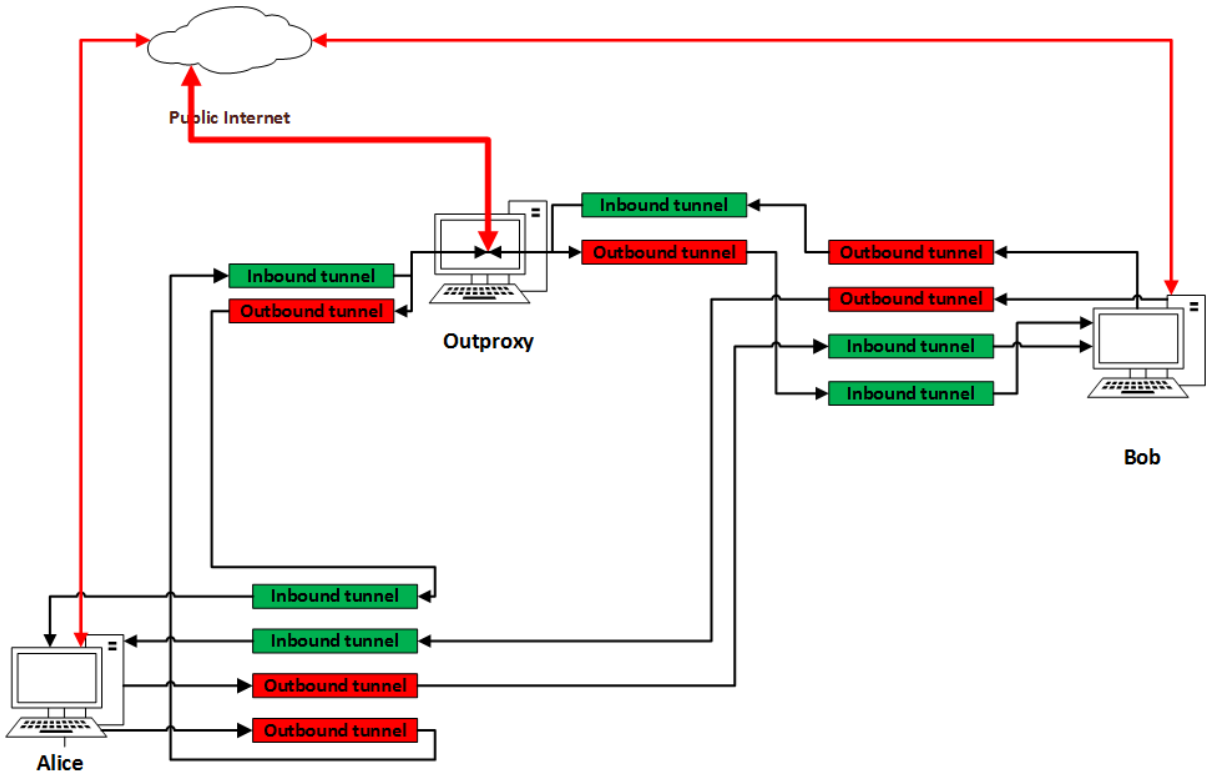

Figure 9. I2P basic layout, including traffic to public Internet

When Alice or Bob contacts the public Internet, all their network traffic is routed directly from their node to the service on the public Internet (the thin red arrows in Figure 9). There is absolutely no anonymity for Bob or Alice when they perform any communication on the Internet.

2.2.3. I2P outproxy functionality

I2P does have the concept of an outproxy, which makes contact to the public Internet possible.
The router software on the client must be configured so that it routes traffic, destined to the public Internet, to this outproxy, which then forwards the traffic to the public Internet, and reroute the return traffic to the client.
However, many users will use I2P for anonymous communication with each other and do not use I2P for accessing the public Internet. Therefore very few outproxies are available, and performance and reliability are low.

2.2.4. I2P and NAT

One problem which can exist with client nodes is the local firewall and network address translations that will happen in the user's router. This might mean that the I2P node is not

reachable from the Internet. I2P uses UPnP [34]to open up channels through the user's firewall and NAT to make the node reachable from the Internet, so most nodes can actually be reached from the internet.

2.3. Short comparison between I2P and Tor

As Tor is the most well-known anonymity network, we make a short comparison between I2P and Tor.
Both anonymity networks are low-latency overlay mix networks that run on top of the existing Internet. Both are aiming for complete anonymity of the users.
The main difference is that Tor is mainly used for enabling anonymous access to the public Internet, while I2P is aiming for moving existing services into the I2P network [35].
Despite these main differences, Tor also has its own Darknet capabilities and I2P has outproxy functionality.
Another important difference is the fact that Tor has a fixed infrastructure and the user connects to that infrastructure, while I2P has no fixed infrastructure, the infrastructure is composed of all the nodes using the network.
In the following table, we present some of the main other differences, concentrating on the working and implementation differences[15], [35], [22].

Table 1 Comparison between Tor and I2P.

I2P	Tor
Message based routing	Circuit based routing
Uni-directional tunnels	Bi-directional tunnels
Distributed network database	Centralized network database
Peer selection based on measurement	Peer selection based on reported values
Supports TCP and UDP	Supports only TCP
I2P-API	SOCKS
No differences between nodes.	Difference between entry-, exit-, and intermediate nodes.
	Centralized control reduces the complexity at each node and can efficiently address Sybil attacks
Fully distributed and self-organizing	
Essentially all peers participate in routing for others	

Although many features are not fundamental differences, they could be applied to both networks. E.g. Support for UDP could be built in in Tor, or I2P could start to support and use unidirectional tunnels.
But two differences are very fundamental, the message-based routing versus circuit based routing, and the centralized network database versus distributed network database.

Message based routing versus circuit based routing
Tor will build a separate circuit for each destination. So, starting the communication with a given destination needs some start-up time, time is needed for the circuit to get

established. I2P will pre-build tunnels and sent all network traffic through these outbound tunnels. So, starting a new communication is almost immediate.

Centralized versus distributed database.
Tor uses a central set of directory servers, which contain all the information about the available Tor routers on the network, while I2P distributes this knowledge over several floodfill servers. Each I2P node can act as a floodfill server, and more floodfill are started automatically when needed.
The central structure of Tor can lead to a lot of overhead traffic on the network, ultimately slowing down the user traffic [36].

3. User requirements and stakeholder analysis of an anonymity network.

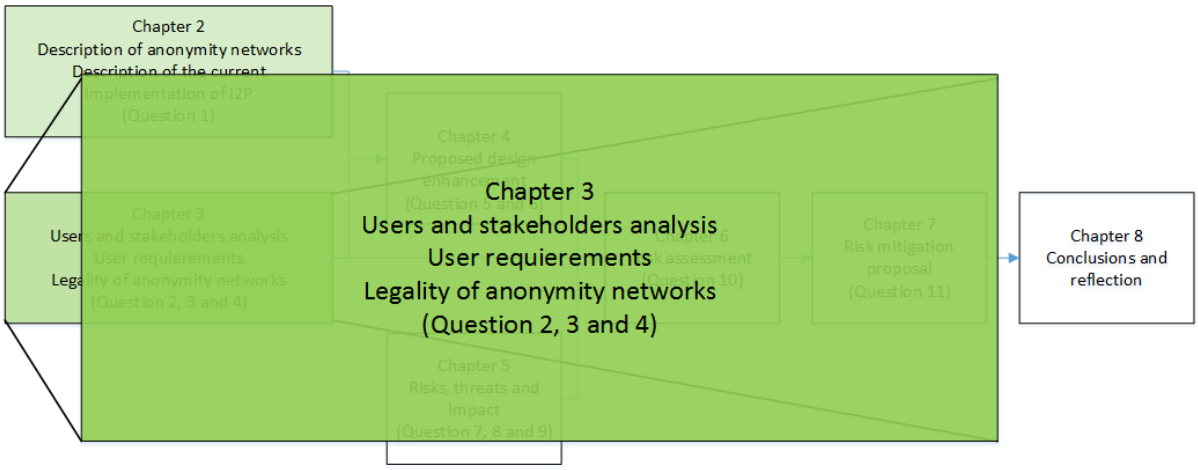

Figure 10 Guidance for chapter 3.

This chapter contains an inventory on the different stakeholders of anonymity networks. Each type of stakeholder is defined and a brief description is given about what his interests are. For the users, we also define the requirements they have. For each type of stakeholder, some typical examples are given. These stakeholders will be used in the risk assessment. Next, we focus on the activities that are performed within an anonymity network (ANNET). We then give a short description of the legal implications for the users of an ANNET. Followed by a short description of the differences and implications of an open ANNET versus a self-containing ANNET. At the end, we derive the requirements of the users. These requirements will be used to define an enhancement proposal (chapter 4), which can then be used as input for the risk assessment (chapters 5 and 6).

3.1. Stakeholder definitions

To our knowledge, only research has been done into some of the users, e.g. the Criminal and the Terrorist. (e.g. [37] [38] [39] [40]). Only one article was found about strategies to collect privacy data from consumers [41]. We therefore compiled the inventory from all kind of known and unknown sources, like common knowledge, brainstorm session, websites and newspaper articles, etc.

Later, we will assess the risks of the proposed enhancements. We are mainly concerned about the risks that involve the users of an ANNET. So, the users are the most important type of stakeholders. However, the user risks can be influenced by other stakeholders as well. Therefore an inventory of all stakeholders is made. The stakeholders are divided in two groups, the internal stakeholders and the external stakeholders.

- Internal stakeholders are those stakeholders that deploy activities to actively use, support, build and operate an ANNET, they can be referred to as “actors” because their acts on are done in the ANNET.
- The external stakeholders are those stakeholders that influence the environment around the ANNET. This can be done by legislation, but also by influencing the public opinion or influencing the legislative authorities.

The internal stakeholders can be divided into two subcategories, the users and the infrastructure deliverers.

- Users are all actors who actively use the anonymizing capabilities of the ANNET.
- Infrastructure deliverers are all actors who actively support the operation of an ANNET.

The “users” category can be divided again in three subcategories, the sincere users, the dishonest users and executive powers.

- Sincere users are those users who perform their activities within the actual law
- Dishonest users are those users who use anonymity to hide unlawful activities or try to break anonymity to abuse the results
- Executive powers are those users that try to break the anonymity of the users.

Internal Stakeholders		
	Users	
		Sincere users
		Dishonest users
		Executive powers
	Infrastructure deliverers	
External stakeholders		

Table 2 Overview of the stakeholder categories

A special remark must be given to the categories “Sincere users” and “Dishonest users” as we regard this from a western world perspective. Where freedom of speech is an important right to these societies, this is not generally accepted throughout the world. So, what is considered a fundamental right in the western world, might even be regarded criminal in other countries. So, the difference between these two groups is not clearly defined, because this is very dependent on the local laws and political viewpoints of a country.

In the following definitions, a stakeholder or an actor is a natural person or an organization. When computer programs are using the anonymity networks, they are initiated by a natural person and so they are considered as being an action of that natural person. Computer programs are thus not seen as separate stakeholders.

Each definition consists of a name, a short description, the needs and the requirements of the stakeholder and some examples of typical users.

3.1.1. Internal Stakeholders, users of the anonymity infrastructure

Actors who make use of the functionalities offered by the anonymity network infrastructure to keep their activities anonymous in order to protect their privacy.

Sincere user, actor whose activities are compliant with the law.
Needs and requirements:

- Anonymity on the network to guard his privacy

- Environment to communicate with anonymous people to gather information without endangering the source of the information.
- Platform for discussing and spreading his ideas without danger of being identified.
- Private and anonymous communication with other users.
- Software that is easy to install and operate and has a high level of security and anonymity.
- Anonymous access to all available information on the Internet.

Typical examples:

- Privacy aware citizen
    - Actor who wants to use the Internet anonymous to keep his anonymity and privacy.
- Journalist
    - Actor who needs privacy and anonymity for his journalistic tasks.
- Activist/Hacktivist
    - Actor striving for an immaterial goal, which is illegal in the country he lives.
- Whistle-blower
    - Actor who wants to publish about misbehaviour in his work.

Dishonest user, actors who use anonymity to hide unlawful activities or try to break anonymity to abuse the results.
Needs and requirements:

- Platform for buying or selling illegal goods without the danger of being identified and arrested.
- Platform for discussing and spreading his ideas without danger of being identified and arrested.
- Software that is easy to install and operate and which offers a high level of security and anonymity. Anonymous access to all available information on the Internet. Anonymous paying system.
- Low level of security and anonymity or back-doors that are only accessible by the actor himself.

Typical examples

- Criminal
    - Actor striving for material gain, in a way illegal in his country.
- Terrorist
    - Actor striving for an immaterial goal, willing to use violence to reach that goal.
- Disgruntled employee
    - Actor in conflict with his employer who is trying to threaten or damage his employer's assets.

Executive powers, actors who try to break anonymity of the users to fulfil their tasks.
Needs and requirements:

- Gather information about people that perform certain activities on the ANNET, like selling drugs, buying explosives or other illegal trading.
- Gather information about regime unfriendly activities.

- Low level of security and anonymity or back-doors that are only accessible by the executive powers.

Typical examples:

- Police
  - Law enforcement officers persecuting criminals.
- Contra-terrorism
  - Law enforcement, specialized in the fight against terrorists
- Intelligence services
  - Organizations that gather information about all kinds of people who might become a threat for society.

3.1.2. Internal stakeholders, infrastructure deliverers.

These are the actors who develop, build, run and research the building blocks that form the infrastructure of an anonymity network. Their main interest is to offer a stable, secure and anonymous service. It is likely that they also have the role of user, but now we focus on the development requirements.

Needs and requirements.

- Insight in all the code, knowledge on security and attacks.
- Public access to the code and the design decisions made during development, insight in attack scenarios and the mitigating measures taken by the developers.
- Legal base for offering these services.
- Stable and performant infrastructure and high-quality software.

Typical examples:

- Developer
  - Actor who works on developing and building the software used in an ANNET.
- Resource provider
  - Actor responsible for offering the resources needed for day-to-day operation.
- Operator
  - Actor responsible for maintenance and operational tasks needed for day-to-day operation.

3.1.3. External stakeholders

Governmental and private organizations whose acts influence the anonymity networks.

Needs and requirements:

- Laws forbidding the use of ANNET's and/or no laws protecting the privacy of their subjects.
- Low level of security and anonymity or back-doors that are only accessible by the executive powers.
- Low amount of traffic and no legal interference with their business.
- Legality of ANNET and low traffic overhead.
- Public and easy accessible ANNET's, open to all citizens; laws protecting the security and anonymity of the ANNET users. Software that is easy to install and operate and a high level of security and anonymity. Anonymous access to all available information on the Internet.

Typical examples

- Company on the public Internet visited by a user over ANNET

    - Any company collecting privacy sensitive information and where the collected user data plays an important role in the business model for the company, an ANNET might be a threat to their business model.
- Legislative powers with positive attitude towards ANNET
    - Government supporting the use of ANNET's to help their citizens to protect their privacy.
- Legislative and executive powers with negative attitude towards ANNET
    - Government opposing the use of ANNET's and thus striving to enhance law enforcement and to protect their citizens against criminals and terrorist attacks.
- Internet service providers (ISP's) and network operators
    - Organisations who offer Internet access and network transport to their customers.
- Internet freedom organisations
    - Organisations striving for digital rights on the Internet, like the EFF[11] and the EDRI[10].
- Researcher
    - Actor doing research into the security of the ANNET.

For defining the requirements, we only use the requirements of the internal stakeholders. For the external stakeholders with a positive attitude towards an ANNET, this will not be a problem, the external stakeholders with a negative attitude will not see their requirements.

3.2. User activities

We now consider the different activities that the users deploy.
We only consider the activities that take place within an ANNET, not the external activities that influence the ANNET.

Activities are defined as actions that actors perform on the ANNET, and that are dependent on the existence of the ANNET. So, all these actions make use of the anonymizing capabilities of the ANNET.

As the goal of the development of ANNET's was to make anonymous communication possible, the different forms of communication still form the basis of most activities. One form of communication is publishing information, so others can access the published information. The second form is direct communication between 2 parties. A third possibility is when activities are dependent on a third party, like with financial transactions. Based on this, the following activities are defined:

- Publishing information
    - Storing information on a node, where the content can be accessed by others.
- Accessing published information
    - Retrieving information which is stored on a node.
- Private communication
    - Communication between two or more actors in such a way that the senders and receivers stay anonymous to each other or to the outsiders who do not take part in the communication.
- Performing financial transactions

- Paying or receiving money, either in the form of official currency, or in the form of virtual crypto currency. The users that perform a financial transaction stay anonymous to each other, as well as to the third party that is involved.

We do not consider activities that are a result of ANNET activities. When an ANNET is used for buying or selling drugs, the exchange of information about the drugs and the financial transactions can take place in the ANNET, however, for delivering the goods, the seller and buyer have to revers to real-life activities as sending goods by post, which means that the buyer will need to drop some of his anonymity by defining an address on which he wants to receive the postal package.

We analysed which activities might be deployed by the actors, the results are shown in Table 3.

Table 3. Activities as performed by the internal stakeholders, per stakeholder

	Publishing information	Accessing information	Private communication	Processing Financial transaction
Privacy aware user	Average	Average	Always	Selden
Journalist	Often	Average	Always	Selden
Activist	Always	Often	Always	Selden
Whistle blower	Often	Selden	Often	Never
Criminal	Often	Average	Often	Always
Terrorist	Often	Average	Often	Often
Executive powers	Selden	Often	Never	Selden

In *Figure 11* we graphically show the kind of activities that are performed on the ANNET.

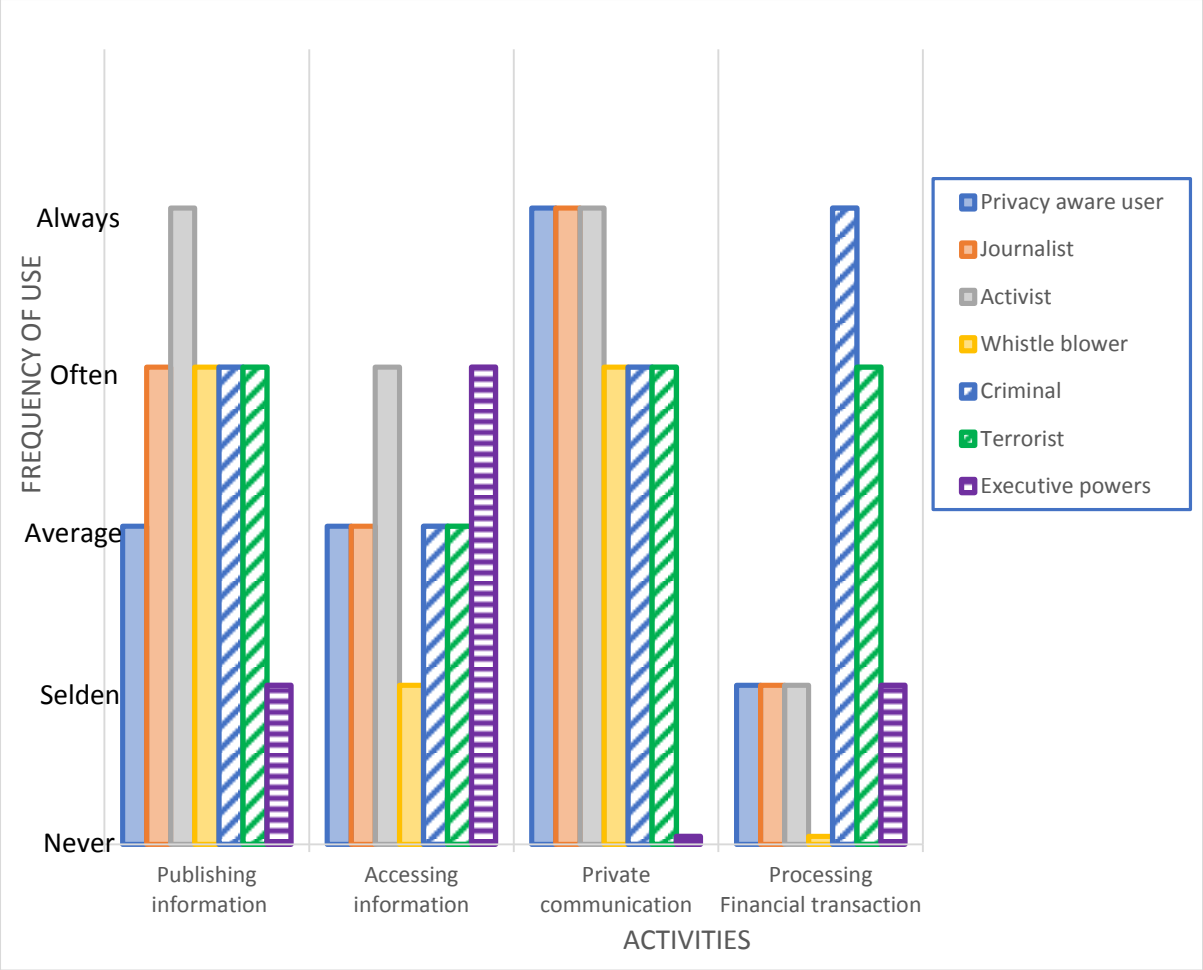

Figure 11 Activities on the anonymity networks, as performed by the users.

As can be seen, all activities are widely used by all kinds of users. There is no clear difference between users tending to perform illegal activities (like criminals or terrorists) and the users preforming legal activities (like journalists, privacy aware users or executive powers). The only exception is “performing financial transactions” as this activity is mainly used by Criminals and terrorists. In general, this leads to the conclusion that an ANNET offers the same anonymizing services to all users and no distinction can be made between legal and illegal activities.

3.3. Stakeholder legal implications.

The legality of the activities are depending on the local laws in a country[42]. Freedom of speech is considered a fundamental right in the western world, but can be limited in countries with a dictatorship. We realize that the borders between legal and illegal are not always clear but it influences the behaviour of internal and external stakeholders and therefore it is taken into account during our research. It also must be noted that the activities themselves are not illegal, but the illegality is depending on the kind of information involved.

There are two different aspects of the legal implications, which are treated separately, they are:

- Civil law
- Criminal Law

As every country has its own laws and its own interpretation of the law, it is impossible to make a complete overview that is valid for all humans and all countries. We focus on Europe and the USA.
The goal is not to give a full covering of all applicable laws in both continents but to develop a basic understanding of the possibilities and dangers for the users of an ANNET.

3.3.1. Civil law

Civil law handles disputes between civilians, either natural persons or organisations. The EU tries to harmonize the laws in different countries, and has two types of "EU law";

- A directive.
    - A directive defines what law must be implemented into national law of all the member states.
- A regulation.
    - A regulation functions as law, it is binding for all EU states.

For this research the important EU legal framework consists of the e-Commerce directive (Directive 2000/31 EU [43]) articles 12, 13, 14 and 15. They are part of "Chapter II: Principles" and then "Section 4: Liability of intermediary service providers"

Article 12 indemnifies the service provider, the directive states: "Member States shall ensure that the service provider is not liable for the information transmitted". Some conditions are given, but this is the core of this article.

Article 13 handles some requirements for caching. Article 14 handles some requirements about hosting and article 15 is about the fact that there shall be no obligation for monitoring network traffic.
The core of these articles state that an Internet provider cannot be held liable for the traffic he passes thru, he can store the information for technical purposes (caching) and is not allowed to alter the content of the information.

For the USA, the most important law for this research is the DMCA (Digital Millennium Copyright Act [44]).
This act also has a clause about the liability of service providers in "§512. Liability of service providers for online infringement of copyright", it states:
''(a) DIGITAL NETWORK COMMUNICATIONS. A service provider shall not be liable for monetary relief, or except as provided in subsection (i) for injunctive or other equitable relief, for infringement for the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or the intermediate and transient storage of such material in the course of such transmitting, routing or providing connections, if …"[44]
Then again it has some conditions, about caching that need to be fulfilled.

So, for the EU and the USA, the service provider is not liable for the traffic he passes through.

These laws are aimed at violations of civil law like copyright violations and trademark law. Information can be divided in two categories:

- Free information
    - This is all information which can be freely distributed and shared without infringement of any civil law.
- Protected information
    - This is all information which cannot be shared without infringing civil law.

This means that not the type of activity is determining whether civil laws are violated but the type of information involved. This is totally independent whether the information is shared anonymously or not, and whether it is shared on the public Internet or within an ANNET.

Contract with ISP

A contract between a person and an organisation is also covered by civil law. Any private person using Internet has a contract with his Internet provider. The Internet provider will usually hold the user liable for the Internet traffic that is sent through his host. The user indemnifies his Internet provider of any liability for the traffic that is passed through his Internet connection (see terms and conditions, e.g. Tele2 article 18 [45], T-mobile article 15[46], Frontier [47]).

Again, not the activities but the kind of information that is sent through the Internet connection can make the user vulnerable. The relating of Internet traffic in itself is legal, but when illegal content is relayed, it still might lead to problems. In such a case, it is up to the user to prove that he acts as a service provider to others, and that the illegal information is not sent by him personal. In fact, in such a case the ISP is no party in the dispute, but the police must first contact the ISP to ask who is behind a certain IP-address. If the ISP finds these requests annoying, he might end the contract with the user. (see for examples the Good and Bad ISP's list from Tor[48].

Network operators

A network operator also has contracts, covered by civil law, with many organisations to handle the network traffic for those organisations. Some of these network operators treat exit-node traffic from a Tor exit-node differently, with a lower priority or maybe even discard it all the way [49]. Some of these treatments are specifically aimed at Tor traffic. This suggests that I2P traffic might face these treatments as well. Although for the EU the directive states that no modification of the content is allowed, dropping network traffic is not seen as modification of the content.

3.3.2. Criminal law

Criminal law handles punishment of criminal offenses. Criminal offenses need to be defined on forehand.

As with civil law, this means that not the activities in itself are illegal. For criminal law the important factor is whether the information that is exchanged has a relation to a punishable offense. Offering stolen goods is a criminal offense, offering a copy of a copyrighted movie is

not a criminal offense, as this is covered by civil law and it is not stated as a crime in criminal law.
The production, possession and exchanging of child porn is (in most countries) a criminal offense.

During a police investigation into a criminal offense, law enforcement can have the right to confiscate equipment to search for evidence. Even if civil law states that a service provider is not liable, during a criminal investigation the service provider is obliged to hand over all information to law enforcement officers.

There is the possibility that some traffic has passed through an outproxy that is possibly illegal. During a criminal investigation, it is possible that the IP-address of the outproxy is found to be suspect. It is possible that police officers will request more information or treat the owner of the outproxy as a suspect. According to the Tor legal FAQ[50] it is not advised to run exit-nodes at home, and the user might even take the risk that law enforcement seizes the computer of the user.
Although the owner of the outproxy has not been part of any illegal activity, it might be difficult to explain this to the law enforcement officers. The Tor website has some templates to answer these kind of requests[51].
As the I2P node does not log anything about the traffic on disk or in memory, there is no information that can be handed over to the police.
Tapping is not possible as no-one knows which traffic should be tapped, and tapping orders can only be given if specified which user must be tapped. Although there is a tendency by governments to tap all network traffic and then filter out what can be interesting for their purposes [7].

3.3.3. Conclusions for stakeholder “users”

Although for a lot of countries in Europe and the USA it is not illegal to relay network traffic, and thus to run I2P with outproxy functionality, it is still possible that users are afraid for the possibility that someday law enforcement comes to them and demand information about network traffic that has passed through their proxy. The Tor legal FAQ advises users not to run an exit node at home for this reason[50]. This could lead to users unwilling to run the I2P software if the outproxy functionality is compulsory.

3.4. Open or self-containing ANNET.

The last aspect we consider, is related with the two fundamentally different aspects of ANNET’s:

- the self-containing ANNET
    - Within a self-containing ANNET, all information that is exchanged stays within the ANNET, e.g. the Freenet.
- the open ANNET.
    - An open ANNET makes it possible to exchange information with the public Internet, e.g. Tor.

This means that all activities have a self-contained and an open version. Publishing information can be self-contained, e.g. the information is placed on a server within the ANNET, or it can be open, and the information is anonymously published on the public Internet.

Most ANNET's does in fact have both aspects at the same time. The self-containing ANNET is mostly referred to by terms like Darkweb or Darknet. Services can be offered within the Tor network, by using the .onion addresses, I2P has this same functionality, using .I2P addresses. But also, Tor has exit-nodes which makes it possible to access the public Internet, while I2P has the outproxy functionality.

Despite the fundamental difference between an open ANNET and a self-contained ANNET, we do not see how this influences the behaviour of the users, for anonymously publishing information he must use the self-containing part of the ANNET, for all other activities it does not make any difference whether he uses the self-containing part or the open part of the ANNET, provided that his anonymity is guaranteed.
This aspect will therefore not be considered in this thesis.

3.5. Design requirements

We now explain which design requirements, considering the usability, anonymity and security aspects, we derive from the analysis of the stakeholders and their activities. We will need these requirements to make a global design of the proposed enhancement of I2P.

Before we define the requirements, we state the conditions for the design:

- We only consider the requirements of the internal stakeholders, the users.
- We only consider requirements for legality, anonymity and security.
- If requirements conflict with each other, we choose the most secure requirement to get an optimal anonymity for the user.
- We focus on the USA and EU, but will adapt to other continents if possible.

Starting point: All nodes will be configured to act as an outproxy. The outproxy functionality is based on the existing tunnel concept in I2P.
This starting point leads to several implications for security, anonymity and legality. We will explain the implications and then explain how these lead to design requirements.

3.5.1. Security Implications.

- Outproxy traffic can leave the ANNET in another country.
  Because of differences in Law, legal traffic might become illegal.
  - Some content might be legal in the country of the user, but could use an outproxy in a country where that content is illegal, thus "illegalizing" the content.

  Functionality depending on the GEO location might fail.
  - Some services are dependent on the GEO location of the client, e.g. some service that serves copyrighted material.

  Requirement 1: GEO location of outproxy must be specifiable by user.
  - At this moment, the endpoint of a tunnel is not aware of the GEO location of the node, so this must be added to the tunnel building routines. Also, the LeaseSet specification has no place for adding such information[52]. There is a proposal for an extension of the LeaseSet[53], but this is not

implemented yet. However, adding extra information about location might lower security because finding the original IP address belonging to an end-point is made easier when less IP-addresses must be reviewed.
So, this requirement will not be fulfilled.

- NetDB will become much larger
    - As all nodes will build and use extra tunnels for the outproxy, much more information needs to be published in the NetDB and more netDB lookups are expected, this might hinder the performance of I2P. At this moment there are about 17.000 LeaseSet's published, adding 50.000 extra LeaseSet's will probably have an enormous impact on the performance of the floodfill routers[52].

Requirement 2: Raise the number of floodfill servers.

- Security and anonymity are best served when as much as possible outproxy nodes exist, as this makes eavesdropping much harder.
    - When all nodes are used for outproxy functionality, this results in the lowest chance of eavesdropping and traffic analysis.
    - On the opposite, when a small number of outproxy nodes are configured, the mixing on network streams is higher, which makes traffic analysis harder.
    - The lead-developer of I2P states that a number between several hundred and several thousand outproxies would be sufficient[52]. When we compare this to Tor, at this moment, (Jan 2018), Tor is running with about 9000 relays and bridges, serving around 4 million users[21], which equates very roughly to about 400 users per relay. Comparing this to I2P with 50.000 users, I2P could handle this with 125 outproxy nodes.

Requirement 3: Enough nodes must be available for the outproxy functionality.

3.5.2. Anonymity Implications.

- Network traffic can contain identifiable information.
    - The network traffic can contain information which can be used to identify the user, e.g. SMTP will send the actual IP-address of the client to the server.

Requirement 4: split computer and I2P node virtually so the IP-address of the client node does not reveal any information about the user.

    - Some software, like JavaScript or Java, can access information on the disk of the user's computer and send this information to a service.

Non-I2P requirement: User must carefully select his client software.
Alternative: Blocking such software from running on the node.
Alternative: Deep packet inspection of the network traffic and removal of anonymity sensitive data, like IP-addresses (network scrubbing).

- A mix between public Internet traffic and outproxy traffic might lead to easier de-anonymization.
    - When a user is using his Internet connection for accessing the public Internet via I2P and at the same time this Internet connection can be used for direct

access to the Internet by the same node, it can be possible to trick the user into access to a website via his public Internet connection, thus breaking anonymity.

Requirement 5: All network traffic from a user node must be relayed by I2P.

3.5.3. Legal implications.

- In some countries, running an outproxy is illegal for users.
    - Especially in countries with an oppressive regime, running the outproxy functionality can be dangerous for the users.

Requirement 6: The outproxy functionality must be optional.

But with an optional outproxy functionality, users can make extensive use of other outproxy functionality without contributing to the I2P network and thus consume more resources than they share, this behaviour is known as free-riding or leeching.

Requirement 7: Anti-free-riding measures must be taken when outproxy functionality can be switched off.

- Law enforcement might become interested in certain outproxy nodes.
    - When the node from a user has been the end-point from where illegal activities entered the Internet, the user might be accused of having performed those activities himself.

Requirement 8: To reduce the risk for the user, each outproxy must only use encrypted connections to the Internet. Thus, lowering the chances that law enforcement can read the network traffic leaving the I2P network.

Requirement 9: Outproxy policies need to be defined, stating the protocols and ports that can be used[52].

Legal alternative: Supply each user with a solid legal document, tuned for his country, with an explanation about the working of I2P.

Table 4 User requirements for I2P enhanced outproxy functionality

Requirement	
1	~~GEO location of outproxy must be specifiable by user~~(Dropped)
2	Raise the number of floodfill servers
3	Enough nodes must be available for the outproxy functionality
4	Split computer and I2P node virtually
5	All network traffic from a user node must be relayed by I2P
6	The outproxy functionality must be optional
7	Anti-free-riding measures must be taken
8	Each outproxy must only use encrypted connections to the Internet
9	Outproxy policies need to be defined

4. Chapter 4 Proposed design enhancement

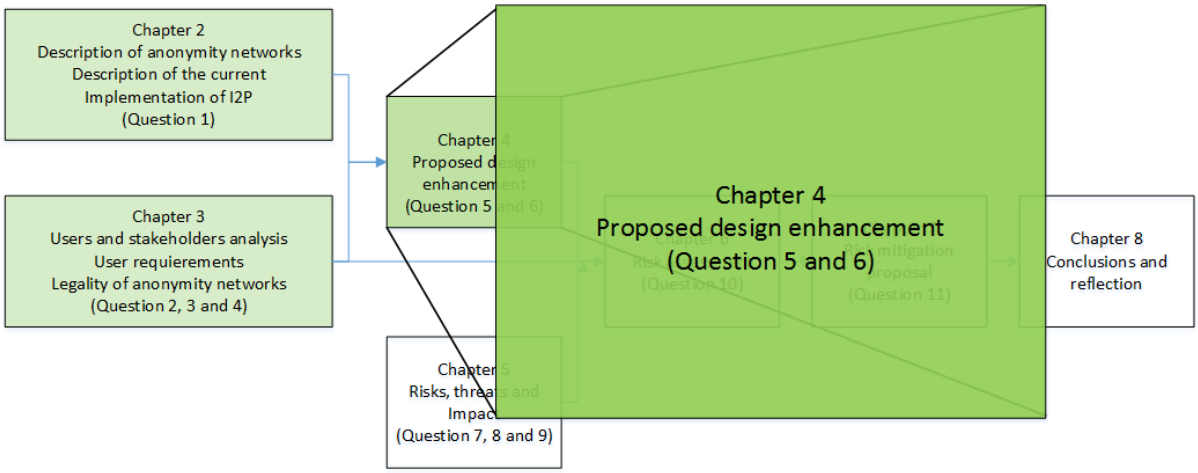

Figure 12 Guidance for chapter 4.

In this chapter, we present how the current I2P design needs to be modified to fulfil the user requirements we derived in chapter 3. It is presented in two steps. We need this global design for the risk assessment, it is not fully developed as that is not the goal of this thesis. At the end of this chapter we shall check whether all requirements are met.

4.1. Proposal for general outproxy design

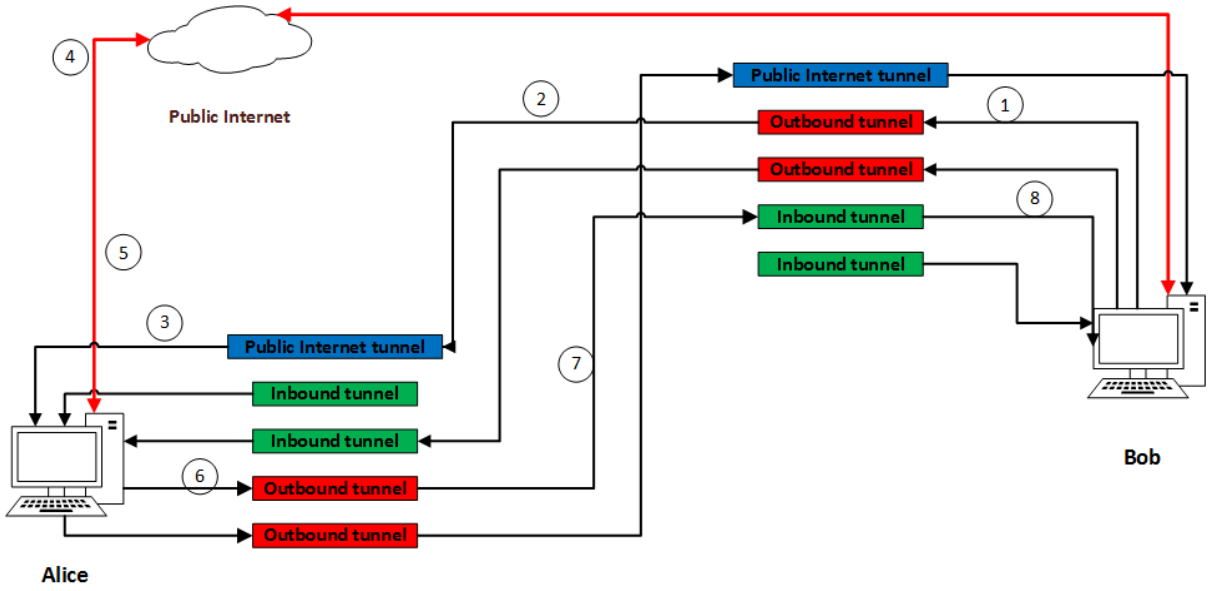

Figure 13 I2P enhancement using public Internet tunnels

Figure 13 shows the first part of the proposed design modification.
Every node not only starts an inbound and an outbound tunnel, but also a public Internet tunnel which is only inbound, in the same way as the other inbound and outbound tunnels are defined.
It then publishes a LeaseSet with the information about this public Internet tunnel to the netDB. The current LeaseSet specifications contain no specifications for this case, so an

extension to the LeaseSet specifications must be defined and implemented. Also, when proxy policies are defined for an outproxy (requirement 9), these policies must be specified in the LeaseSet, and LeaseSet's must be searchable for these policies.
For example, when a user wants to send anonymous mails, he needs an outproxy which is willing to relay mails. So, he needs to search for an outproxy which is allowing SMTP traffic on port 25.
We think that a limitation on the possible outproxy policies is needed, to prevent huge numbers of different policies. But now we get the problem that a user might want to use several different applications, connecting to the public Internet. There are two fundamentally different solutions for this:

- The I2P node asks for each different application a dedicated public Internet tunnel, and routes the network traffic for each application to the corresponding public Internet tunnel; or
- The I2P node queries the netDB for a LeaseSet which contain all the necessary policies for the applications the user wants to us.

The first solution will need an extra capability inside the I2P software, to route all the network traffic to the correct tunnel, the second solution is easier for the I2P node, but might lead to a very limited set of outproxy routers that fulfil the needed policies. This could in turn lead to a very limited subset of outproxies which are actually used. Given the complexity of the first solution, we think that each I2P node needs to select an outproxy that satisfies all requested policies. We think that, with a careful definition of the policies, the number of outproxy routers that fulfil a policy will be high enough.
This means that the way the netDB answers queries has to be changed. In the current situation, the netDB is queries for a LeaseSet, based on a unique ID of the destination. Querying the netDB on a totally different attribute (e.g. a public Internet policy) is not logically. We suggest that via a predefined algorithm the needed policies are calculated into an ID. This ID will then be used by the I2P node to query the netDB. This ID is not unique, it serves only as a search key to find a LeaseSet for a router that supports the requested public Internet policies.
The LeaseSet for a public Internet outproxy must be treated equal to the LeaseSet's from internal I2P services, the I2P node itself is responsible for querying the netDB for a new LeaseSet when the old one expires.

When Bob wants to anonymously access the public Internet, he asks the netDB for the endpoint of any public Internet tunnel, based on the required policy. The netDB must answer with one or more LeaseSet's from routers that support the requested outproxy policy. The given LeaseSet's must be randomly chosen from the available LeaseSet's on the floodfill router. After a suitable LeaseSet has been received by the I2P node, the communication can start.
These steps are also numbered in Figure 13.

1. Bob then sends a message to his outbound tunnel.
2. That message is sent from the endpoint of his outbound tunnel to the entry-point of the public Internet tunnel, using the information that he received from the netDB.
3. The I2P node whose Internet tunnel is used, receives the message.
4. That I2P node must sent the request to the public Internet. The message from Bob also contains the entry-point of his own inbound tunnel
5. The I2P node receives an answer from the Public Internet.

6. The I2P node send this message to his own outbound tunnel.
7. The message is sent to the inbound tunnel from Bob.
8. The message arrives at Bob's computer. So, Bob's access to the Internet was anonymous.

This can be enhanced by three extra possibilities:

- To reduce the risk on eavesdropping the public Internet connection, we could design the new functionality in such a way that always several public Internet tunnels are used during an Internet session where some kind of round-robin selection decides which tunnel is used for any network session.
- The second option is to reduce the risk for the user of being accused of being part of illegal organisations, based on the fact that some illegal activity was performed through his outproxy. This risk can be mitigated by only passing encrypted traffic to the public Internet. This must then be specified in the LeaseSet for the outproxy.
- The third enhancement is to make the outproxy functionality optional, this meets requirement 6. This to protect users in repressive regime countries where it might be dangerous to relay the "wrong kind of traffic". This introduces the possibility of free-riding, people switching off their outproxy and thus declining the use of their resources to the network, but consuming other user's resources for their own benefit.

Other possibilities that we do not take into account, are:

- An option is not to use every node as an outproxy, but simply adding dedicated outproxies as is used by Tor, with its dedicated exit-nodes. At this moment I2P has a few of these dedicated outproxies. However, the I2P network will then consist of a fluid infrastructure, combined with a small fixed infrastructure, and could be more vulnerable to traffic analysis attacks, based on this. We can also think about a solution where outproxies are added and removed again, based on the actual usage. Like the floodfill routers which are also dynamically added and removed.
- An already existing option is to relay the public Internet traffic into Tor with an application called "Orchid"[54]. This reduces the risk for users as the network traffic is not directly sent to the public Internet. Orchid acts as a proxy and opens a SOCKS5 port on the local node. Traffic sent to this proxy will be sent through to the Tor network. But now the network traffic is routed over I2P and routed over Tor, this might lead to more attack planes for an adversary and is not automatically more anonymous than routing over one anonymity network. This solution needs the functionality of outproxies connecting to Tor in the same way as connecting directly to the Internet. So, the advantages of this solution are limited, while latency might become problematic as all the network traffic is first routed over I2P and then through Tor.

However, in this new situation two problems still exist:

- Bob can still (accidently) bypass the I2P tunnels and setup a direct communication with a public Internet service, thereby revealing privacy related information, e.g. his IP-address.

- Several protocols, such as SMTP, send the IP-address of Bob in the request, thus de-anonymizing Bob. Also, tracking software on a public Internet site might try to discover the IP-address or other privacy related information from Bob.

We enhance the proposed design, such that the two, still existing problems, will be solved.

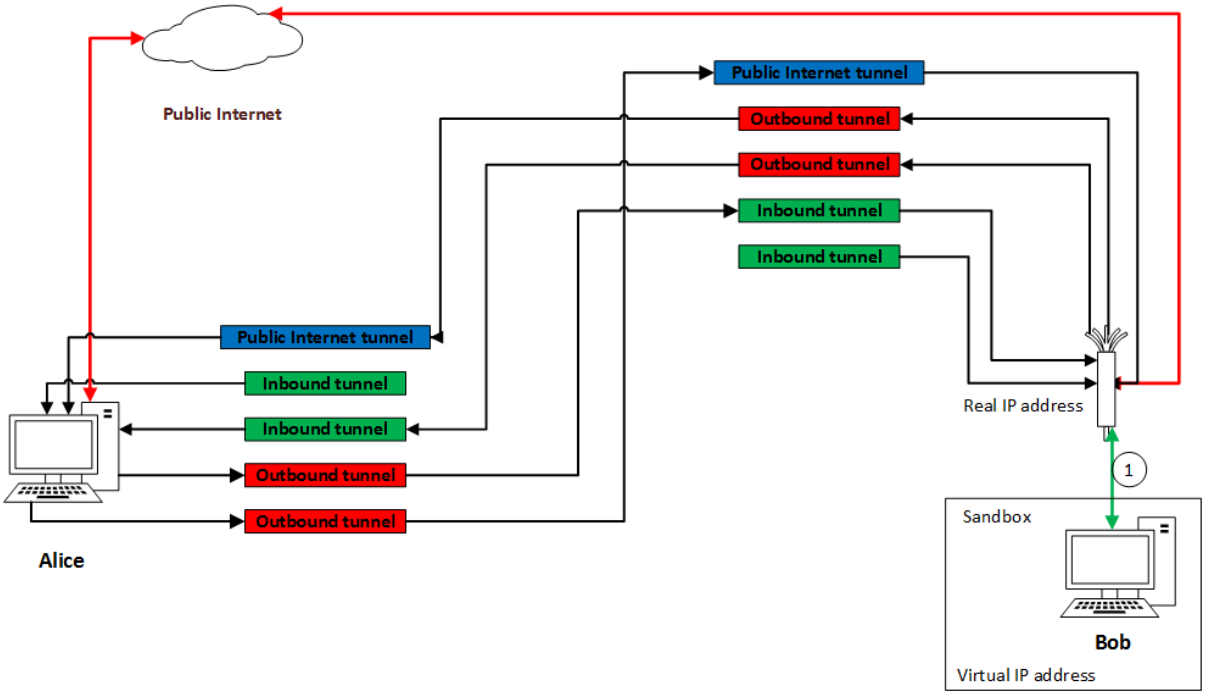

Figure 14 I2P layout with public Internet tunnels and network separation

The solution for the IP-address leakage can be found in creating a virtual I2P node running on the actual node. (this is also hinted at by B. Zantout [31]).
When it is arranged that only the I2P software can connect to the Internet, and the "computer" cannot connect to the Internet anymore but can only connect to the I2P software via the connection noted as 1 in Figure 14, the "computer" can then use a virtual IP-address. Because the computer is running in a "disconnected" and protected mode, this method is commonly known as sandboxing. When the computer is given a private network IP-address (e.g. from the 192.168.0.0 range) that is shared with many other I2P nodes, the practical value for recovering the IP-address is useless.
This solves the problem with leaking IP-addresses by other software, as well as problems that some software tries to bypass proxies. It might also be possible to use a sandbox system based on compartmentalization[55], like Qubes OS[56].
Still, some protocols might leak privacy sensitive data, and some software is able to access information on the disk or in memory. More research is needed to analyse whether this solution enlarges the risk of de-anonymizing by analysing metadata.
With this solution, there is always the risk that an application is able to break the sandbox and contact the public Internet because there must be some connection possible for the I2P software.
Another, maybe even better, solution would be to use a small dedicated node, running the I2P software which functions as a router/proxy combination between the actual

computer and the local Internet access point, e.g. use a raspberry PI or a dedicated router for that purpose. In that case there is no possibility to break out of the sandbox.

4.2. Requirements completeness analysis

Some requirements are not incorporated in this design, because they have no impact on the risk assessment we perform. An overview of these requirements is given here:

- This design is missing a solution to prevent free-riding. The problem of free-riding is already existent in I2P (but not a major issue[52]). It is partly countered by maintaining peer-profiles but it is possible that it becomes larger when these enhancements have been implemented. When a solution can be built, based on these peer-profiles, it will probably not have a large impact on the security.
- The tunnel building methods need to be adapted to use more nodes for Internet access tunnels. At this moment, the tunnels nodes are selected from the fast peers around a node. But that needs to be changed to use many more nodes as an outproxy node. This ensures that statistical analysis is made much harder for any adversary.
- The number of floodfill routers must be raised. As every node is starting a public Internet tunnel, every node is also publishing a LeaseSet to the netDB. So, the netDB traffic becomes heavier, the netDB larger so more floodfill routers are needed. As the number of active floodfill routers is determined by the automatic opt-in rules of I2P, these rules have to be adapted so that the number of floodfill routers will be raised. The current opt-in rules lead to about 6% of the routers that act as a floodfill.

We realise that many more problems will have to be solved when the design is completed. This design proposal is quite global and can only be used as input for the risk assessment, it is not developed far enough to start implementing.
We have tried to specify as much of the design as is needed for the risk assessment.

5. Risks, threats and impact

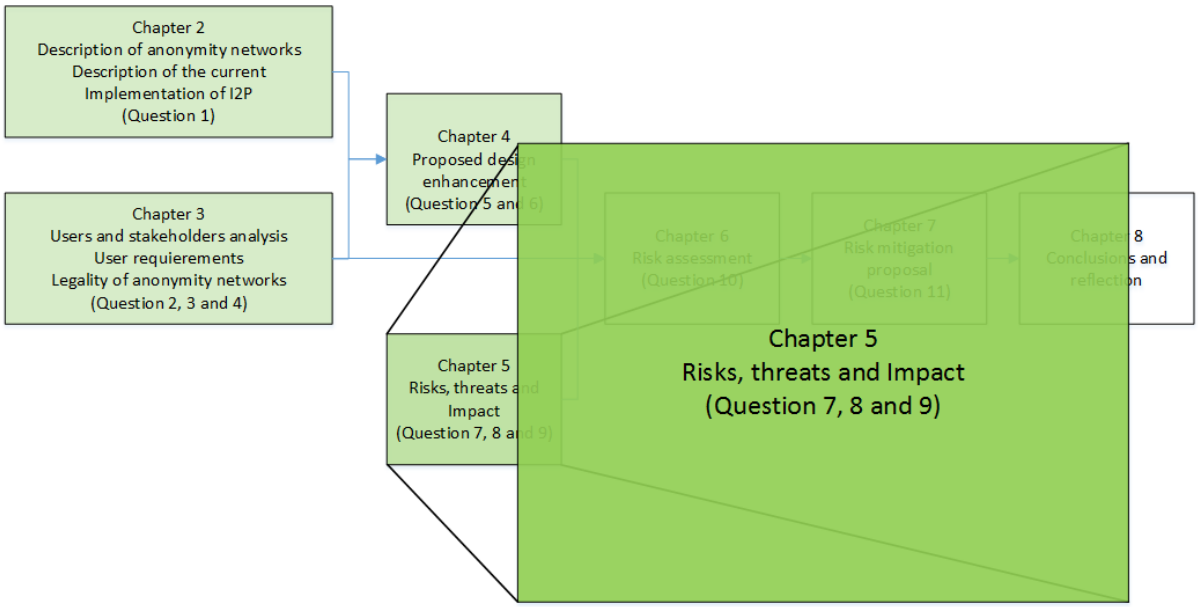

Figure 15 Guidance for chapter 5.

In this chapter, we start with describing the threat actor capability model, threat actors, impact model and a new threat classification model. Then we present an inventory of the different known attack methods (threats) that can be applied to anonymity networks. The I2P website[15] describes many of these attacks. Although the I2P website, and the literature concentrates on the technical attack scenario's, we also present a short inventory of non-technical attacks. After that we continue this chapter with an inventory of new possible attacks that are introduced by the design enhancements we presented in chapter 4.
We conclude this chapter with an impact analysis for the different risks.
With the results of this chapter, we have a complete overview about the threats that we will use as input for the risk assessment in chapter 6.

5.1. Threat actor capability model

As a first step, we are interested in the capabilities of the adversary. We define the technical threat actor capability model ,close to the threat model of Dingledine et al.[57] as follows:

In the technical threat actor capability model, we assume an adversary:

- who can observe some, but not all, network traffic.
- who has knowledge of the infrastructure
- who can generate, modify, delete, or delay traffic
- who can run his own controlled nodes, with a maximum of 20% of the nodes[58]

We also impose some limits on the capabilities of the adversary:

- He cannot correlate packets based on content as the contents are encrypted[59]
- He cannot correlate packets based on size, as packet padding is used[59]
- He cannot break the encryption[58]

This threat model is specifically designed for identifying technical vulnerabilities. The model considers only intentional human threats and not any natural disasters. It concentrates on the capabilities of the adversary which forms the fundament of the different threats that the adversary can deploy. So, the actual threats (attacks) describe how the adversary can use his capabilities to reach his goals.

However, there are also threats originating outside the technical environment, the non-technical threats. To our knowledge, no research has been done into this subject.

For the non-technical threat actor capability model, we assume an adversary:

- who can influence the legislative powers
- who can influence the executive powers
- who can influence the media
- who can influence large companies and their behaviour

Some researchers extend the threat actor capability model with a global adversary[59], while others state that there is no defence possible by any low-latency anonymity network against a global passive adversary[60].

5.2. Threat actors

Threat actors are the persons or organisations that execute the threats. They can be very diverse and might execute the same threats but for different reasons. Any stakeholder can act as a threat actor. In the risk assessment phase, we will add information about the threat actors.

5.3. Impact model

We now have defined what capabilities the adversaries have. As a next step, we must define what their goal is, and thus what the impact is for the users.
Some literature describes the goal of the adversary, but it is often limited and tuned for specific purposes [59], [60].
For our research, as we are interested in the impact on anonymity and privacy of the users of I2P, we limit our scope to unavailability impact and de-anonymization impact.
we define the following impacts:

- Service unavailability impact, the unavailability of services in the I2P network
- Network unavailability impact, the unavailability of the complete I2P network, thus including the service unavailability impact.
- Service de-anonymization impact, the de-anonymization of services on the I2P network
- User de-anonymization impact, the de-anonymization of users on the I2P network

5.4. Threat classification

As we now have some knowledge about threat actors, their capabilities and their goals, we will look into the methods they can employ to reach their goal.
These methods are commonly referred to as threats. We only consider intentional threats, these are also known as attacks.

We make a classification of threats, based on their goals and their methods.
Our first division defines four groups, based on their goal. They correspond with the earlier defined risks:

- Service unavailability attacks, aimed at a specific service
- Network unavailability attacks, aimed at the complete network
- Service de-anonymization attacks, aimed at the services running on the ANNET
- User de-anonymization attacks, aimed at the users of the ANNET

5.4.1. Unavailability attacks

Goal of these attacks is to render services or the network unavailable to the users. Besides the already defined Service unavailability attacks and the network unavailability attacks we see a third option, the legal existence attacks. So, we define three groups of unavailability attacks:

- Service unavailability attacks, aimed at a specific service
- Network unavailability attacks, aimed at the complete network
- Legal existence attacks, these attacks are aimed at the legality of the existence and the operation of the ANNET. An example is a law to forbid the use of an ANNET.

5.4.2. De-anonymization attacks

Goal of these kind of attacks is to break anonymity of the users or services. It might be aimed at developing a way to break anonymity for all users or it might be targeted at specific users or services.

These attacks can be used to de-anonymize both users and services. So, we make a distinction based on the methods that are used.
We define 7 groups of de-anonymization attacks:

- Traffic analysis attacks, any attack based on following and analysing the network traffic
- Sybil attacks, any attack based on the usage of many nodes owned by the attacker
- Application attacks, abuse the applications to gather extra information, like using JavaScript, cookies or protocols
- Metadata attacks, any attack based on searching, collecting and analysing metadata
- Central infrastructure attacks, any attack aimed at the central infrastructure of the running anonymity network
- Harvesting attacks, any attack aimed at collecting and analysing data about the running nodes in the network
- Out-of-band attacks, these attacks are not aimed at the running anonymity network, but try to attack in a complete different way, circumventing the running anonymity software. These attacks are not specific for I2P or any other ANNET. Example is trying to insert rogue code in the development tree[61].

For this thesis, we also define a group, “New attacks”, for we don’t know yet what new attacks can be introduced by our proposed design enhancement.

We now present an overview of all the identified attacks. In the next chapter, we will use this overview to make a risk assessment for each of these groups of attacks, as well as for the newly introduced attacks.

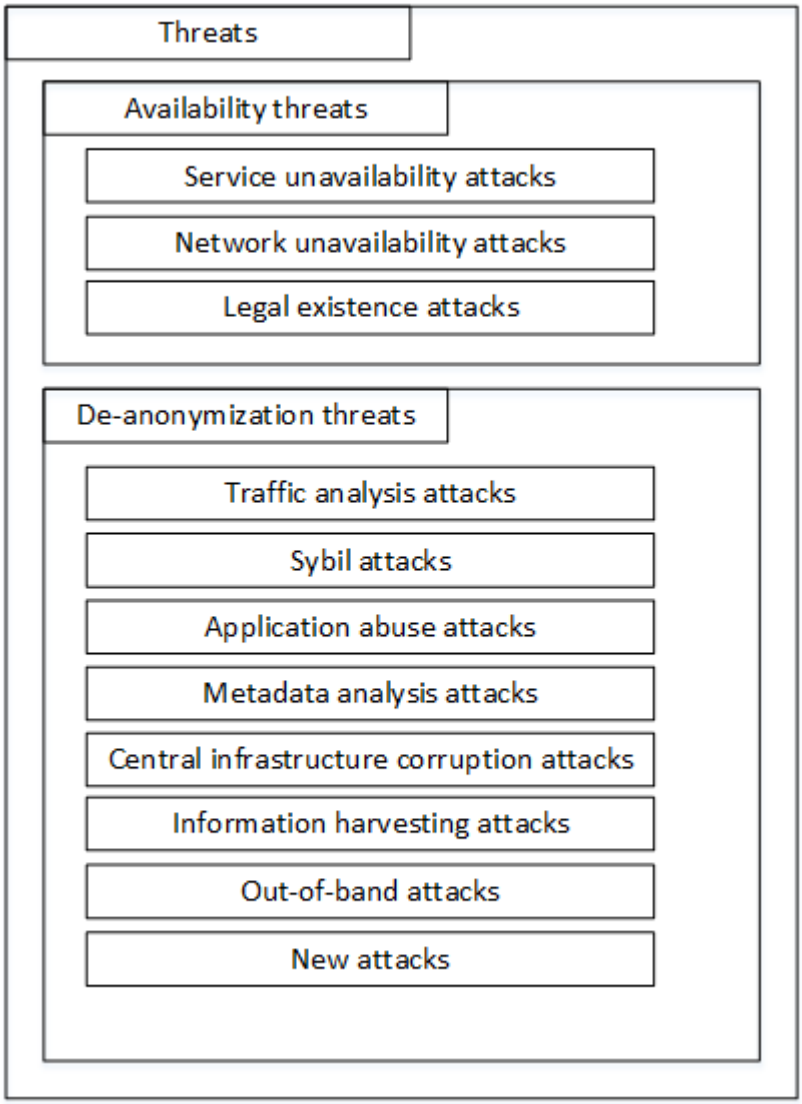

Figure 16 Overview of the attack groups

5.5. Unavailability attacks

This family of attacks are all aimed at the availability of the ANNET, or parts thereof. They are not interested in de-anonymizing, but at hindering or preventing the use of an ANNET.

5.5.1. Service unavailability attacks

These attacks are directed at a specific service. It could be used by states or activists to make unwanted services inoperable, e.g. a criminal market type of service. They can be divided into three types of attack, based on the used method.

- Flooding attack
  - This attack tries to make a destination, a tunnel or a node inoperable by sending a massive amount of information. I2P has no defences against this kind of attack. Although after a tunnel is blocked, it will detect this and build a new tunnel, but that can then be flooded too.
  - This attack can be used in combination with Sybil attacks to aid de-anonymization attacks [32], [58].
- CPU load attack
  - This attack is based on the possibility to make a node perform extensive cryptographic operations, and thereby exhausting the CPU of the node. This can be mitigated by good engineering and coding practises.
- Eclipse attack
  - This attack is based on a Sybil attack. Goal is to surround a target with servers owned by the adversary. These servers can then block all traffic to and from the target, eclipsing the target from the network [62], [58], [63], [32].

5.5.2. Network unavailability attacks

In general, these attacks are used by an adversary which opposes the use on an ANNET. The goal is to make the ANNET inoperable. This might be to force users to leave the ANNET and make them vulnerable again for profiling, or to lure users to another solution, which protects the anonymity of the users not as well.

- Greedy user attack
  - This attack consists of people trying to consume much more resources than they will attribute to the network, in P2P networks they are commonly referred to as “free-riders”. As such, it is not really meant as a DoS attack, as the users want to be able to use the network for their own purposes, and not to disable the network. However, too many of these “free-riders” will effectively slow down the network and result in denial of service to other users.
- Starvation attack
  - This attack consists of a hostile user who creates a significant number of nodes in the network. These nodes do not deliver any resources to the network, and might be offering bad performance or provide intermittent services. This forces the other nodes to search through a larger number of nodes, which will cost more resources and influence the performance of the network. Mitigation is done by maintaining peer profiles. When the network grows, this makes it harder for these kinds of attacks, as then the “significant number of nodes” becomes very large and practically impossible.
- Flooding attack

    - This can also be used to try to make the network inoperable, but that would need a massive number of servers and a massive amount of data. A DDoS could be used for this.
- floodfill DoS attack
    - This attack[58] can also be used to try to make the network inoperable. It would mean that all floodfill servers should be compromised by the attacker or rendered inoperable by flooding them with data. But then I2P will promote other servers to floodfill as well, so it is nearly impossible to take the complete network down with this attack.
- floodfill takeover attack
    - This attack is a combination of a Sybil and DoS attack[62]. The attacker tries to launch a large number of Sybil nodes, and tries to promote them to floodfill servers. When he owns a large number of the floodfill servers, he can control the network.

5.5.3. Legal existence attacks

In general, these attacks are used by an adversary which opposes the use of an ANNET. The goal is to make the legal existence of an ANNET impossible. To our knowledge, no research has been done into the non-technical attacks, except the case of network blocking [49]. The Tor Project publishes experiences, positive and negative, with ISP's on their website which also indicates that some ISP's and network operators block or forbid ANNET network traffic[48]. However, we do think that some attacks are already existing and active. We present some possible attacks, but more research is needed.

- Legal protection attack
    - A government can introduce law that forbids the use of ANNETs, to protect their citizens and aimed at criminals and terrorists, This will also forbid the use of an ANNET for legal purposes, so the legal protection is also the attack.
- Encryption backdoor attack
    - This attack is aimed at the encryption used in ANNETs. A government can demand that a backdoor, only known to the government, must be added to the encryption methods in such a way that only the government can decrypt the encrypted information.
- Data protection attack
    - This attack is aimed at Internet users, concerned with their privacy. Government, but also lobby organisations, can start a campaign to convince users that an ANNET is not necessary when they have concerns about their privacy and that current data protection laws and regulations give an optimal protection to the user, in order to keep the users from using an ANNET.
- Framing attack
    - This attack is also aimed at the Internet users, concerned with their privacy. The legitimate demand for privacy is continuously associated with criminal and terrorist activities by the government, lobby organizations and the media.
- Entry-point blocking attack
    - When the entry-points of an ANNET are unreachable, accessing the ANNET is impossible, this can be done for the Tor network by blocking the known entry-points. For I2P this will only work as a bootstrap attack, as only during

bootstrapping a new client fixed entry points are defined. These attacks are likely performed by government or network operators.

- Exit-point blocking attack
    - As Khattak et al.[49] describe, some network operators treat network traffic from a known Tor exit point differently. At this moment, I2P is also vulnerable for this attack, as only a few outproxy servers exist. These attacks are likely to be performed by government or network operators.
- Service refusal attack
    - Another option is that the service provider refuses to answer network request from a known ANNET exit-point. Both Tor and I2P are currently vulnerable to this approach. These attacks are likely to be performed by service providers who are gathering privacy data from their users.
- Harassment attack
    - When a government has a very negative attitude towards an ANNET, they can start criminal investigations into any possible criminal offense that has used the ANNET. They can then seize all computers that have played a role in the criminal offense, thus making operating an exit-node unattractive.
    - Harassment can also be used by organisations fighting against copyright violations by suing ISP's or private users for copyright infringement.

5.6. De-anonymization attacks

The next Group are de-anonymization attacks, they are all aimed at de-anonymizing users or services.

5.6.1. Traffic analysis attacks

They are aimed at the network traffic that runs over the public Internet. It tries to find out who are communicating with each other.

- Tagging attack
    - This attack tries to tag, to modify messages so to identify them later. But as all traffic in the tunnels is encrypted, it is not possible to identify the tagged messages, unless the attacker has more than one compromised nodes in a tunnel. However, the attacker can only find out that his nodes are part of the same tunnel, since the tunnel nodes can already find this out, a tagging attack does not reveal any information.
- Predecessor attack
    - This attack tries to analyse the tunnels to a destination statistically by participating in the tunnels. More frequent nodes are then presumed to be closer to the destination as others, and this could reveal the real node behind the destination[64]. I2P tunnel building code was especially designed to mitigate these kinds of attacks.
- Traffic analysis attack
    - As stated above, it is not a secret that I2P is running on a node, however some mitigating measures have been taken to make some of the I2P traffic less easily recognizable. There are plans to add more obfuscation, based on the work of Hjelmvik [65].
- Flow correlation attack

    - This type of attack analyses the input and output of a mix-network to try to find a correlation between these streams [66], [59]. However, the feasibility of this attack is very dependent on the number of exit points, as all exit points must be watched to find out where the input stream is exiting.
- Intersection attack
    - This attack is watching a certain target and is constantly monitoring which nodes are connecting to the target. This will reveal information about which nodes are most used for tunnels for the target, and that can then be used as a basis for other kinds of attacks [67], [62]
- Timing attack
    - This is a large group of different techniques to “fingerprint” a server. Like for example clock skew[60], analysing time patterns in incoming and outgoing network streams[68], using round trip times[69], and using the variable latency as induced by a variable load on a node[70],

5.6.2. Sybil attacks

They are performed by launching a large number of legitimate nodes, which can collude to de-anonymize users or services.

- Partitioning attack
    - This attack tries to separate the network by cutting the connections between nodes, to try to create a fragmented section around the target. I2P mitigates this by maintaining statistics about all peers, and tries to find new routes to and from the fragmented section.
- Sybil attack
    - This attack was first described by Douceur [71] and can form the basis of other attacks [58], [32]. The adversary simply joins the network with a massive number of nodes so to assure that his nodes are part of the network and can be used to launch other attacks. When the network becomes larger, it needs a very powerful adversary to succeed. However, one example is given[58], it is also possible to add a small number of floodfill routers (20) all in a partial key-space which can then be used as a DoS attack to a particular destination. Some possible solutions are given[63], [72]. However, according to Douceur[71], there is no definitive solution possible without a centralized authority.
- floodfill lookup attack
    - When a floodfill router, and its closest peers are owned by one owner, correlation between publishing netDB entries and their lookup might reveal the owner of the data[62], [73].
- Buddy exhaustion attack
    - This attack[73] relies on a Sybil attack, the attacker controlled node refuses any tunnel building request which does not completely consist of own nodes. This will result in tunnels where all the nodes are controlled by the attacker. It is partly mitigated by the peer profiling from I2P but when an adversary controls enough Sybil nodes he can still succeed. This can be a dangerous version of a Sybil attack.

5.6.3. Application abuse attacks

They are aimed at applications used by the anonymous user, which can sometimes leak information.

- Cookie attack
  - Allowing cookies will be dangerous, as sometimes these cookies can be used to gather information about the host and the user, or, with shared cookies, they can be used later to identify a client when the client contacts the server again without using an ANNET.
- Protocol attack
  - There are several ways to use a network protocol to gather information. Some protocols, like SMTP, send their IP-address to the receiver of the mail. Some protocols can be used to bypass the local proxy, so that it will directly connect to a service, which will then know the IP-address.
- Software abuse attack
  - Some software, like JavaScript and Java, has access to the disk of the node, and can be abused to read information from the disk and transfer this information to the service.

5.6.4. Metadata analysis attacks

They are aimed at metadata contained in published content or metadata in the running services.

- Metadata configuration attack
  - These attacks try to break anonymity of the users, based on extra information they gather from services or users. A possible option is to abuse configuration errors to break anonymity. They can be used to reveal the real IP-address of the hidden websites on the I2P network[74].
- Metadata content attack
  - Another option is to use published content, like office documents, which might contain metadata that can be used to identify the owner, creator or publisher of the content[75].

5.6.5. Central infrastructure corruption attacks

They are aimed at the central resources of an ANNET.

- Central resource attack
  - As there are few centralized resources necessary for the I2P network, no central resource attacks are known. For other ANNET's which are using central resources, like Tor, this is a possible option. These attacks are aiming at taking down the central infrastructure, and thus rendering the network in an inoperable state.
- Bootstrap attack
  - This is a special case of a partition attack, aimed at new nodes entering the network (bootstrapping). As these new nodes have no prior knowledge of available nodes, they will start bootstrapping based on the information published on a reseed website. By taking over such a website, the adversary might be able to force new clients to bootstrap into an isolated I2P network that is "owned" by the adversary.

5.6.6. Information harvesting attacks

They are aimed at harvesting information about users and services finding patterns or correlations.

- Harvesting attack
  - These attacks try to harvest which computers take part in the network. This information is however available in the netDB, so no defence against this attack is available. The only information is that a node is running the I2P software. It can form the basis on which another kind of attack can be launched[35]. However, when the user lives in a country where the use of anonymity networks, like I2P, is forbidden, the sheer fact that his IP-address can be harvested, should stop a user from joining the I2P network.
- floodfill anonymity attack
  - The floodfill routers contain all the information in the netDB and thus might be exploited to break anonymity. This is a special form of a harvesting attack. This is acknowledged by the I2P project but more research is needed.

5.6.7. Out-of-band attacks

They are aimed at development and implementation, rather than at the running network.

- Cryptographic attack
  - This is a broad line of attacks, aimed at breaking the encryption methods. These kinds of attacks are a threat to any type of software that uses encryption and form a separate section of research. When a cryptographic algorithm is broken, this will also have impact on encrypted information that has been sent and stored in the past.
- Development attack
  - This attack tries to insert malicious code in the source during the development of the source code. For open software, like I2P, this is mitigated by making all code public and review all code before it is added to a release.
- Bug attack
  - These attacks try to find bugs (implementation errors) in the code, which is publicly available. These attacks are also mitigated by making all the code public, so everyone can review the code and submit bug-reports and solutions for found errors.
- Client-node attack
  - These kinds of attacks aim at infecting the client-node with malicious software that has the capability of circumventing the I2P software and thus trying to break anonymity of the node. Mitigating measures to these kinds of attacks must be taken by the node owner by keeping his computer clean and have proper virus-detection installed. They can be based on a harvesting attack to attack only active users of the network.

5.7. New attacks.

We give an inventory of new attacks that are made possible by our design enhancements. Since all nodes will act as an outproxy, we see a larger attack area, and the following attack possibilities:

De-anonymization information harvesting attack

- Internet Tunnel correlation attack
    - Because extra information about Internet tunnels is published in the netDB, it might reveal extra information that can possibly be used to correlate Internet tunnels with nodes.

Network unavailability attack

- Outproxy attack
    - Use the outproxy feature as an attack vector, as all nodes have a direct connection to the Internet, it might be possible to "inject" network traffic into the I2P network as a DoS attack.

Existence impossibility attack

- Outproxy traffic routing attack
    - It might be possible that the outproxy traffic can be identified by a certain fingerprint. This fingerprint can then be used by network operators to block or delay the network traffic.

Since we split the node from the I2P software, the I2P software will act as the Internet access point of the node, meaning that all network traffic will pass through I2P. This might make extra variations of application attacks possible.

Protocol attacks are no longer possible. As the I2P software has its own IP-address, the user-node can use a fake IP-address, therefore, a protocol attack will only reveal the fake IP-address.

De-anonymization application abuse attacks
These are becoming more dangerous. As all connectivity from the node is passed through I2P more possibilities might become available to exploit this.

- Sandbox circumvention attack
    - It might be possible that software running on the node, and having network connectivity can find out what the IP-address and the identifier is of the I2P node, and then send that IP-address and identifier to an adversary, maybe even together with other identifying information as found on the computer.
- Cookie attacks
    - These attacks are probably also becoming more dangerous. Many Internet services will not work properly without accepting cookies by the user. The cookies will be transported and stored on the user-node. So, special care must be taken to prevent information leakage.

5.8. Impact

Before we start the risk assessment, we will handle the impact separately. As is noted in this chapter, we only see 4 different kinds of impact, three types of unavailability and 1 type of de-anonymization. However, from a user perspective, there is no difference between the user's service unavailable and network unavailable impact, so we combine these into a service unavailable impact.

We assess the impact for these 3 types for the users, as defined in 3.1.1. With this information we then have a general overview of the impact of the different risks. We present each of the impacts in a half bow tie diagram.

5.8.1. Service unavailable impact

We start with the bow tie (see Figure 17). It represents only the impact half of a bow tie diagram. We adapted it to present the impact for each of the three user types we defined in chapter 3.1.1.
The overall impact is that the network or services are unavailable but no security or privacy risks occur, so the impact is considered Medium.

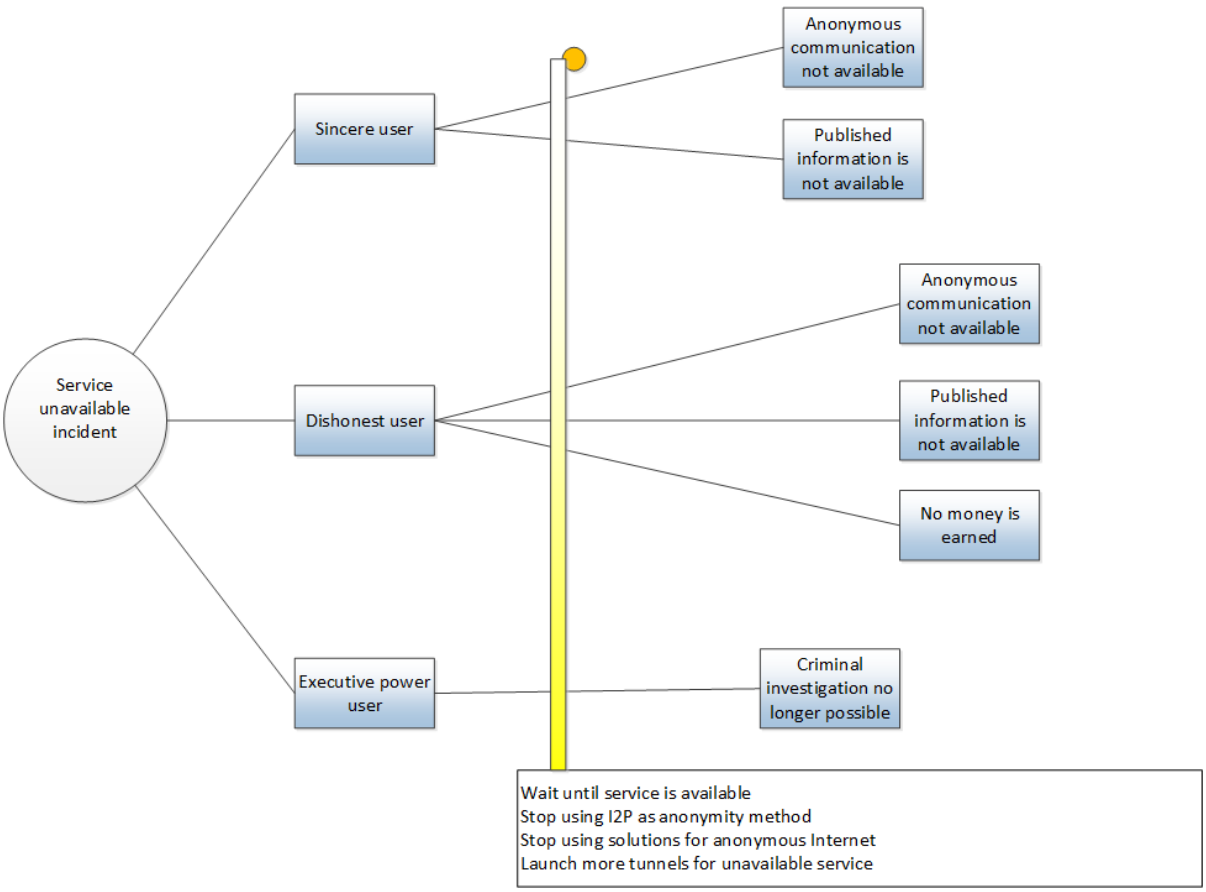

Figure 17 Impact of the service unavailable incident

Impact for Sincere user
Both communication and publishing or reading information is impossible. For the typical example users, this will lead to the following impact:
Sincere users

- Privacy aware citizen
  - He can only communicate without anonymity. He probably has to stop some types of communication.
- Journalist

    - The journalist is not able to communicate anymore with people sending him information. When he is relying on these sources, his investigating work will stop.
- Activist
    - The activist is depending on the availability of the services to spread his ideas or to communicate with equal stemmed groups. The spreading of ideas stops.
- Whistle-blower
    - The whistle-blower cannot publish information about misbehaviour. He has to use other means to reach his goals.

The impact for the sincere user is Low, there are not many activities with an urgent character, so probably "waiting till the incident has been solved" is acceptable.
Reverting to other anonymity solutions, or working without anonymity are not likely solutions. When only one service is unavailable, adding tunnels to this service could overcome the unavailability.

Impact for Dishonest user
Not only communication and publishing/accessing information is impossible, also financial transactions are impossible.

- Criminal
    - When a criminal is using the darkweb to earn money with his criminal deeds, the heaviest impact is that his source of earning money stops.
- Terrorist
    - He cannot pay for goods and services, nor is he able to get paid. He is not able to spread his ideas.

As the main activities for these users are no longer possible, the impact is considered Medium. Waiting until the incident is solved is possible, but some loss in money or time is inevitable.
As these groups are very dependent on their anonymous contacts, reverting to another anonymity solution is not feasible.

Impact for Executive power user
Communication and accessing information is impossible.

- Police
    - Criminal investigations on the darkweb have to stop
- Contra-terrorism
    - Investigation into terrorists group have to stop
- Intelligence services
    - Gathering information about other states in an anonymous way have to stop

Reverting to other anonymity solutions is possible, especially where the anonymity network is used as a means during investigation, and is not the target of the investigation.
We consider the impact Low.

5.8.2. Legal existence impact

When the use of the network is declared illegal, it has impact on all the users. As with I2P it is quite easy to determine which nodes are part of the network, and therefore it can be very easy to determine the illegal users.
There is no difference anymore between Sincere users and Dishonest users. The impact is considered High.

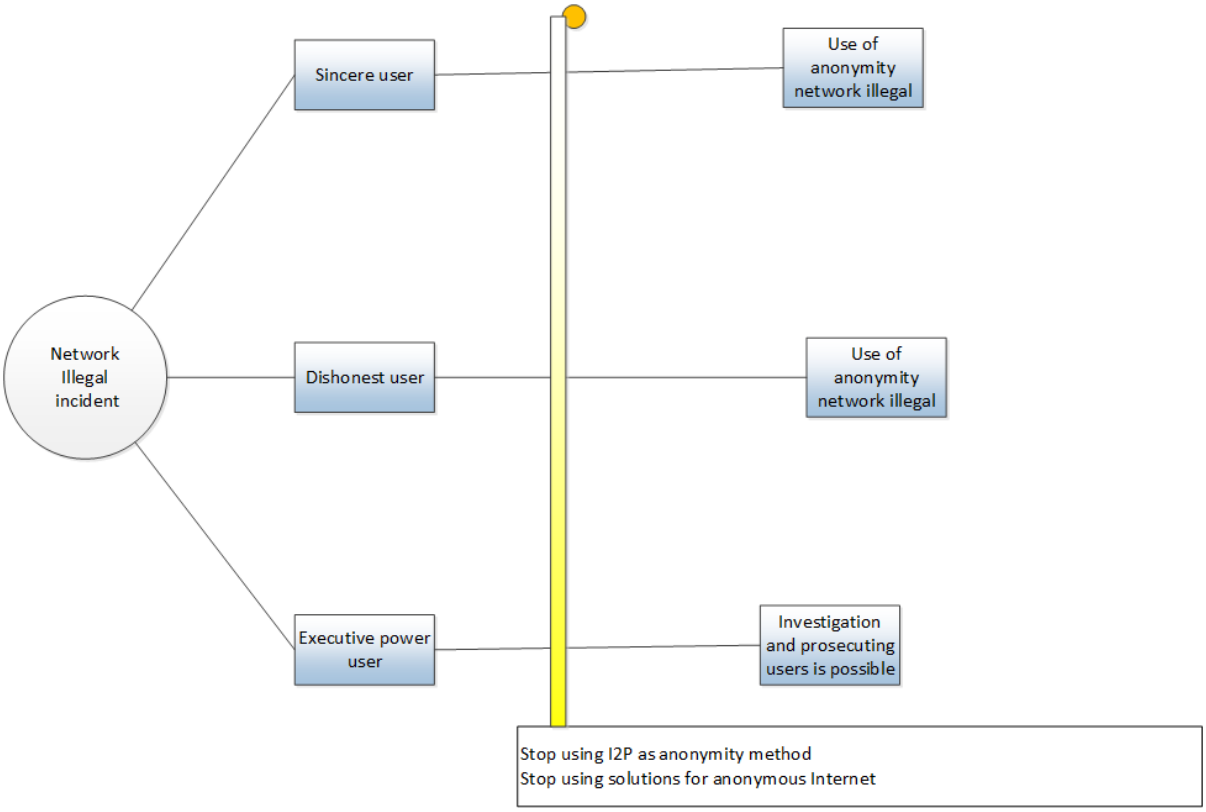

Figure 18 Impact of the network illegal incident

Impact for Sincere user and Dishonest users
As the use of I2P is illegal, all users face arrest for mere running the I2P software on their computer. Depending on the penalties that are defined and the level of active prosecuting, the I2P network can be impossible to use. The impact is estimated as High, because all users have to revert to other solutions.

Impact for Executive power user
They have the ability to prosecute all users. The impact is estimated as Medium, as probably most users will leave the network. This includes users under active investigation.

5.8.3. De-anonymization impact

For this impact analysis, we also make a difference between the type of society where the user lives. We see a difference between a free country and countries with an oppressive regime.
Also important in some cases is which kind of threat actor has de-anonymized the user or service.

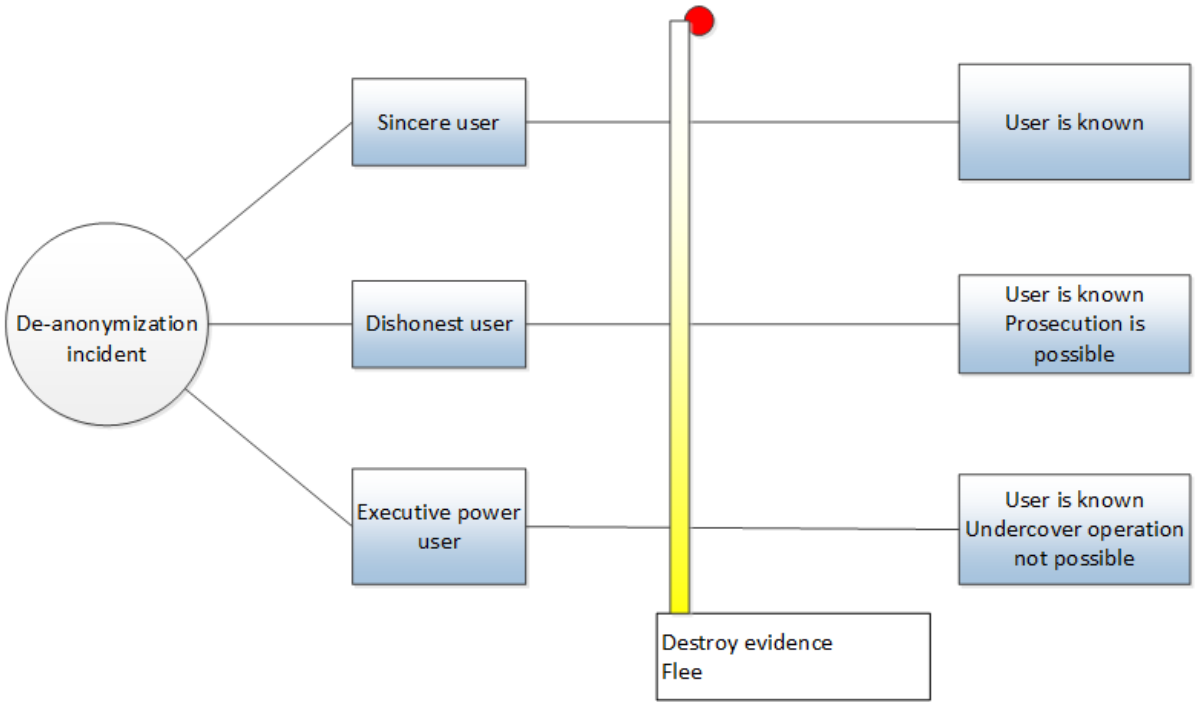

Figure 19 Impact of the de-anonymization incident

The impact is dependent on the adversary and the type of government in the country where the user lives.
When this is a democracy, and the adversary is an executive power, and the user does not employ illegal activities, the impact can be low.
However, when the user is not living in a democracy, and the adversary is an executive power, the chances for arrest and trial are much higher, as many activities can be regarded by the government as a threat for society.

When the adversary is not an executive power, but a criminal or activist group, blackmail is possible, or his activities can be revealed to others, which could harm the user.

In all cases the impact can be High, in the worst case de-anonymization can be life-threatening.
As no recovery is possible the impact is considered High.

For the typical example users, this will lead to the following impact:
Sincere users

- Privacy aware citizen
    - When he is de-anonymized, the impact can be low. However, depending on the type of activities and his social status, he might become vulnerable for blackmail.
- Journalist
    - The journalist might lose the trust from his informers and it becomes more difficult to gather information and news. In totalitarian states, he might become unemployed and get trialled.
- Activist

    - When the identities become known from activists, it can become more difficult to employ their activities.
- Whistle blower
    - When his identity becomes known to the organisation he has accused of misbehaviour, he might lose his job, or in a totalitarian state he could get arrested and trialled for treason.

Impact for Dishonest user

The dishonest user is known to the adversary. As the chances are high that executive powers have de-anonymized him, prosecution becomes possible.

- Criminal
    - He is not able to perform his activities anymore, it is possible that he will get arrested and trialled for his criminal behaviour.
- Terrorist
    - He is not able to deploy any activities anymore, it is possible that he will get arrested. In some countries, he might face a death penalty for his activities.

Impact for Executive power user

When they become known, informers will lose their trust in the executive powers, and their undercover activities end. It is possible that prosecution or investigations have to be stopped.

- Police
    - Investigations might have to stop and prosecution might become impossible, thus some criminals might be able to continue their criminal activities.
- Contra-terrorism
    - It is possible that they lose track of terrorists or terrorist groups.
- Intelligence services
    - It is possible that their undercover operations have to end, and that they will lose valuable sources of information.

6. Risk assessment

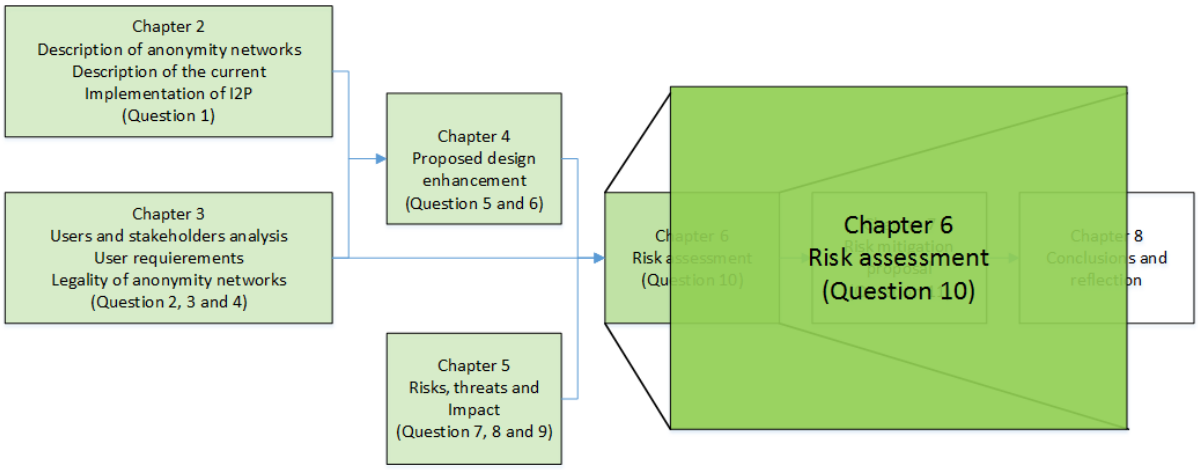

Figure 20 Guidance for chapter 6.

In chapter 5, the threat actor capabilities, the threat actors, the threat classification and impacts are defined. In this chapter, we combine this information with the information about the new proposed design (chapter 4) and the information about the users and stakeholders (from chapter 3) to make a risk assessment for each of the classified threats. We start with the definitions we use throughout this thesis, explain the method and describe the way how we present the results of the risk assessment.
Then for each threat group a quantitative assessment of the risk is made. We conclude the chapter with a general overview of the results.

6.1. Definitions and method of risk assessment

For our definitions and method, we use the ISO standards (27005[76] and 31010[77]).

Asset	People, property or information.
Vulnerability	Weakness in an asset.
Threat	Anything that can exploit a vulnerability and damage an asset. When an intentional threat is considered, this is also referred to as “attack”.
Threat actor	Person or organisation who is intentional threatening an asset.
Risk	The potential for loss of or damage to an asset.
Incident	The occurrence of loss of or damage to an asset.
Likelihood	Expressing how likely it is that an incident occurs in a qualitative way, usually expressed semi-quantitatively as intervals, such as Low, Medium and High.
Impact	The impact on the user or organisation when the incident occurs, also expressed as Low, Medium or High.
Extra definitions:	
Simplicity	The skill level and resources needed for an attack in a qualitative way.
Effectivity	Expresses the chance and time that a launched attack will lead to an incident in a qualitative way.

Table 5 Risk assessment definitions

We will use an estimation of the simplicity and effectivity of an attack to make an estimation of the likelihood that an attack will lead to an incident.

The impact of the incidents was already described in chapter 5.

Confusing is that the asset is used in two meanings, in the definition of risk and in the definition of vulnerability. The reader must keep in mind that these are very different assets. An asset in the definition of vulnerability can be anything that has a weakness that can be exploited to damage the asset as used in the definition of risk.

6.1.1. Method

For our research, we define the anonymity of the users and the availability of the services as the assets that need to be protected. So, the risk assessment in this chapter is aimed at assessing the risk for these assets.

As the attacks are developed to damage an asset, the threat actor will have its reasons for this. For each risk, we will give some examples of the reasons of the threat actors, to give more insight who these threat actors might be and how powerful these threat actors are as this will influence the likelihood and effectivity of an attack.

For each threat, the risk is dependent on the likelihood, the chance that the incident will happen, and the Impact.
As the likelihood of an attack is difficult to estimate, we added two concepts to give a better understanding of the estimation of the likelihood. The likelihood itself is dependent on the simplicity of launching an attack and on the effectivity of the attack. When the simplicity is Low, and the effectivity is High, the resulting likelihood is High.
The likelihood is also dependent on the effectivity of prevention controls. Prevention controls can lower the effectivity or simplicity of the attack, and thus have influence on the likelihood.
For each risk, we give an evaluation of the likelihood of the threat and of the effectivity of the controls. The impact when the threat occurs, together with the potential recovery controls is already given in the previous chapter. The risk is than rated with the likelihood and impact in a risk matrix.

We present Bow tie diagrams for each risk, with the following legend:

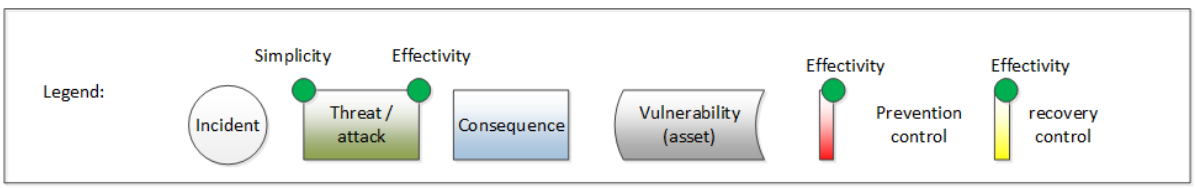

Figure 21 Legend of the bow tie diagrams

With each threat/attack, an assumption of the simplicity of that attack is given with a coloured circle in the upper left corner, where green means low, orange means medium and red means high. The simplicity of an attack is depending on the resources and skills needed to launch an attack.

For the threats, a coloured circle on the right denotes the effectivity of the threat, where green means low effectivity, orange medium effectivity and red a high effectivity. Effectivity is the chance that a launched attack will lead to the incident.
For the controls, a coloured circle on the right denotes the effectivity of the control, where green means high effectivity, orange medium effectivity and red a low effectivity.
All these coloured circles are chosen in such a way that green circles attribute to a lower risk, while red circles attribute to a high risk.
For each vulnerability is also expressed what asset contains the vulnerability.

6.2. Unavailability risks

These are the first three attack groups, service unavailability, network unavailability and existence impossibility attacks.

6.2.1. Service unavailability risk.

The service unavailability attacks are aimed at a specific service that is offered on the I2P network. The goal of these attacks is to make the selected service unavailable.
Reasons could be that the service is offering illegal goods (e.g. Darknet market place), is spreading unwanted information (e.g. terrorist group or activists opposing a regime) or is supporting communication between suspect groups or individuals.
Threat actors are likely to be law enforcement, criminals and hacktivists.

We present an overview of the service unavailability risk in the following bow tie diagram.

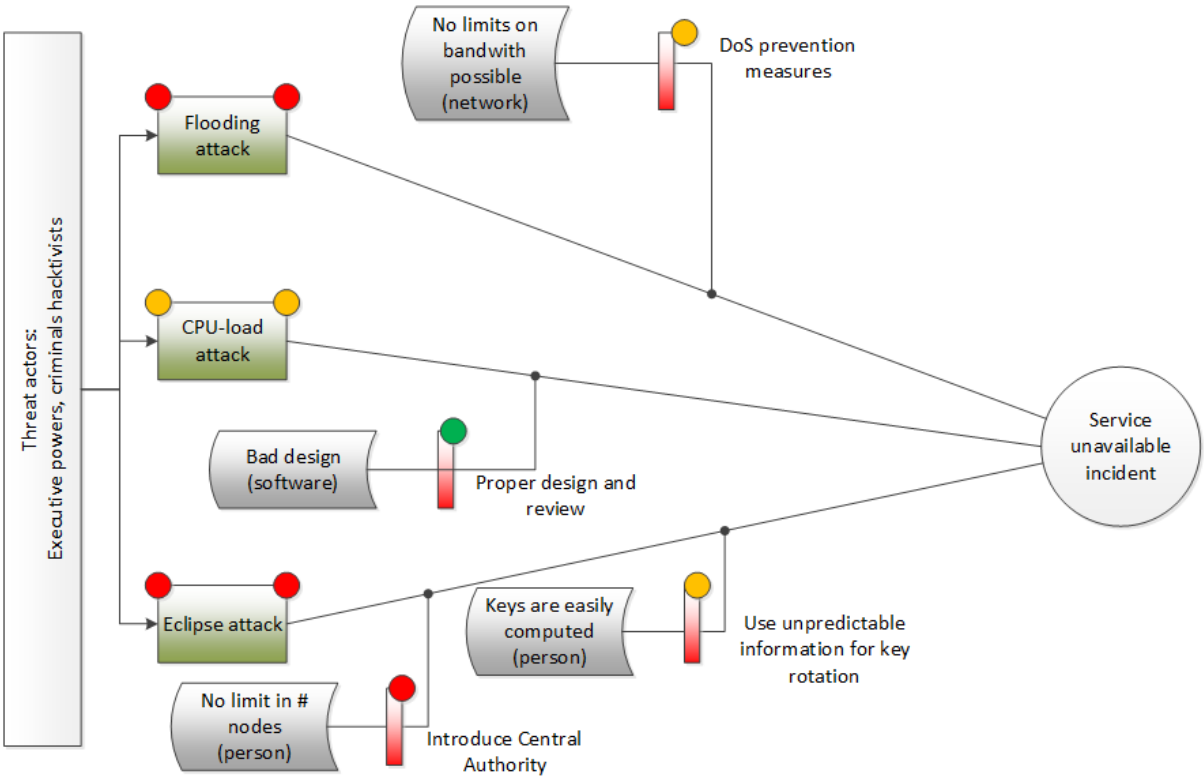

Figure 22 Bow tie diagram of the service unavailability risk

Evaluation

Simplicity.

The Simplicity is High, as not much resources are needed for a flooding attack or an Eclipse attack, these attacks are easily deployed and do not need very specific knowledge.
Simplicity reducing controls:

- for CPU-load attacks is proper software development. The system of public source code review can be effective.

The simplicity for this group of attacks is estimated as High.

Effectivity.

Effectivity is estimated High. Research has shown that the Eclipse attack is very effective, and can make a service practically unreachable.
Effect reducing controls:

- For flooding attacks, all known DoS prevention controls can be used, they still need a lot of resources and are not easily deployed. Only larger organisations might have the resources for implementing these controls.
- For Eclipse attack, the introduction of a central authority in I2P as a prevention control is very unlikely. Changing the system that computes the DHT search keys of the nodes should make key rotation less predictable, however whether that solution is sufficient is not known. More research is needed.

As the effectivity of the threats is High and the Simplicity is high, the Likelihood is considered High.

Risk
The likelihood is considered High.
The impact is considered Medium.

Table 6 Risk matrix of service unavailability risk

Likelihood impact	Low	Medium	High
High			
Medium			X
Low			

6.2.2. Network unavailability risk.

The network unavailability attacks are aimed at the complete I2P network. The goal of these attacks is to make the network unavailable.
Reasons could be that a government is opposing the use of ANNET's or free-riding behaviour by users.
Threat actors are likely to be executive powers or users.

We present an overview of the network unavailability risk in the following bow tie diagram.

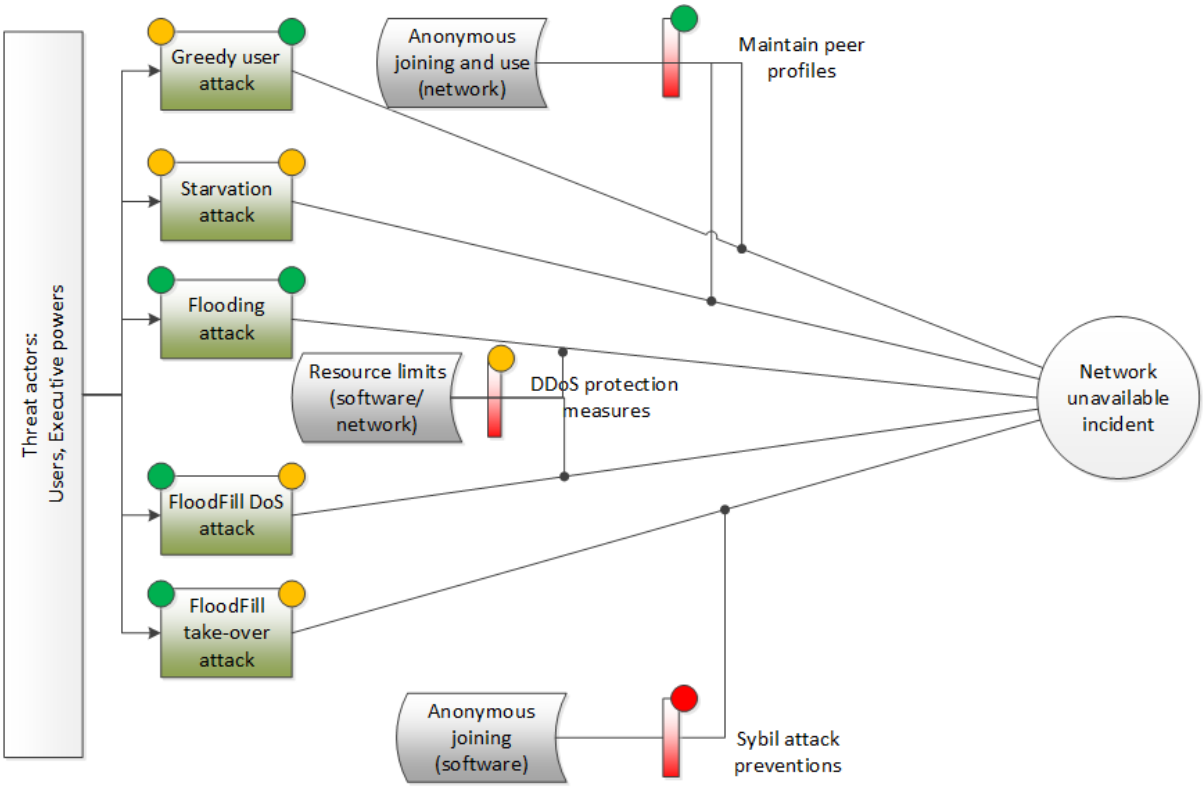

Figure 23 Bow tie diagram of the network unavailability risk

Evaluation

Simplicity.

The simplicity is estimated as Low or medium, most attacks will need a lot of resources and many adversary-owned nodes.

Simplicity reducing controls:

- The peer profiling mechanism in I2P is effective against starvation and greedy user attacks.

Effectivity is estimated Low or medium. The I2P network will automatically try to add more floodfill routers to mitigate the floodfill attacks.

Effect reducing controls:

- For flooding attacks, all known DoS prevention controls can be used, they still need a lot of resources and are not easily deployed. Only larger organisations might have the resources for implementing these controls. The Sybil protection measures are not very effective, but I2P will itself mitigate floodfill attacks.

As the effectivity of the threats is Low/Medium, while simplicity is low, the likelihood is estimated as Low.

Risk

We consider the likelihood as Low.

The impact is considered Medium.

Table 7 Risk matrix of network unavailability risk

Likelihood / impact	Low	Medium	High
High			
Medium	X		
Low			

6.2.3. Legal existence risk.

The legal existence attacks are aimed at the existence of the I2P network. The goal of these attacks is to make the existence of I2P and other ANNETS impossible or illegal.
Reasons could be that a government opposes strongly to anonymity of citizens, or companies who see anonymity as a threat to their business model.
Threat actors are likely to be legislative powers with negative attitude to ANNET, executive powers, ISP's and network operators and companies on the Internet.

We present an overview of the legal existence risk in the following bow tie diagram.

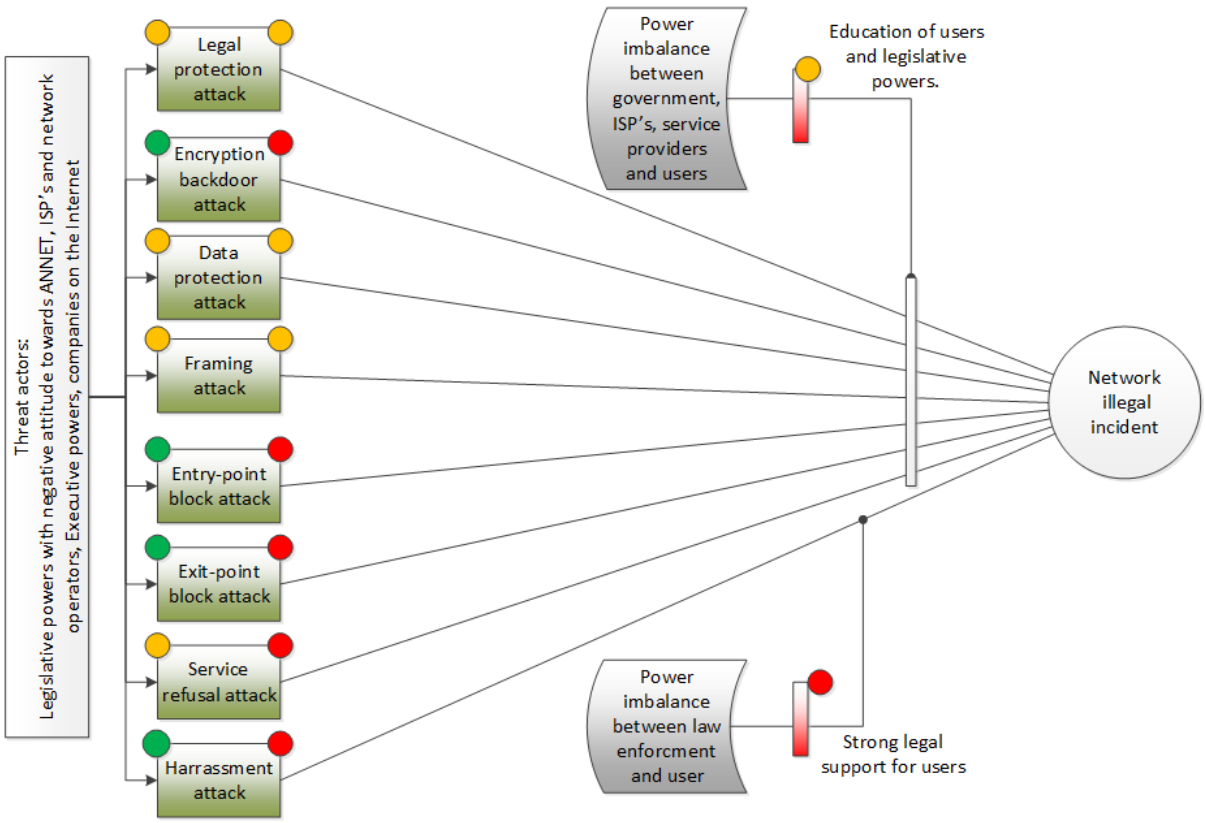

Figure 24 Bow tie diagram of the legal existence risk

Evaluation

Simplicity

The simplicity is estimated as Low/Medium. Some attacks have already been seen in history (exit-point blocking attack, encryption backdoor attack). For Europe and the USA these attacks have not yet been very successful. It takes a long time of preparation and skilful lawyers. Outside Europe and the USA there can be a much higher simplicity when a

government can define new laws without democratic process. E.g. the entry-point blocking attack is actively supported by the Chinese Government.

Effectivity
Effectivity is estimated Medium/High.
Effect reducing controls:

- For Europe and USA, education of users and mobilisation of the public opinion is reasonably successful, in other countries, where a free press is not possible, these controls will have no effect.

With a Low/Medium simplicity and a Medium/High effectivity, the likelihood of a succesfull attack is considered Medium.

Risk
We consider the likelihood as Medium.
The impact is considered High.

Table 8 Risk matrix of legal existence risk

Likelihood impact	Low	Medium	High
High		X	
Medium			
Low			

6.3. De-anonymization risks

Next, we will assess all the de-anonymization attacks.

The de-anonymization attacks are aimed at specific services or specific users on the I2P network. The goal of these attacks is to de-anonymize the services or users.
Reasons could be that services are considered illegal or users are suspected of illegal activities.
Threat actors are likely to be executive powers.

6.3.1. Traffic analysis risk.

We present an overview of the traffic analysis risk in the following bow tie diagram.

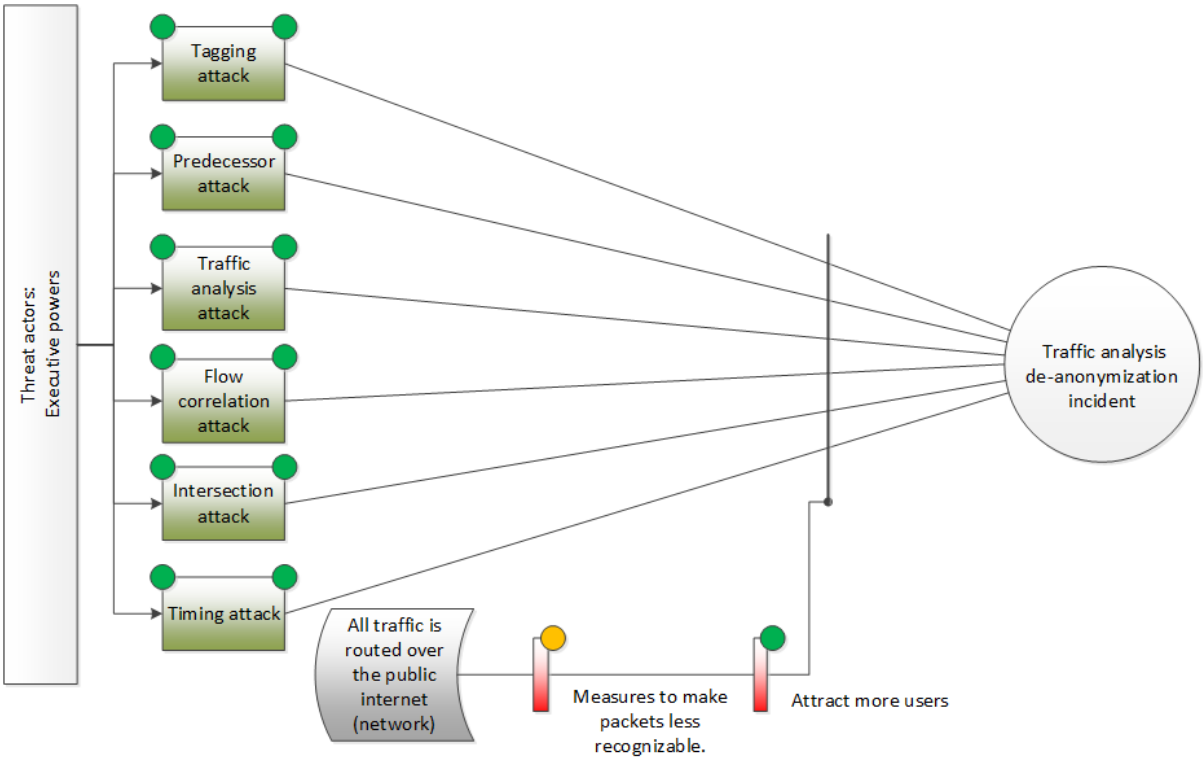

Figure 25 Bow tie diagram of the traffic analysis risk

Evaluation

Simplicity

The Simplicity is estimated as Low. Most attacks need a global adversary to be successful, but that capability is not in scope. (See paragraph 5.2)

Simplicity reducing controls:

- The number of users has a large impact on the simplicity, with more users the amount of resources for an attack grows.

Impact

Effectivity is estimated Low. As most users are not using the outproxy functionality, and most network traffic stays internal in the I2P network, most attacks are not successful.

Effectivity reducing controls:

- The number of users has a large impact on the effectivity, with more users the success rate of the attacks drops, thereby reducing the effectivity.

With a Low simplicity, and a Low effectivity, the chance of a successful attack is Low, so the likelihood is Low

Risk

We consider the likelihood as Low.

The impact is considered High.

Table 9 Risk matrix of traffic analysis risk

Likelihood impact	Low	Medium	High
High	X		
Medium			
Low			

6.3.2. Sybil risk.

We present an overview of the Sybil risk in the following bow tie diagram.

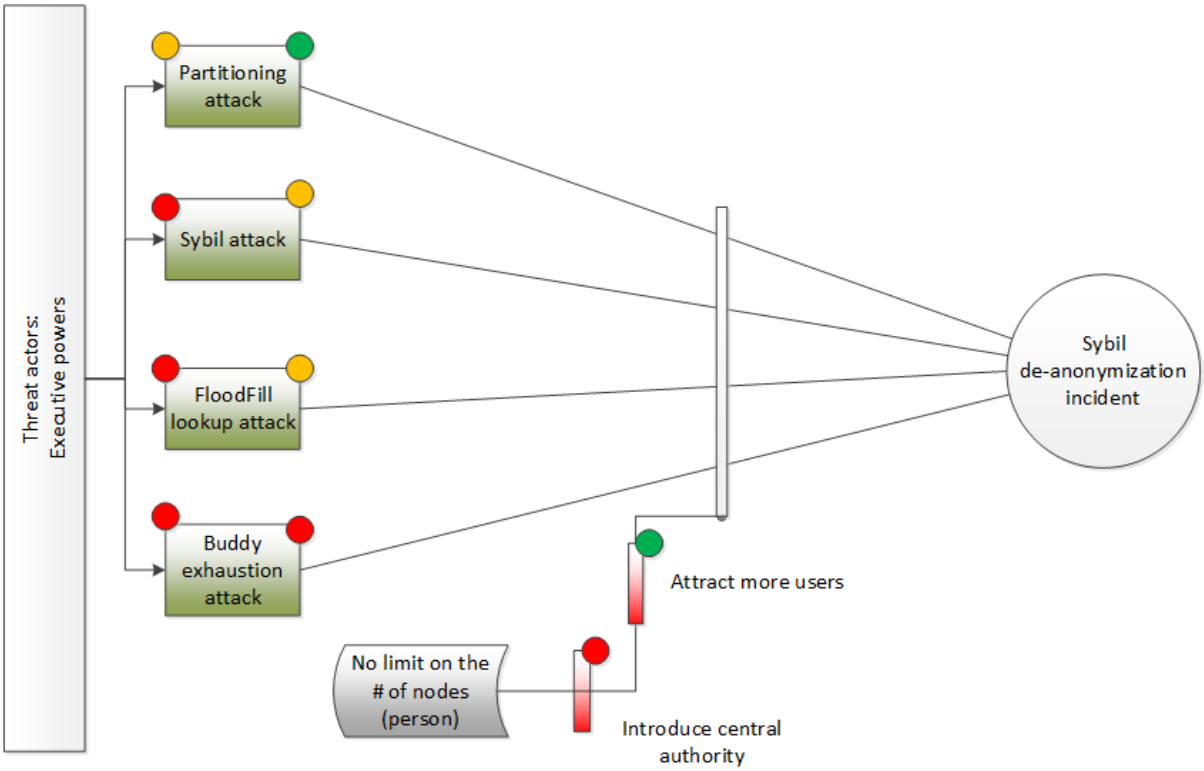

Figure 26 Bow tie diagram of the Sybil risk

Evaluation

Simplicity

The simplicity is estimated as High. Because of the anonymous nature of an ANNET, it is very easy to add Sybil nodes to the network. The resources needed for adding several nodes are low.

Simplicity reducing controls:

- A central authority which issues certificates might be able to prevent Sybil nodes, but this is unlikely for I2P as no central authority exists.
- A prevention control is to attract as much users as possible, as this will make the number of Sybil nodes, needed for an attack, also much larger, and thus more difficult.

Effectivity
Effectivity is estimated Medium/High. There is no difference between a normal node and a Sybil node, so recognising a Sybil attack is very difficult. And a powerful adversary can launch a powerful attack with a high chance of success.
The effectivity is considered High. Combined with a High simplicity, the chance of a successful attack is High, thus the likelihood is High

Risk
We consider the likelihood as High.
The impact is considered High.

Table 10 Risk matrix of Sybil risk

Likelihood impact	Low	Medium	High
High			X
Medium			
Low			

6.3.3. Application abuse risk.

We present an overview of the application abuse risk in the following bow tie diagram.

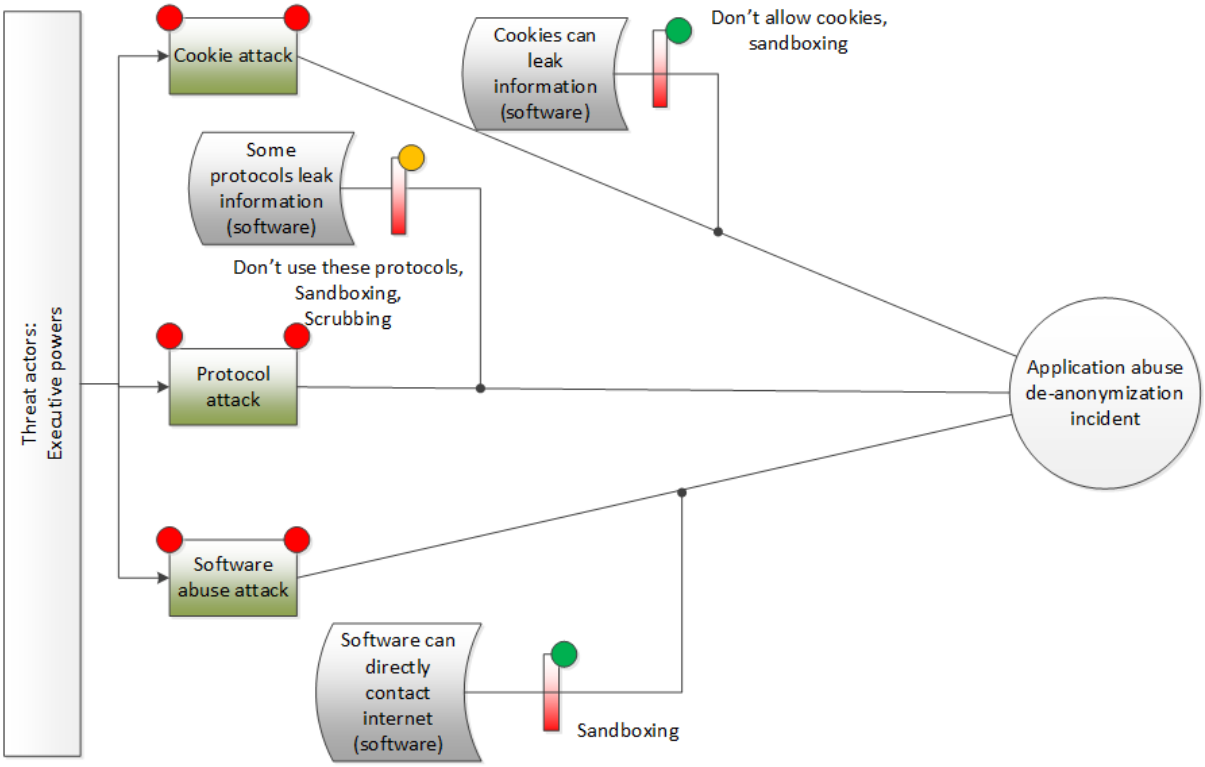

Figure 27 Bow tie diagram of the application abuse risk

Evaluation

Simplicity

The simplicity is estimated as High, an attack can be launched without much resources or knowledge.

Simplicity reducing controls:

- The Simplicity can be influenced by carefully choosing the right protocols and not allowing cookies.

Effectivity

Effectivity is estimated High as most attacks will reveal some privacy information, like IP-addresses.

Effectivity reducing controls:

- Sandboxing seems a good control to prevent the leaking of IP-addresses and other related information. It cannot control however that applications try to send information without the user knowing this.

As the effectivity of the threats is High and the simplicity is High, the chance of a successful attack is High, but fortunately, the effectivity reducing control of sandboxing is highly effective, therefore the Likelihood is reduced to Medium.

Risk

We consider the likelihood as Medium.

The impact is considered High.

Table 11 Risk matrix of the application abuse risk

Likelihood impact	Low	Medium	High
High		X	
Medium			
Low			

6.3.4. Metadata analysis risk.

We present an overview of the metadata analysis risk in the following bow tie diagram.

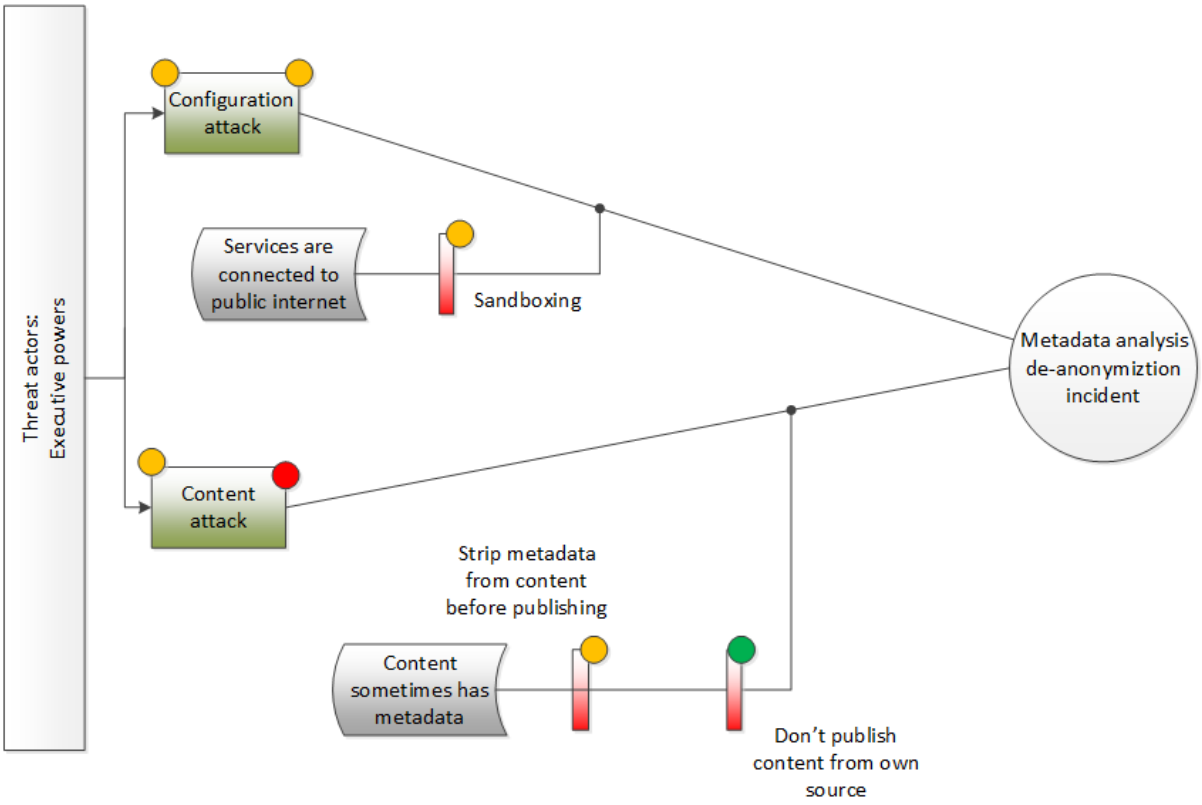

Figure 28 Bow tie diagram of the metadata analysis risk

Evaluation

Simplicity

The simplicity is estimated as Medium, it has to be directed at one specific service or at specific content and therefore a certain amount of knowledge of that specific service or contents is needed.

Effectivity

Effectivity is estimated Medium to High. There is a relatively high chance to find configuration errors in a service, or metadata with the published content.

Effect reducing controls:

- Careful with publishing information from a source and stripping metadata from content can prevent metadata leakage.
- Sandboxing will reduce the chance that configuration errors will reveal information.

As the effectivity of the threats is Medium/High, but the controls can be effective, the effectivity is considered Medium. With a simplicity also Medium, we consider the likelihood of a successful attack Medium.

Risk

We consider the likelihood as Medium.

The impact is considered High.

Table 12 Risk matrix of metadata risk

Likelihood impact	Low	Medium	High
High		X	
Medium			
Low			

6.3.5. Central infrastructure corruption risk.

We present an overview of the central infrastructure corruption risk in the following bow tie diagram.

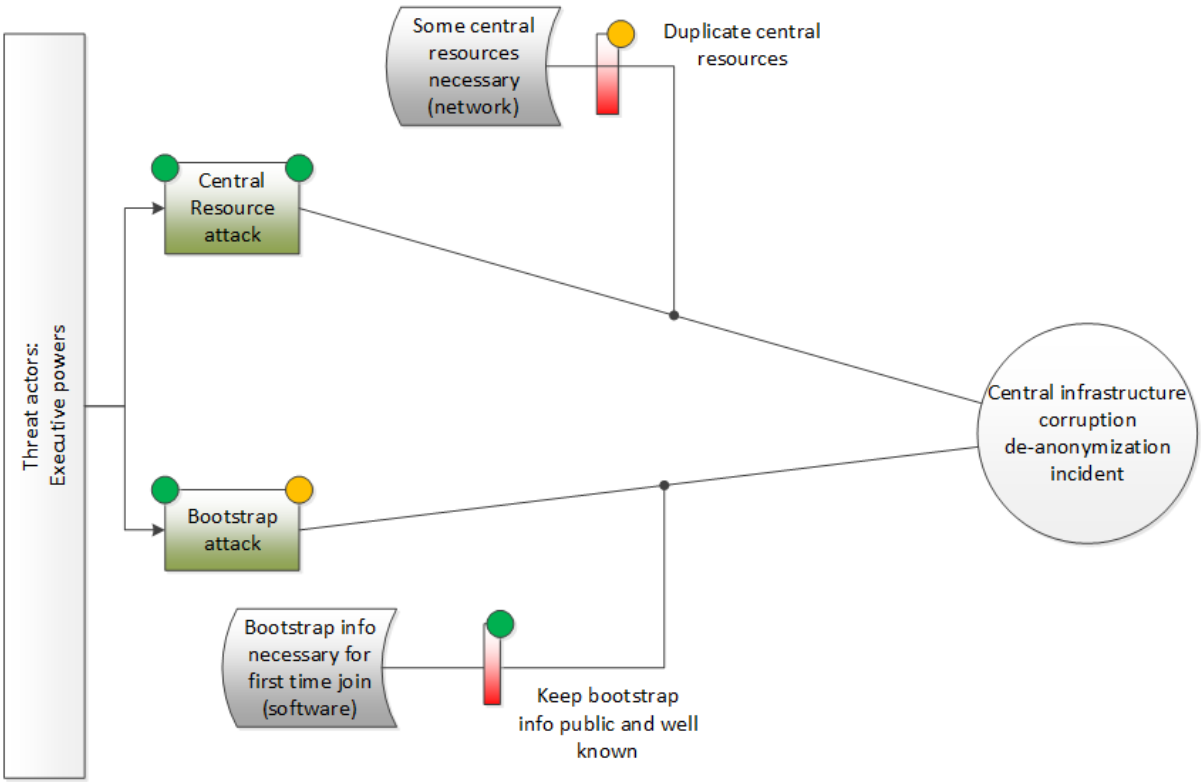

Figure 29 Bow tie diagram of the central infrastructure corruption risk

Evaluation

Simplicity

The simplicity is estimated as Low. There are not much central resources in I2P, especially not in the running ANNET. Only bootstrapping a new client is dependent on central infrastructure. A lot of knowledge and resources are needed to corrupt the central infrastructure.

Simplicity reducing controls:

- Publish the bootstrap information widely and keep new users well-informed where to find this information.

Effectivity

Effectivity is estimated Medium. Only new users are effected.

Effect reducing controls:

- Duplicate central resources over several instances, so corruption of all central resources is unlikely.

As the Simplicity of the threats is Medium, the effectivity is Medium and the controls will be effective, the likelihood is Low.

Risk
We consider the likelihood as Low.
The impact is considered High.

Table 13 Risk matrix of central infrastructure corruption risk

Likelihood / impact	Low	Medium	High
High	X		
Medium			
Low			

6.3.6. Information harvesting risk.

We present an overview of the information harvesting risk in the following bow tie diagram.

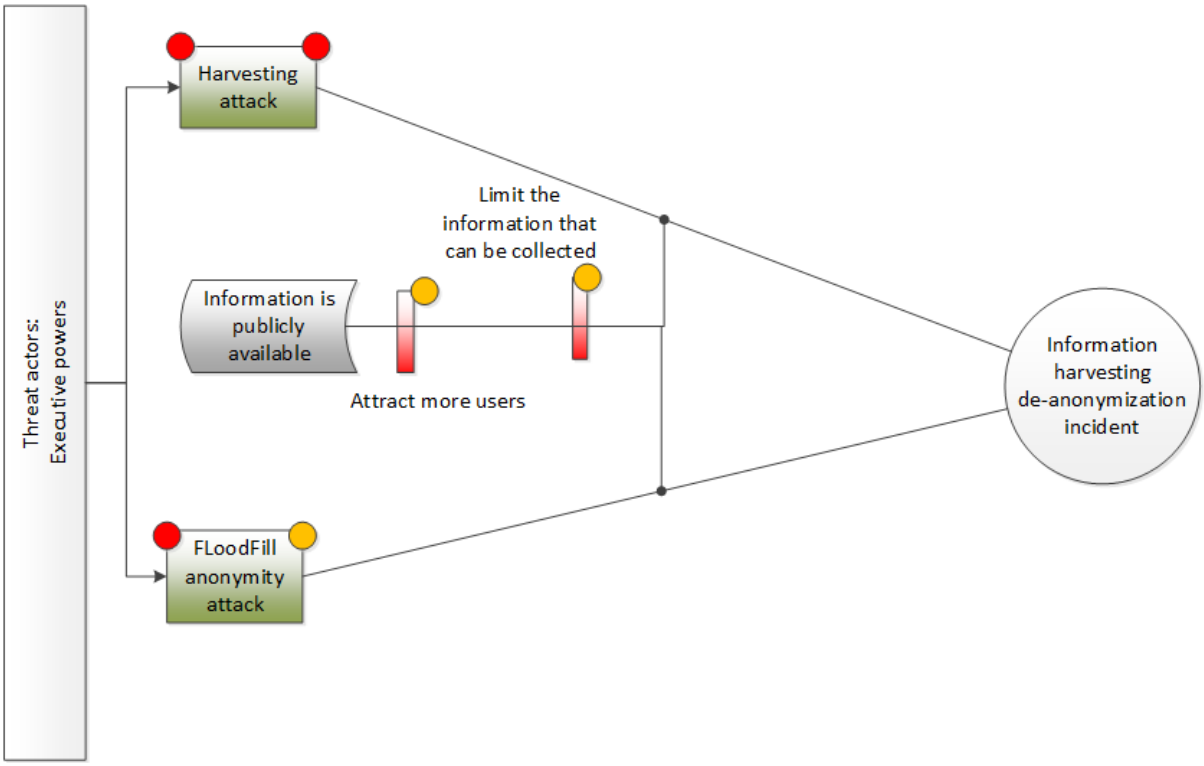

Figure 30 Bow tie diagram of the information harvesting risk

Evaluation
Simplicity

The Simplicity is estimated as High, no special resources and skills are necessary,
Simplicity reducing controls:

- When there are more active users it's harder to correlate all information and the chances are lower that a specific user or service can be de-anonymized.

Effectivity
Effectivity is estimated Medium/High. Due to the public availability of all information, it is very likely that information can be correlated and users and service can be de-anonymized.
Effect reducing controls:

- Limiting the amount of information that can be collected, this must be carefully tuned to prevent problems with operating the network.

As the effectivity of the threats is Medium/High and the simplicity is High, the likelihood is considered High.
One special remark with this attack: every node that joins the network will publish the IP-address of the node in the routerInfo. When a user is living in a country where the use of I2P is suspicious or even forbidden, the executive powers can easily harvest all IP-addresses form the netDB and expose the user. In that situation, it is impossible to use I2P without risk.

Risk
We consider the likelihood as High.
The impact is considered High.

Table 14 Risk matrix of information harvesting risk

Likelihood / impact	Low	Medium	High
High			X
Medium			
Low			

6.3.7. Out-of-band risk.

We present an overview of the out-of-band risk in the following bow tie diagram.

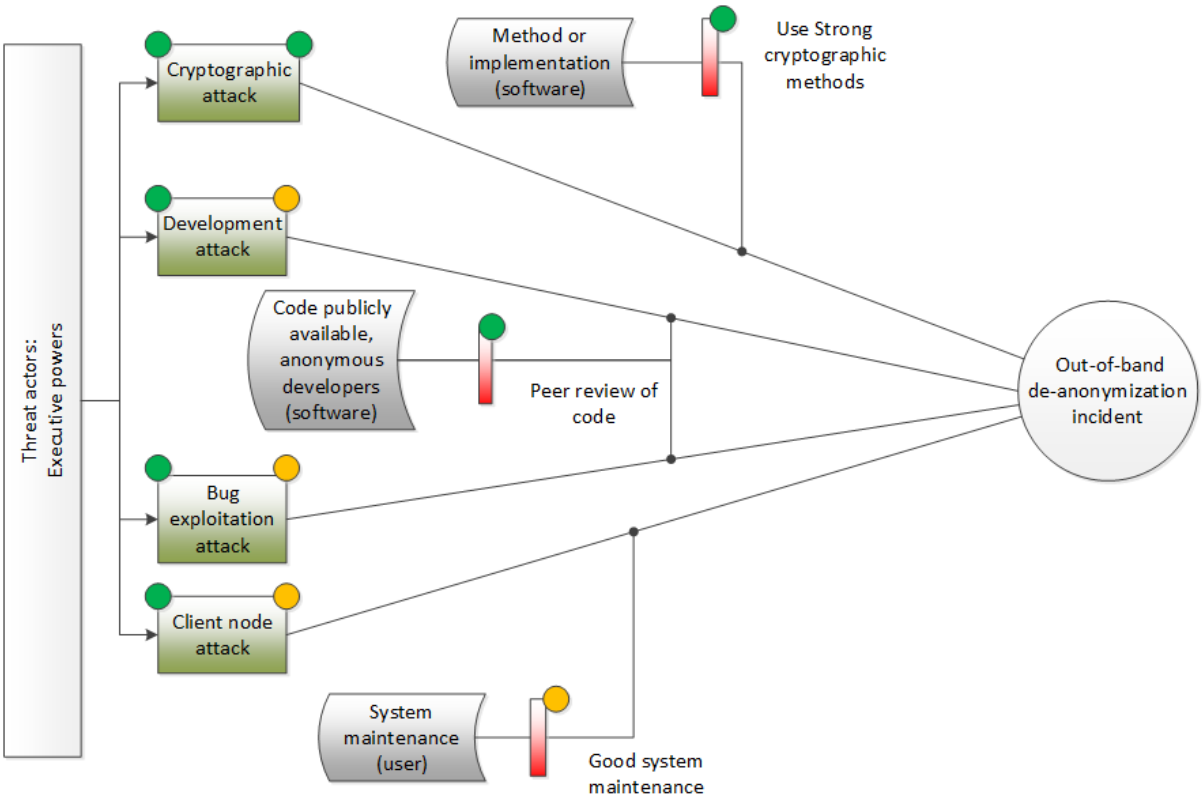

Figure 31 Bow tie diagram of the out-of-band risk

Evaluation

Simplicity

The Simplicity is estimated as Low. A high skill level is needed for these attacks, they probably will cost a lot of time and resources.

Simplicity reducing controls:

- Most important is that the developed code is reviewed and checker regularly, this will reduce the likelihood.

Effectivity

Effectivity is estimated Low/Medium. The chance that a successful attack can be developed is Low.

Effect reducing controls:

- System maintenance is important for the user to keep his system clean.

As the effectivity of the threats is Low/Medium and the simplicity is Low, the likelihood is considered Low

Risk

We consider the likelihood as Low.

The impact is considered High.

Table 15 Risk matrix of out-of-band risk

Likelihood impact	Low	Medium	High
High	X		
Medium			
Low			

6.4. New unavailability risk.

The new unavailability attack possibilities are aimed at the availability of the outproxies. Reasons could be that the adversary is against the use of anonymity networks
Threat actors are likely to be executive powers.

We present an overview of the new unavailability risk in the following bow tie diagram.

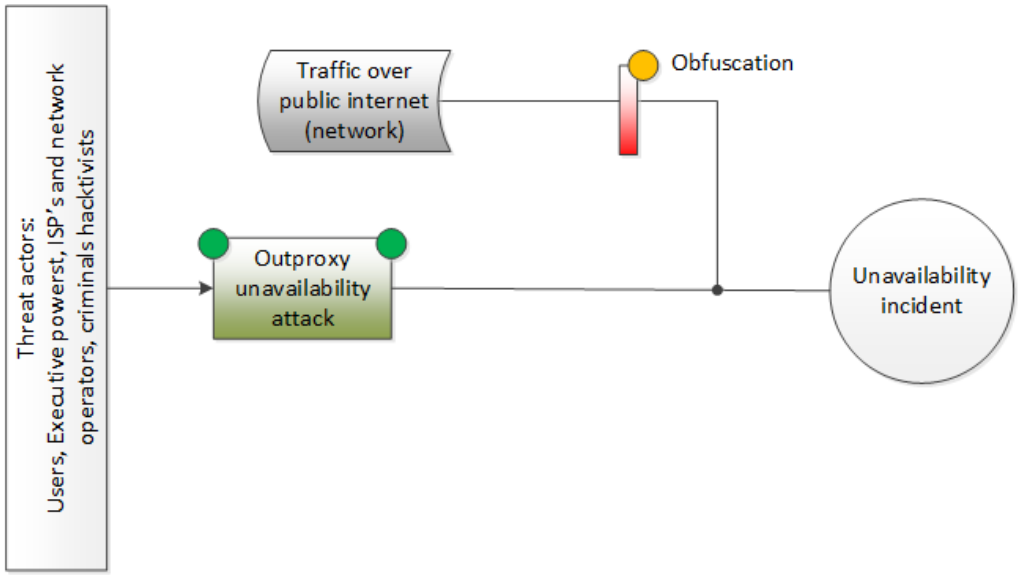

Figure 32 Bow tie diagram of the new unavailability risk

Evaluation

Simplicity
The simplicity is estimated as Low. Large resources are needed to make the outproxy functionality unavailable.
Simplicity reducing controls:

- When obfuscation is used, the detection of outproxy traffic is more difficult.

Effectivity
Effectivity is estimated Low. I2P will start to use other outproxy nodes so probably only some nodes will be unavailable.

As the effectivity of the threats is Low, and the simplicity is low, the likelihood is considered Low.

Risk
We consider the likelihood as Low.
The impact is considered Medium.

Table 16 Risk matrix of new unavailability risk

Likelihood impact	Low	Medium	High
High			
Medium	X		
Low			

6.5. New de-anonymization risk.

The new de-anonymization attack possibilities are aimed at the de-anonymization of users and services.

We present an overview of the new de-anonymization risk in the following bow tie diagram.

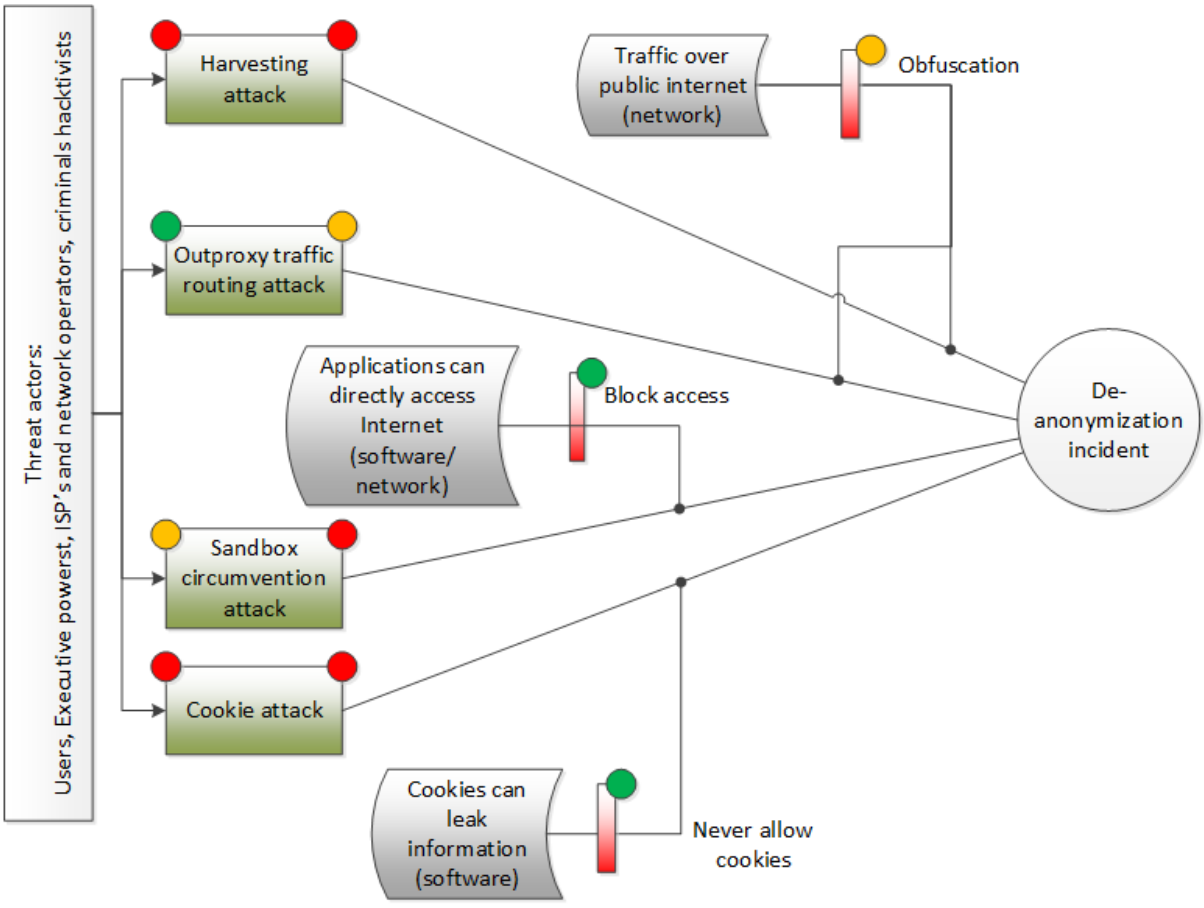

Figure 33 Bow tie diagram of the new de-anonymization risk

Evaluation

Simplicity

The simplicity is estimated as Medium to High. Especially harvesting attacks and cookie attacks are likely to occur.

Simplicity reducing controls:

- Disallowing cookies in the application will prevent a cookie attack.
- Blocking direct Internet access from the computer will prevent sandbox circumvention attacks.

Effectivity

Effectivity is estimated Medium/High.

- For Outproxy unavailability attacks and outproxy traffic routing attacks, obfuscation of the network packets could lower the effectivity.

As the Effectivity of the threats is Medium/High, and the most dangerous attack, the harvesting attack is not influenced by the controls, the likelihood of a successful attack is considered High.

Risk

We consider the likelihood as High.

The impact is considered High.

Table 17 Risk matrix of new de-anonymization risk

Likelihood impact	Low	Medium	High
High			X
Medium			
Low			

6.6. Result overview

We will give a short overview of the results of the risk assessment, first we present all the attack groups with their calculated risks, and then by combining the results in one risk matrix.

Table 18 Overview of attack group per risk level

Risk	Code	Name
High		
	SU	Service unavailability attacks
	IH	Information Harvesting attacks
	S	Sybil attacks
	ND	New de-anonymization attacks
	A	Application abuse attacks
	L	Legal existence attacks
	M	Metadata analysis attacks
Medium		
	T	Traffic analysis attacks
	O	Out-of-band attacks
	C	Central infrastructure corruption attacks
Low		
	NU	Network unavailability attacks
	NWU	New unavailability attacks

Table 19 Risk matrix of all attack groups

Likelihood / impact	Low	Medium	High
High	**T, C, O**	**L, A, M**	**IH, S, ND**
Medium	**NU, NWU**		**SU**
Low			

As can be seen from the results, there are still 7 attack groups with a high risk for the users. We will explain in more detail in the next chapter for these attack groups which attacks have the highest risk, and we will propose some possible mitigating measures for these attacks.

7. Risk mitigation proposal.

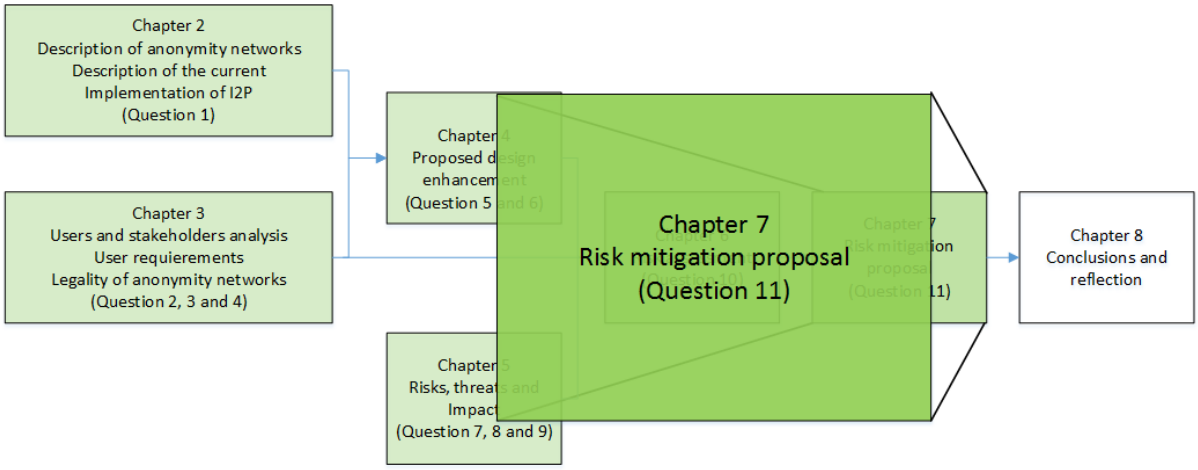

Figure 34 Guidance for chapter 7.

The risk assessment in the previous chapter identified 7 attack groups that have a high risk. These 7 attack groups contain 44 different attacks One attack group is completely reviewed (Legal existence attacks), the other attack groups attribute 8 different attacks. For each of these attack groups we explain in more detail which attacks cause the high risk, and then suggest some mitigating measures for each high-risk attack.
We will separately look into the new risks that are introduced by our proposed design enhancement.

7.1. Service unavailability attacks

The Flooding attack and Eclipse attack are the high-risk attacks from this attack-group. A flooding attack, which is a specialized form of a DDoS attack, is hard to mitigate and mitigation will cost a lot of resources.
The Eclipse attack is dangerous because it makes, in a stealthy way, a service unavailable.

7.1.1. Detailed description flooding attack

A flooding attack is aimed at a specific service. The specific service is known to the adversary by its unique ID (UID). This UID is used to query the netDB and ask for the LeaseSet of the service. This LeaseSet contains the public key of the service, as well as the information where the entry-point of the inbound tunnel(s) of the service are situated.
The adversary then starts sending messages to the endpoints and generate a high load. When this load is high enough, either the service itself or any of the tunnel nodes will overload and stop responding. Then the service is also unavailable to any other node on the network through that tunnel.

The service can build new tunnel and publish new LeaseSets to circumvent this situation, as the I2P node will do anyway because all tunnels are short-lived. However, the adversary knows this is happening so it will keep querying the netDB for the LeaseSets of the service

and, as soon as a new entry-point is published, he will adapt his DoS attack to attack the new entry-point.

7.1.2. Mitigating the flooding attack

The problem with mitigation in this case are the resources needed for this. The adversary can use any computer connected to the Internet to send the packets to the entry-point. He does not need to use I2P nodes, so a distributed DoS attack is easy to start.
To mitigate this attack, not only the service owner, but every tunnel node must be able to survive such a DDoS attack. Only large organizations have the resources and capabilities to survive a DDoS attack. Therefore, we think that mitigation measures must take place at the tunnel entry-points.
When the entry-point starts dropping traffic, the complete tunnel will survive the attack. However, dropping traffic will also mean that the non-DDoS traffic will be dropped, so, the result will be the same: the service is unavailable.
As a mitigation measure, more inbound tunnels can be launched by the service, thus making it more difficult for the adversary to block all tunnels. Especially as the entry point for his inbound tunnels can be located everywhere.

As the mitigation measure will probably only be effective for a small-scale flooding attack and cannot stop a large-scale attack, the likelihood lowers to Medium and consequently the risk drops to Medium.

7.1.3. Detailed description eclipse attack

The eclipse attack is slightly more difficult, but less resources are needed. Also, compared to flooding, it is a stealthier type of attack.
When a service publishes its LeaseSet (the UID for the service as used by others to find the service), this is stored in the netDB.
Each node also stores it RouterInfo in the netDB. The information is stored in the nearest netDB router (floodfill router), based on the UID of the router.
However, a first line of defence is already introduced. Before the UID is stored in the netDB, it is appended with the date, and then hashed, this gives a search-key that is used to find the service. This means that as soon as the date changes, all search-keys change. This means that the nearest floodfill will also change, and for the next 24 hours, a different set of floodfill routers will serve the search-key on the netDB.
So, if an adversary has carefully booted several rogue floodfill routers close to his intended target, after 24 hours he has to reconfigure his rogue routers again.
However, because a fixed appendix is used (the date) it is possible for an adversary to pre-calculate the router keys that he needs for the next period of time, so this line of defence is easily broken.

One of the vulnerabilities is that any node can access the I2P network and become a floodfill router. There is no central authority that can prevent these kinds of nodes to start. Because of the anonymous nature of I2P, it is also not likely that such a central authority will ever be introduced. As no fundamental difference can be seen between an ordinary node and a rogue node, there is no solution to prevent the launching of Sybil nodes.

7.1.4. Mitigating the eclipse attack

We suggest the following measures:
A solution could be to make joining the I2P network for the first time a heavier process, in terms of resources. Thus, making it more difficult to calculate new UID's and re-joining the network with a new UID. However, joining the network is then made more difficult to any normal user as well, while at the same time for a powerful adversary this might give no problems. This needs more research before a definite choice can be made.

Another solution is that all keys will be appended with *n* different fixed values. This means that for each node *n* different search-keys are generated, which will be served by *n* different sets of floodfill routers. This will at least make it more difficult for an adversary as he needs to introduce *n* times more rogue floodfill servers.

We suggest that a non-fixed value should be appended as well to the UID. It must be "impossible" to pre-calculate this value, so that the adversary is not able to prepare for the near future. This non-fixed value must be accessible by every user, and must not be owned by someone. It was suggested to use a search-result from Google, but this is not feasible as the non-fixed value also needs to be stable for a certain period of time.
We think that using a blockchain for this could solve this problem. A blockchain is not predictable, and the time between "updates" is more or less configurable. One could either use an existing (external) blockchain, or use an I2P specific (internal) blockchain where every node is spending some CPU time for mining. Advantage of an external blockchain is that it is publicly available and already configured. Disadvantage might be that it is not always available for all the users.
Advantage of an internal blockchain is that the configuration can also be managed by I2P. Disadvantage is that it will cost extra CPU time of the nodes, and it might be vulnerable to a powerful adversary that can use his powerful resources to steer the blockchain.

We think that after taking these measures, the likelihood will lower to Medium and consequently the Risk will lower to Medium.

7.2. Legal existence attacks

These attacks are high-risk because they are aimed at the existence of the ANNET. Although the likelihood is Medium, their effect is devastating.

7.2.1. Detailed description legal existence attacks

There is not much known about these attacks. Not even whether these attacks are deliberately aimed at the existence of ANNET's or that the threat for ANNET's is coincidental.
But we see, as already mentioned in the introduction, a trend that governments, in their fight against crime and terrorists, are continuously threatening privacy and anonymity, e.g. [78], [79].
More research into this particular type of threats is necessary.

7.2.2. Mitigating legal existence attacks

Mitigation is only possible in countries with a democratic government where the public opinion can be influenced by a free press.
We doubt whether the privacy protection will survive the pressure from the executive powers.
The Likelihood will stay Medium, the risk is High.

7.3. Sybil attacks

Sybil attacks oppose a high risk because they are very difficult to recognize. More active users on the ANNET have a mitigating effect, because the number of Sybil nodes needs to be higher to gain effect for the adversary. As already stated before, because of the anonymous nature of I2P, it is impossible to prevent an adversary to launch several Sybil nodes.
But the sheer existence of Sybil nodes in itself is not a threat. The Sybil nodes can form the basis of which other attacks can be launched.
The mitigation of Sybil attacks is not a high priority. In our opinion it is more important that mitigation is made for the attacks that are based on the Sybil attack.
The buddy exhaustion attack is the highest risk attack that is based on a Sibyl attack.

7.3.1. Detailed description of the buddy exhaustion attack

An adversary controls many nodes but all of his controlled nodes refuse any tunnel building request which does not completely exist of controlled nodes. A large number of Sybil nodes is needed, but this attack can lead to tunnels that are all based on the adversary controlled Sybil nodes and thus to de-anonymization.

7.3.2. Mitigating buddy exhaustion attacks

Attracting users is one good mitigation measure, as the number of Sybil nodes the adversary needs to launch to start an effective attack, is dependent on the number of active nodes in the network.
Another mitigation measure would be to punish a refused tunnel build request heavier within I2P to prevent that tunnels will be built by using such a node.

When these measures are implemented, we think that the Simplicity stays the same, but the effectivity drops to Low, thus the Likelihood is reduced to Low, and the Risk is consequently reduced to Medium.

7.4. Application abuse attacks

All application abuse attacks are high-risk, this is inherent with the design of computers and Operating Systems. Once a user has logged in to his system, all information on this system is available to him, and to the applications he starts. Whenever an application can connect to the Internet, all local information can be sent through.
Cookie attacks can be stopped completely by not allowing cookies.
Software abuse can be stopped by Sandboxing, and protocol abuse by careful selection of the allowed protocols. However, a combination of software abuse and protocol abuse is still possible.

7.4.1. Detailed description of combining software abuse and protocol abuse attacks.

When an installed application is using an allowed protocol, it can still send information to the public Internet. When a user allows a piece of software to run on his node, the possibility exists that this will happen. It can be done by a special piece of software, designed by an adversary to send this information to his own services. But it could also be the result of an ordinary application. We can think of several applications that check their server for updates, and with their update information can leak enough information about the node to de-anonymize a node.

7.4.2. Mitigating a combined attack

However, when enough nodes are using the outproxy functionality together with sandboxing, and as long as the packets sent from the outproxy node to the public Internet are not recognizable as I2P packets, the service receiving information from a node will not know that the information was sent through I2P. He might receive some personal information, but he cannot discover from which node this is originating. So, the level of de-anonymization is low.

We think that the likelihood of this combined attack will drop to Low when these measures are implemented, and thus the risk drops to Medium.

7.5. Metadata analysis attack

Configuration attacks are still possible, even when sandboxing is used, but the chances that important information is available is reduced. Most information will not lead to de-anonymization. No further measures are needed.
Metadata from published content can be more problematic.

7.5.1. Detailed description of the content attack

Many files which contain data, also contain metadata, which is not always obvious to the user. This can be any type of file, like office documents, pictures, photos and even printed copies of a file.
The metadata can be any type of information, like dates it was created or modified, but also information about the user who created or modified the file, or GPS coordinates where a photo was made, and sometimes hidden codes can be placed in pictures or print-outs (called steganography, as example, see [80]).
When an adversary copies the information from a hidden service including metadata, he can start looking for information that connects the metadata to a specific user.

7.5.2. Mitigating a content attack

Mitigation measures must be taken by the users publishing information. At this moment, the amount of metadata and the different types of adding metadata are so diverse, that not a technical measure can be thought of that can be implemented in I2P and will work as a solution for the different types of content that exist.

We suggest that extra information about metadata attacks, combined with guidelines how to circumvent the dangers, should be made public on the website.
We think that when all the users know about the dangers of Metadata, the effectivity of a content attack will drop to Low, so the likelihood will drop to Low and the risk will be reduced to Medium.

7.6. Information Harvesting attacks

The risk assessment reveals that harvesting attacks can be very dangerous. The risk can be lowered by attracting more users and by limiting the information that can be collected.

7.6.1. Detailed description of the harvesting attack.

Every node that joins the I2P network publishes its RouterInfo. This RouterInfo contains the IP-address and port where to contact the I2P software on the node.
Every service publishes its LeaseSets which contain information about the end-point of their inbound tunnels. As the tunnels expire after ten minutes, every ten minutes a new LeaseSet is published for a destination. The time of ten minutes is chosen as this seems a good value for defence against traffic analyses attacks, while at the same time the performance impact is acceptable.

Based on this information, an adversary can start harvesting all known I2P nodes by reading and querying the netDB for all RouterInfo. This will eventually result in a complete overview of all I2P nodes[35] and their IP addresses and ports.
So, with a regular ping sweep over all these routers, the adversary will know which routers are active at the time, and which ones are not.
At the same time, by collecting the LeaseSets that are published, one can also reveal which services are actively running. By combining this information with the information about active routers, one could reveal a much higher correlation between services and IP-addresses (which are published in the RouterInfo).
Harvesting is a very stealthy way of collecting information. Probably the only thing that a user can notice is that it is somehow pinged by an external computer.

Harvesting can also be used as a basis for, or can be enhanced by, combining it with other attacks. One possible scenario is that after having found a high correlation between a service and some IP-addresses, a flooding attack can be launched against the suspected IP-addresses to strengthen the correlation.

Harvesting is dangerous as well for users living in a country where the use of I2P is illegal. As the executive powers can harvest information and find out which nodes use an IP-address from that country, they can find illegal users.

Our new enhancement makes the risk even higher. As we propose that every active I2P node has to start an inbound Internet tunnel and publish the LeaseSet from that tunnel. This means that a much higher correlation can be found between the public Internet tunnel LeaseSets and the routers that offer this service.

7.6.2. Mitigating a harvesting attack

This extra risk can be mitigated by generating a separate search-key for the Internet tunnels and never use the same search-key as is used for a service.
If we also generate the Internet tunnel search key in a random way, the correlation between router and search-key is only valid for ten minutes, and will only have historical value.
We think that with this extra addition, the use of Internet tunnels will not be vulnerable anymore for an information harvesting attack.

On the other hand, we suppose that by introducing our enhancements, I2P will be attractive for a larger audience, and thereby attract more users. When more users are active on the system, harvesting will create much more data and the chances that a proper correlation is found lowers, thus lowering the risk.

As caused by the anonymous nature of I2P, it is not possible to control who can have access to what information, meaning that all users must have access to all information stored about Routers and Leases. So, it is not possible to prevent harvesting. Any mitigation measure must concentrate on preventing the correlation between Leases and Routers.

We think that sandboxing can be helpful, as this makes the computer-node unreachable via the Internet without passing the I2P software. When the I2P software will only respond to I2P requests, a simple ping sweep has become impossible, and the availability of a service can only be determined by actual passing a request to the service and wait for an answer. This means that much more resources are needed by the adversary.
If the sandboxing is implemented in a separate node, like a raspberry PI, it is even possible that the server node is down, while the separate I2P node is still running. In this case, an adversary will never notice the difference between an available service and the service not being available anymore.

We also suggest that it should be possible for nodes to switch off the publishing of their IP-address to the netDB. This would mean that their node will not contribute to the resources of the I2P network and this might lead to free-riding users. This could be solved by lowering the throughput to nodes without a published RouterInfo. We think that in this way it is possible for users in non-democratic countries to join the network without immediate danger.

We think that after implementing these measures, the effectivity of an attack will drop, and thus, the likelihood of a succeeded attack will drop to Low. The risk is then reduced to Medium.

7.7. New de-anonymization attacks

Harvesting attacks, sandbox circumvention and cookie attacks are the high-risk attacks that are influenced or introduced by our enhancements.
See for the harvesting attacks above in 7.6.
Cookie attacks can be reduced completely by not allowing cookies. However, legitimate websites on the public Internet quite often use cookies to enhance the user experience. So,

the downside of not allowing cookies is sometimes a lower quality of user experience. The user himself must consider this trade-off.

Sandbox circumvention attacks are a new version of application abuse attacks, these attacks try to contact the Internet, without the user knowing that this is happening. See the discussion above in 7.4.

As the new de-anonymization attacks are already reviewed, we will not present them separately in the table and risk matrix.

7.8. Overview

We present the same table and matrix as in 0, but we have adapted it, according to our findings above.

Table 20 Risks for I2P after mitigation measures have been implemented

Risk	Code	Name
High		
	L	Legal existence attacks
Medium		
	T	Traffic analysis attacks
	SU	Service unavailability attacks
	IH	Information Harvesting attacks
	S	Sybil attacks
	M	Metadata analysis attacks
	A	Application abuse attacks
	O	Out-of-band attacks
	C	Central infrastructure corruption attacks
Low		
	NU	Network unavailability attacks
	NWU	New unavailability attacks

Table 21 Risk matrix after mitigating measures have been implemented for High risk attacks

Likelihood impact	Low	Medium	High
High	**T, C, O, S, M, IH, A**	**L**	
Medium	**NU, NWU**	**SU**	
Low			

As can be seen, several High risks have been reduced to Medium risk, but still there is one High risk threat left, the legal existence threat.
One conclusion we can draw at this time, is that it seems that most technical threats can be mitigated, but at this moment the non-technical threats form a much higher risk for the existence of I2P (and other ANNET's, like Tor of Freenet).

Although this results in a better situation than before, we do feel that more research is needed, as even a Medium risk can be too high for some of the users, especially as the Impact can be severe for them.

7.8.1. Some remarks about the number of users

There is a positive influence on the number of users on the anonymity of users. This is the result of two effects:

a. When there are more users, the likelihood that a certain user is attacked is lowered.
b. When there are more users, the effectivity of some attack groups will be lower, and thus the likelihood of a succeeded attack will be lower.

But users must realise that these effects are no protection to a directed attack. If a user or a service attracts the attention of an adversary, and the adversary is determined to de-anonymize the user or service, or make it unavailable, then the increased number of users offers no protection anymore.

7.8.2. Some remarks about I2P and Tor

In chapter 2 we gave a short comparison between I2P and Tor. The most important differences are the circuit based design and centralized infrastructure of Tor versus the message based design of I2P and the decentralized infrastructure with a distributed directory.

We have found no indication that the circuit based or message based design makes a difference in security or anonymity.

The centralized versus decentralized infrastructure however, has a major impact in the types of attacks that can be expected.
The centralized infrastructure of Tor makes it resistant to Sybil attacks and more resilient to information harvesting attacks. This at the cost of more overhead and probably less performance when the user base grows.
The decentralized infrastructure of I2P, and thus the fact that every joining node becomes part of the network, has a positive influence on the performance and makes I2P resistant to central infrastructure attacks. But this comes at the cost of a higher vulnerability to Sybil attacks and information harvesting attacks.

We think that for other attack groups, the vulnerability of both anonymity networks is roughly the same.

The Tor network has the advantage that is has a very large user-base compared to I2P, which lowers the effectivity of many attacks, so the likelihood of a successful attack on a specific user is generally lower than for I2P users.

8. Conclusions and reflection

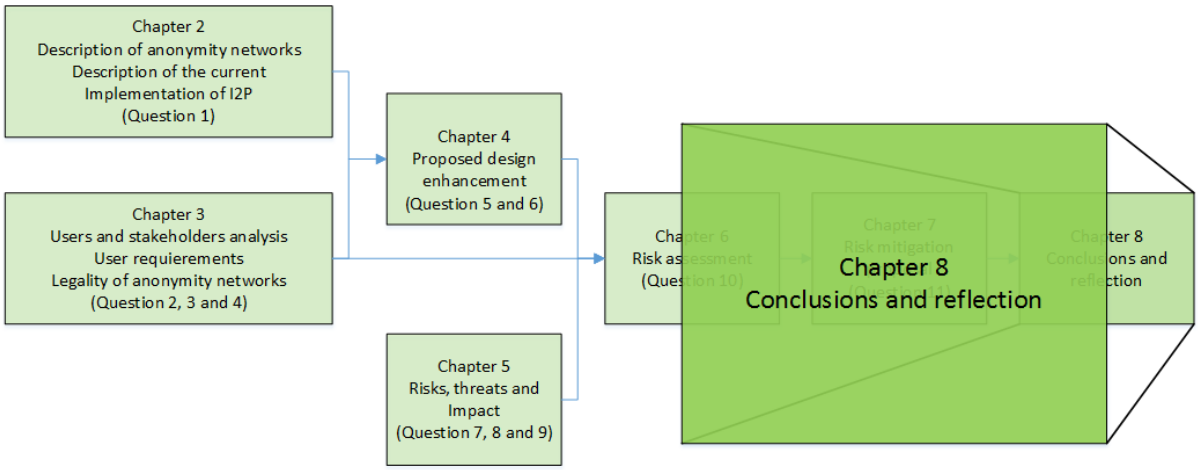

Figure 35 Guidance for chapter 8.

In this chapter, we draw some conclusions from the previous chapters and reflect on the results we have derived in this thesis.

8.1. Conclusions

We look back to the research questions as defined in chapter 1. In this chapter, we stated the main question as:

> "Assuming that I2P will be enhanced to add outproxy functionality to all nodes, in the way as described in this thesis, what are the risks for the anonymity and privacy of the users?"

To answer this question, we started our research with an inventory of the users and other stakeholders from anonymity networks.
This led us to the following conclusions:

- More research is needed into the users of anonymity networks, as, to our knowledge, no research has been done into this subject.
- In Europe and the USA, there are no legal objections to using and supporting an anonymity network, nor is there any legal objection to relaying network traffic for others. Relaying network traffic with illegal content does not make the relaying party responsible for the content.
- In non-democratic countries, using an anonymity network can lead to suspicion by the government and can therefore be dangerous for the users.

We then made a design proposal to enhance I2P to add outproxy functionality to all nodes participating in the network.
After that, we made an inventory of the known threats to availability and anonymity of the users. This was assembled from information from the I2P website and from a literature search. This chapter brought us the following conclusions:

- We had to define our own classification scheme, as no good threat classification was found.

- We had to assemble our own inventory as no source has a complete overview of all possible threats for I2P or any other anonymity network.
- We defined a complete new type of attack group, the legal existence attacks, which is a non-technical attack group.

In the next phase, we made a risk assessment, based on the information we assembled so far. This gave us the following conclusions:

- There are seven attack groups which lead to a high risk for the users. Six of these groups can cause de-anonymization, and one attack group is about service unavailability.

On the basis of these risk assessments, we tried to suggest some possible mitigation measures for the High-risk attack groups, and tried to estimate their influence on the risk. This gave the following results:

- With the implementation of our measures, we can reduce the risk for six out of seven attack groups from High to Medium.
- The only remaining High risk attack is the legal existence attack, which is the only non-technical attack group. The technical attacks can be mitigated, but the highest risk threat for anonymity networks comes from legislative powers.
- The extension of the outproxy functionality, as in our proposed design enhancement, will not lead to a higher risk for the users, we even think that in some cases it lowers the risk for the users.
- When users live in a country where the use of I2P is forbidden, it is impossible for them to use I2P, as their IP-address will be publicly published in the netDB.

So, the final conclusion:

- If we extend I2P with our design enhancement, and we take the measures as defined, the I2P network will be more resilient to de-anonymization and service unavailability then without these measures. Also, if I2P will attract more users this will have a positive influence on the resistance against de-anonymization attacks.

Some other general conclusions:

- The distributed design of I2P makes it resilient to all kinds of central infrastructure attacks, and makes it impossible that some party “owns” the network.
- But this strength is also its weakness, anybody can join the network without hindrances, and the I2P network is therefore vulnerable to many types of Sybil attacks.
- The growth of the number of active users has a positive influence on the anonymity of the users.

8.2. Reflection

At last, we make some remarks about this thesis.

8.2.1. Relevance

This thesis contains several relevant conclusions. Our suggestions for mitigating measures will be relevant for the designers of I2P and will lead to a more anonymous network. Some

of our suggestions may even be relevant for other anonymity networks, as is our threat classification. The thesis is reviewed by two of the I2P developers (ZZZ and Echelon[52],[55]).

8.2.2. Transferability

We think that our work on the threat categorization will be transferable to other anonymity networks, such as Tor.

8.2.3. Contribution to body of knowledge

We presented an overview of users and stakeholders on anonymity networks.
We defined a new classification scheme for threats, which results in 10 attack groups.
We presented a complete overview of the current known threats to I2P.

8.2.4. Future research

More research is needed into the actual users of anonymity networks. We suggested a few typical examples, but more insight into their requirements and behaviour is needed.

More research is needed into attacks on anonymity networks. We were the first ones to present a complete overview of threats for I2P, but this work needs to be extended to other anonymity networks.

More research is needed into the motives of many governments why they propose legislative measures that form a threat to privacy and anonymity, in favour of criminal investigations.

List of tables and figures.

Bibliography

[1] D. L. Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms,” *Commun. ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[2] B. P. Kehoe, “Zen and the art of internet,” *1992*. [Online]. Available: https://www.cs.indiana.edu/docproject/zen/zen-1.0_10.html#SEC91. [Accessed: 06-Jun-2017].

[3] S. M. Bellovin, D. D. Clark, and D. Song, “Global Environment for Network Innovations A Clean-Slate Design for the Next-Generation Secure Internet Status : Final A Clean-Slate Design for the Next-Generation Secure Internet,” no. July, 2005.

[4] A. Gavras, A. Karila, S. Fdida, M. May, and M. Potts, “Future Internet Research and Experimentation: The FIRE Initiative,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 3, pp. 89–92, 2007.

[5] J. Roberts, “The clean-slate approach to future Internet design: A survey of research initiatives,” *Ann. des Telecommun. Telecommun.*, vol. 64, no. 5–6, pp. 271–276, 2009.

[6] R. PAN, J.; PAUL, S.; JAIN, “A Survey of the Research on Future Internet Architectures,” *Commun. Mag. IEEE , [S.l.], v.49, n.7*, no. July, p. p.26–36, 2011.

[7] “Voorstel van wet inzake wijziging Wet op de inlichtingen- en veiligheidsdiensten,” 2016. [Online]. Available: https://www.rijksoverheid.nl/documenten/kamerstukken/2016/10/28/voorstel-van-wet-inzake-wijziging-wet-op-de-inlichtingen-en-veiligheidsdienten.

[8] “Met een sleepnet door het internet op zoek naar terroristen.” [Online]. Available: https://www.nrc.nl/nieuws/2017/02/06/met-een-sleepnet-door-het-internet-op-zoek-naar-terroristen-6580813-a1544813. [Accessed: 14-Apr-2017].

[9] “DUTCH HOUSE OF REPRESENTATIVES PASSES DRAGNET SURVEILLANCE BILL.” [Online]. Available: https://bof.nl/2017/02/16/dutch-house-of-representatives-passes-dragnet-surveillance-bill/. [Accessed: 14-Apr-2017].

[10] “EDRI members.” [Online]. Available: https://edri.org/wp-content/uploads/2013/09/EDRi_member_map-1.png. [Accessed: 14-Apr-2017].

[11] “EFF website.” [Online]. Available: https://www.eff.org. [Accessed: 08-Oct-2017].

[12] “Onion routing, a brief selected history.” [Online]. Available: https://www.onion-router.net/History.html.

[13] “JonDoNym website.” [Online]. Available: https://anonymous-proxy-servers.net/index.html. [Accessed: 14-Apr-2017].

[14] T. W. Clarke, I., Sandberg, O., Wiley, B., and Hong, “A distributed anonymous information storage and retrieval system,” *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2001.

[15] “I2P website.” [Online]. Available: https://geti2p.net. [Accessed: 03-Apr-2017].

[16] “TOR website.” [Online]. Available: https://www.torproject.org. [Accessed: 27-Mar-2017].

[17] “Freenet website.” [Online]. Available: https://freenetproject.org. [Accessed: 02-Apr-2017].

[18] “GNUnet.” [Online]. Available: https://gnunet.org/about%0D. [Accessed: 14-Apr-2017].

[19] “TAHOU-lafs website.” [Online]. Available: https://tahoe-lafs.org/trac/tahoe-lafs. [Accessed: 14-Apr-2017].

[20] “SAFE network website.” [Online]. Available: https://safenetwork.org. [Accessed: 14-Apr-2017].

[21] “Tor users.” [Online]. Available: https://metrics.torproject.org/userstats-relay-country.html. [Accessed: 04-Jul-2017].
[22] B. Conrad and F. Shirazi, “A Survey on Tor and I2P,” *Proc. 9th Int. Conf. Internet Monit. Prot. (ICIMP 2014)*, no. c, pp. 22–28, 2014.
[23] “The Invisible Internet Project (I2P), outproxy.” [Online]. Available: https://geti2p.net. [Accessed: 04-Jul-2017].
[24] “Merriam Webster.” [Online]. Available: https://www.merriam-webster.com/dictionary/anonymity. [Accessed: 23-May-2017].
[25] “Learners Dictionary.” [Online]. Available: http://www.learnersdictionary.com/definition/observation. [Accessed: 04-Jun-2017].
[26] R. Marques and A. Zuquete, “Social networking for anonymous communication systems: A survey,” in *2011 International Conference on Computational Aspects of Social Networks (CASoN)*, 2011, pp. 249–254.
[27] “Anonymizer.” [Online]. Available: https://www.anonymizer.com. [Accessed: 07-Oct-2017].
[28] M. K. M. Reiter and A. D. A. Rubin, “Crowds: Anonymity for web transactions,” *ACM Trans. Inf. Syst. …*, vol. 1, no. 1, pp. 66–92, 1998.
[29] Roger R. Dingledine, “The Free haven project.”
[30] “I2P statistics.” .
[31] B. Zantout and R. A. Haraty, “I2P Data Communication System,” no. c, pp. 401–409, 2011.
[32] M. Herrmann and C. Grothoff, “Privacy-implications of performance-based peer selection by onion-routers: A real-world case study using I2P,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6794 LNCS, pp. 155–174, 2011.
[33] J. P. Timpanaro, I. Chrisment, and O. Festor, “Monitoring the I2P network,” 2011.
[34] IETF, “RFC 6970, Universal Plug and Play (UPnP) Internet Gateway Device - Port Control Protocol Interworking Function.” [Online]. Available: https://tools.ietf.org/html/rfc6970. [Accessed: 18-Dec-2017].
[35] J. S. Peipeng Liua,Lihong Wang, Qingfeng Tan, Quangang Li, Xuebin Wang, “Empirical Measurement and Analysis of I2P routers,” vol. 9, no. 9, pp. 2269–2278, 2014.
[36] J. McLachlan, A. Tran, N. Hopper, and Y. Kim, “Scalable onion routing with torsk,” *Proc. 16th ACM Conf. Comput. Commun. Secur. CCS 09*, p. 590, 2009.
[37] K. Soska and N. Christin, “Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem,” *24th USENIX Secur. Symp.*, no. August, pp. 33–48, 2015.
[38] Z. Spalevic and M. Ilic, “The use of dark Web for the purpose of illegal activity spreading,” *Ekonomika*, vol. 63, no. 1, pp. 73–82, 2017.
[39] T. Van Remunt and J. Van Wilsem, “Wat wordt er nu eigenlijk gezegd? Een verkennend onderzoek naar communicatiepatronen op het Darkweb *,” *Proces*, vol. 95, no. 1, pp. 24–39, 2016.
[40] M. Spitters, S. Verbruggen, and M. Van Staalduinen, “Towards a comprehensive insight into the thematic organization of the tor hidden services,” *Proc. - 2014 IEEE Jt. Intell. Secur. Informatics Conf. JISIC 2014*, no. March, pp. 220–223, 2014.
[41] C. Bösch, B. Erb, F. Kargl, H. Kopp, and S. Pfattheicher, “Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns,” *Proc. Priv. Enhancing Technol.*, vol. 2016, no. 4, pp. 237–254, 2016.

[42] H. Haughey, G. Epiphaniou, and H. M. Al-Khateeb, “Anonymity networks and the fragile cyber ecosystem,” *Netw. Secur.*, vol. 2016, no. 3, pp. 10–18, 2016.
[43] European Union, “Directive on electronic commerce - Directive 2000/31/EC,” *Eur. Union*, vol. L178, no. June, pp. 1–53, 2000.
[44] G. Stobbs, “The Digital Millennium Copyright Act,” *Multimed. Secur. Technol. Digit. Rights Manag.*, vol. 2860, no. 105, pp. 457–482, 2006.
[45] “Tele 2 Terms and conditions.” [Online]. Available: https://www.tele2.nl/wp-content/uploads/2016/11/Tele2-Multimedia-Diensten-vanaf-1-juli-2017.pdf. [Accessed: 28-Sep-2017].
[46] “T-Mobile Terms and conditions.” [Online]. Available: https://www.t-mobile.nl/consumer/media/pdf/voorwaarden/thuis/algemene-voorwaarden-t-mobile-thuis.pdf. [Accessed: 28-Sep-2017].
[47] “Frontier Terms and conditions.” [Online]. Available: https://frontier.com/~/media/corporate/terms/hsi-residential-internet-service-052017.ashx?la=en. [Accessed: 28-Sep-2017].
[48] (Tor project), “Good and Bad ISP’s.” [Online]. Available: https://trac.torproject.org/projects/tor/wiki/doc/GoodBadISPs. [Accessed: 23-Nov-2017].
[49] S. Khattak, D. Fifield, S. Afroz, M. Javed, S. Sundaresan, V. Paxson, S. J. Murdoch, and D. Mccoy, “Do You See What I See: Differential Treatment of Anonymous Users,” *Ndss*, no. February, pp. 21–24, 2016.
[50] “Tor Legal FAQ.” [Online]. Available: https://www.torproject.org/eff/tor-legal-faq.html.en. [Accessed: 28-Sep-2017].
[51] “Tor Abuse templates.” [Online]. Available: https://trac.torproject.org/projects/tor/wiki/doc/TorAbuseTemplates. [Accessed: 28-Sep-2017].
[52] ZZZ, “Review comments from I2P developer ZZZ.” .
[53] ZZZ, “New NetDB entries.” [Online]. Available: https://geti2p.net/spec/proposals/123-new-netdb-entries. [Accessed: 10-Jan-2018].
[54] Subgraph, “Orchid.” [Online]. Available: https://subgraph.com/orchid/index.en.html. [Accessed: 18-Dec-2017].
[55] Echelon, “Review comments from I2P developer Echelon.” .
[56] “Qubes OS.” [Online]. Available: https://www.qubes-os.org. [Accessed: 08-Jan-2018].
[57] R. Dingledine, N. Mathewson, and P. Syverson, “Tor: The Second-Generation Onion Router,” 2004.
[58] C. Egger, J. Schlumberger, C. Kruegel, and G. Vigna, “Practical attacks against the I2P network,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8145 LNCS, pp. 432–451, 2013.
[59] Y. Zhu, X. Fu, R. Bettati, and W. Zhao, “Anonymity analysis of mix networks against flow-correlation attacks,” *GLOBECOM - IEEE Glob. Telecommun. Conf.*, vol. 3, pp. 1801–1805, 2005.
[60] S. Murdoch, “Hot or not: Revealing hidden services by their clock skew,” *Proc. 13th ACM Conf. Comput. …*, pp. 27–36, 2006.
[61] T. (Forbes) Fox-Brewster, “Hackers Hid Backdoor In CCleaner Security App.” [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2017/09/18/ccleaner-cybersecurity-app-infected-with-backdoor/#4b098e2a316a. [Accessed: 28-Oct-2017].
[62] G. N. Tchabe and Y. Xu, “Anonymous Communications : A survey on I2P.”

[63] J. P. Timpanaro, T. Cholez, I. Chrisment, and O. Festor, “Evaluation of the Anonymous I2P Network’s Design Choices Against Performance and Security,” *Icissp*, pp. 46–55, 2015.
[64] M. K. Wright, M. Adler, B. N. Levine, and C. Shields, “Passive-Logging Attacks Against Anonymous Communications Systems,” *ACM Trans. Inf. Syst. Secur.*, vol. 11, no. 2, pp. 1–34, 2008.
[65] E. Hjelmvik and W. John, “Breaking and Improving Protocol Obfuscation,” p. 31, 2010.
[66] Y. Zhu, X. Fu, B. Graham, R. Bettati, and W. Zhao, “On flow correlation attacks and countermeasures in mix networks,” *Priv. Enhancing …*, no. May, pp. 1–17, 2005.
[67] B. Zantout and R. Haraty, “I2P data communication system,” *ICN 2011, Tenth Int. Conf. …*, no. c, pp. 401–409, 2011.
[68] J. Feigenbaum, A. Johnson, and P. Syverson, “Preventing active timing attacks in low-latency anonymous communication: (Extended abstract),” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6205 LNCS, pp. 166–183, 2010.
[69] N. Hopper, E. Y. Vasserman, and E. Chan-TIN, “How much anonymity does network latency leak?,” *ACM Trans. Inf. Syst. Secur.*, vol. 13, no. 2, pp. 1–28, 2010.
[70] G. Danezis, S. J. Murdoch, and G. Danezis, “Low-cost traffic analysis of Tor Low-Cost Traffic Analysis of Tor,” no. November, 2015.
[71] J. R. Douceur, “The Sybil Attack,” pp. 251–260, 2002.
[72] N. Balachandran and S. Sanyal, “A Review of Techniques to Mitigate Sybil Attacks,” *arXiv Prepr. arXiv1207.2617*, pp. 1–6, 2012.
[73] Q. Wang, P. Mittal, and N. Borisov, “In Search of an Anonymous and Secure Lookup Attacks on Structured Peer-to-Peer Anonymous Communication Systems,” *ACM Conf. Comput. Commun. Secur.*, pp. 308–318, 2010.
[74] A. Crenshaw, “Darknets and hidden servers: Identifying the true IP/network identity of I2P service hosts.”
[75] C. Alonso, E. Rando, F. Oca, and A. Guzmán, “Disclosing Private Information from Metadata, hidden info and lost data,” 2009.
[76] International Organization for Standardization, “ISO/IEC 27005:2011,” *Inf. Secur. Risk Manag.*, p. 68, 2011.
[77] International Organization for Standardization, “ISO/IEC 31010:2009 Risk management - Risk assessment techniques,” *Risk Manag.*, vol. 31010, p. 92, 2009.
[78] “Germany, France lobby hard for terror-busting encryption backdoors – Europe seems to agree.” [Online]. Available: https://www.theregister.co.uk/2017/02/28/german_french_ministers_breaking_encryption/. [Accessed: 14-Dec-2017].
[79] “De Maizière will Ausspähen von Privat-Autos, Computern und Smart-TVs ermöglichen.” [Online]. Available: http://www.rnd-news.de/Exklusive-News/Meldungen/November-2017/De-Maiziere-will-Ausspaehen-von-Privat-Autos-Computern-und-Smart-TVs-ermoeglichen. [Accessed: 14-Dec-2017].
[80] “Why printers add secret tracking dots.” [Online]. Available: http://www.bbc.com/future/story/20170607-why-printers-add-secret-tracking-dots. [Accessed: 14-Dec-2017].