Universiteit Leiden

ICT in Business and the Public Sector

The usage of digital platforms to circumvent gatekeeping mechanisms in Africa

Name: Clemens Gonesh
Student-no: s1159291

Date: 23/02/2020

1st supervisor: Mirjam van Reisen
2nd supervisor: Peter van Veen

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

Abstract

Many Eritrean refugees have fled their countries with hopes of reaching Europe and with that a better future. They traverse countries such as Ethiopia, Sudan and Libya ultimately crossing the Mediterranean Sea into Europe. During their journey they face many deceitful situations where barriers are imposed to limit gathering and sending information. This essentially creates a black hole where access to information is very limited and often goes via middlemen. These middlemen can be corrupt which can cause dangers such as human trafficking for ransom. These middlemen can be called gatekeepers as they try to control the information that leaves and enters the refugee communities. Refugees are then the gated. Refugees have however used innovative digital methods to circumvent barriers imposed by these gatekeepers. These barriers can be called gatekeeping mechanisms.

This research aims to explore the digital innovations used by the refugees to circumvent gatekeepers. This extreme situation where gatekeeping mechanisms can be analyzed in near isolation shows the influence of digital communication on the directionality of communication. Network gatekeeping theory is used to see analyze influence of these innovations on the dynamics between gatekeepers and gated. Network gatekeeping theory differs from traditional gatekeeping theory by bringing more focus to the gated. Traditional gatekeeping theory focused on the gatekeeper and usually treated the gated as a passive entity. Network gatekeeping theory expanded the vocabulary of gatekeeping and introduced the concept of gatekeeping salience. Gatekeeping salience describes the power dynamics between gatekeeper and gated through four attributes; political power, information producing capabilities, relationship and alternatives. The attributes possessed by the gated, the higher the salience. The expectation is that digital tools have increased the means which can be used to increase the salience.

This research explores the situation of the Eritrean refugees by using literature research, news articles, online resources and semi structured interviews with resource persons and refugees. The goal was to construct a list of innovations and select a few for further technical analysis. The results have shown that many innovations are used to increase the information producing capabilities of refugees. This is often done through digital services and social media platforms. The results have also shown that governments are the largest type of gatekeepers utilizing surveillance and social media shutdowns to increase their own political power while decreasing that of the refugees. However, refugees and other gated groups try to limit these by using digital tools to circumvent this.

Nevertheless, the exploration of the innovations has shown that digital means can be used to increase the salience. Using these innovations gated can circumvent the gatekeeper and exchange information with other networks of gated. They very much depend on this exchange of information that goes in both directions. Furthermore, other gatekeepers such as activists and journalists that can reach a far larger audience, but also depend on the

information given by these gated. Social capital is needed before this exchange of information happens and this is built by publishing the right information. All of this shows that communication in gatekeeping doesn't follow the traditional top-down directionality where traditional mediums are the only source of information. Communication between gated communities is horizontal and two-way communication. Communication between gated and alternative gatekeepers such as activists is circulatory and both top-down and bottom-up also showing two-way communication. This gives arguments for the expansion of gatekeeping with two-way communication.

Table of Contents

Chapter 1: Introduction

The UN refugee agency estimated that at the end of 2018 there were over 500 000 Eritrean refugees worldwide[1]. Most of the refugees were hosted by Ethiopia and Sudan, but many were also hosted in European countries such as Germany, Switzerland and the Netherlands. In order to reach Europe, these refugees have often travelled through African countries including Ethiopia, Sudan, Egypt and Libya ultimately crossing the Mediterranean Sea into Europe. This is no small journey and information plays a crucial role for many refugees. With this information refugees get to know the latest news, where to go, where not to go, where and how to receive aid and so on. This information is largely obtained through middle men and digital means, depending on the circumstances. Countries in Africa have different infrastructures, different laws and differently equipped refugee camps all influencing the ability to use digital means.

Refugees residing in black holes without (adequate) digital infrastructure are often dependent on middle men while refugees in better connected areas with adequate digital infrastructure do have the option to get information from digital means. However, in both situations there can be acts of gatekeeping impeding the ability of refugees to receive and send information that is very important for their migration. This is even the case when there is an adequate infrastructure for digital communication. However, due to the nature of digital communication it has increasingly become harder for gatekeepers to impede the ability of refugees to obtain and send information. This has however barely been researched. This provides to reason why this paper will be exploring these (digital) gatekeeping mechanisms and how digital means have been utilized by Eritrean refugees to circumvent these mechanisms.

1.1. Problem Statement

Gatekeeping involves controlling the access to information. Gatekeeping has traditionally been very simple before widespread usage of the internet. Information was spread through traditional mediums such as newspapers, television and radio. Gatekeeping mechanisms largely revolved around those mediums where publishing of information was usually done by a central agency or government. These agencies or governments would filter before publishing allowing control over information. With the widespread usage of the internet and more importantly, the widespread usage of social media platforms, these dynamics could have changed.

The internet has enabled many digital innovations. Examples are social media applications and websites used by all ages such as WhatsApp and Facebook. Many social media platforms involve publishing pictures, videos and audio besides text. Essentially the internet

[1] UNHCR, *Global Trends 2018*, (2018), 17, Retrieved January 10, 2020 from https://www.unhcr.org/globaltrends2018/

is a medium that enables doing what newspapers, radio stations and television broadcasting networks can do within a single medium. The only requirement to take part in such media is having a working internet connection. However, getting a working internet connection isn't as simple as it sounds. The realities are often far more complicated.

It has been estimated that there are over 4 billion mobile broadband subscriptions worldwide (United Nations, 2017). But in many African countries the number of individuals using internet is lower than 10% (Broadband Commission, 2018). This includes the countries in Africa where Eritrean refugees travel to such as are Libya, Somalia, Eritrea and Sudan. This is visualized in Figure 1. Africa barely has any presence on the internet.

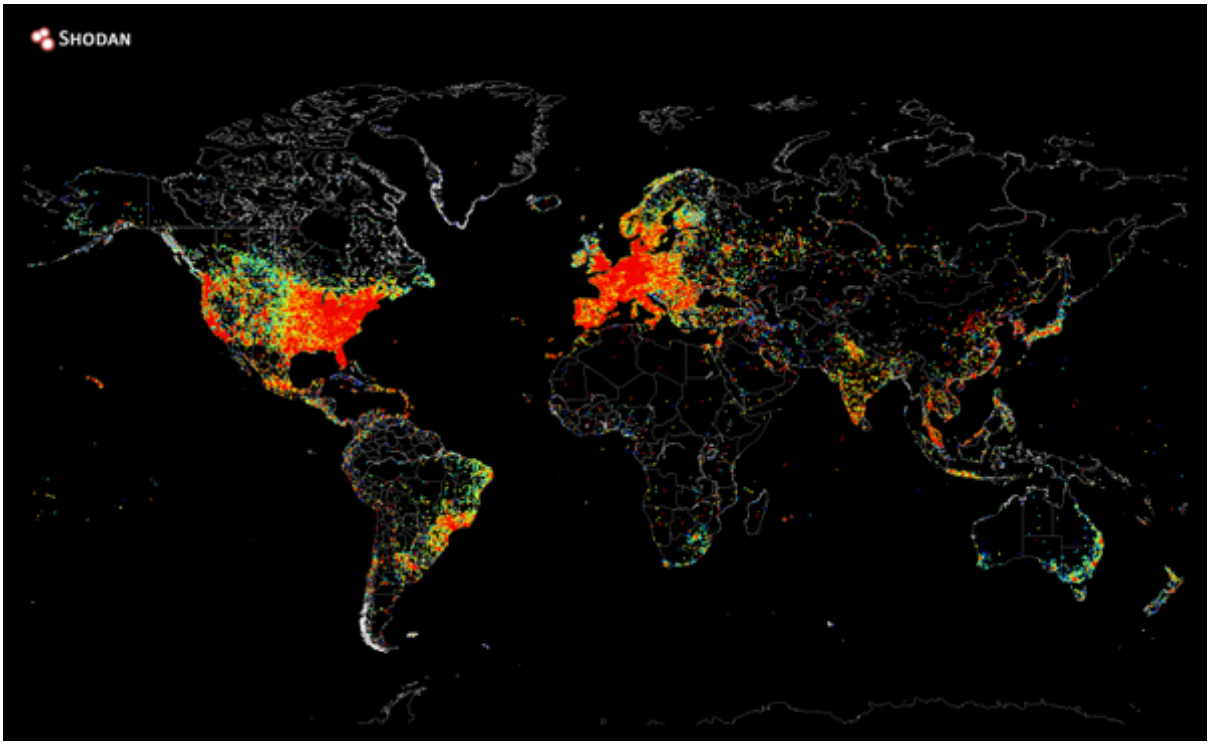

Figure 1: Internet Heat Map[2]

The goal of the Broadband Commission is to promote broadband access in every country[3] (Broadband Commission, 2019). The ultimate goal is to bridge the broadband gap between developed and developing nations and to close the broadband divide between nations. Closing the digital gap might not however not be as simple or even viable. Furthermore, this attempt if not done carefully could have negative consequences that were unforeseen. This is due to historical reasons as explained by fractal theory.

[2] Matherly, J, 28 August 2014, *Internet Heat Map*, Retrieved January 10, 2020, from https://twitter.com/achillean/status/505049645245288448

[3] Broadband Commission, *Focus Areas*, Retrieved January 10, 2020, from https://www.broadbandcommission.org/Pages/default.aspx

1.1.1. Fractal Theory

Fractal theory explains how a slight variation of the starting value can provide very different results (van Reisen M. , 2017). The theory explains how the slightest (historical) differences between nations can have a very large impact on the digital developments of a country. Digital progress of developing nations therefore moves in a very different direction rather than following the trajectory of advanced nations. This is a very important notion as the common (false) idea is that every country develops itself along the same trajectory. Developing nations being behind and developed nations being ahead.

1.1.1.1. Geographical differences between Africa and Europe

An example is given by the uptake of cabled broadband connections. It is very common in Western Europe to have a cabled broadband connection whereas the opposite is true in Africa. There it is more common to have a mobile broadband connection through 3G or 4G. This difference is caused by the historical and geographical differences. From a geographic perspective, Europe is quite densely populated and relatively small whereas Africa is less densely populated but much larger than Europe. It is not hard to see how a broadband connection and even mobile connections will be more expensive in Africa. This geographic difference has been depicted in Figure 2 and Figure 3. Figure 2 shows the map that is often used, heavily shrinking the African continent. Figure 3 depicts a more accurate size for Africa. From this figure it should be clear that having the same amount of coverage as in Europe would be a far more expensive task. The same can be said for electricity which could be the reason that it is often very expensive and inaccessible in Africa. As a result, more power-hungry devices such as desktops and laptops also become more expensive to use.

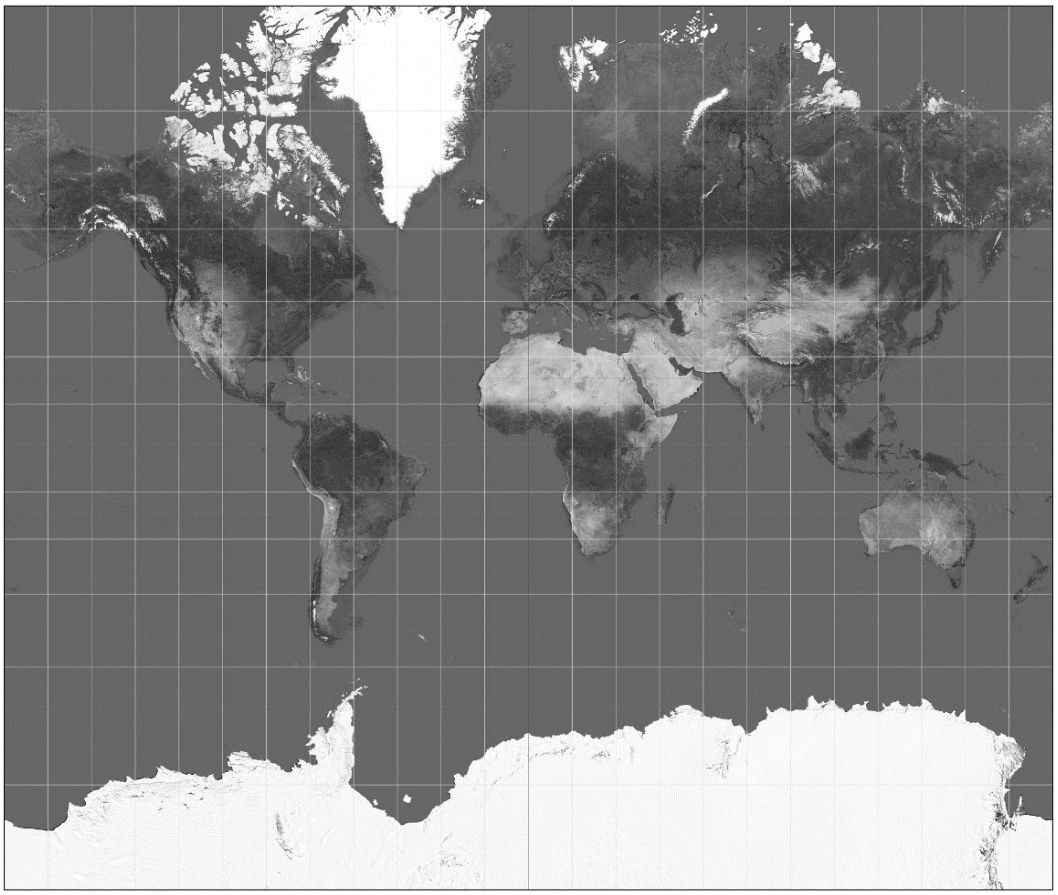

Figure 2: The Mercator map (van Reisen, et al., Black Holes in the Global Digital Landscape: The Fuelling of Human Trafficking on the African Continent, 2019)

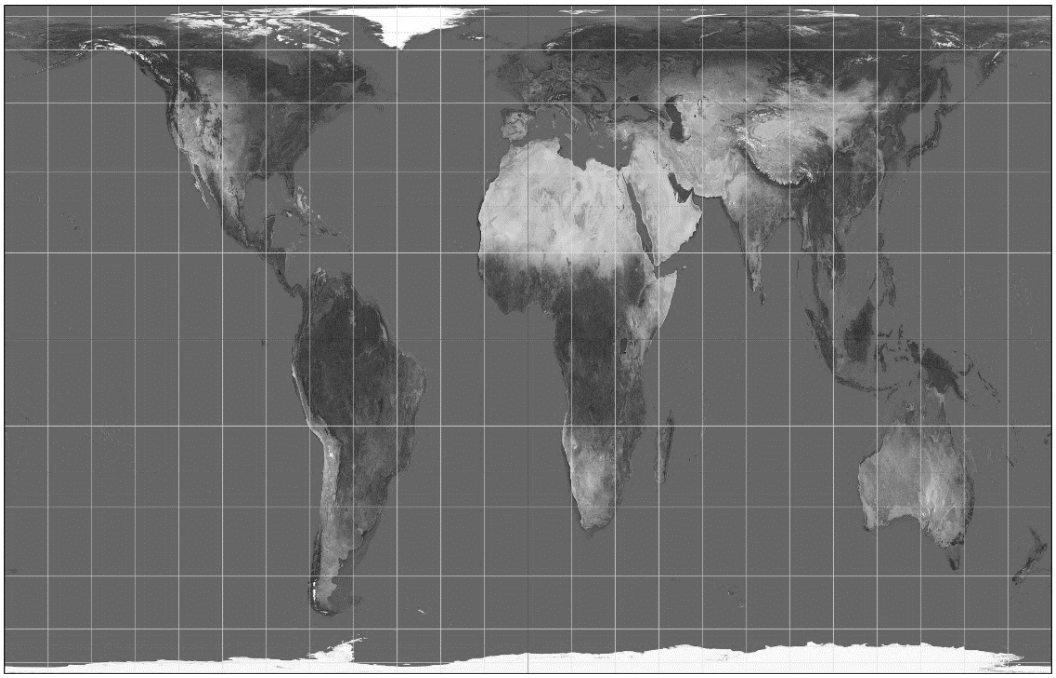

Figure 3: The Gall-Peters map (van Reisen, et al., Black Holes in the Global Digital Landscape: The Fuelling of Human Trafficking on the African Continent, 2019)

1.1.1.2. Societal systems and heritage

Fractal theory also shows how societal systems and the heritage thereof can have an impact on technical systems. The difference between European and African societal systems is explained by the difference paradigm perspectives (van Stam, 2019). African communities often live according to a we-paradigm where the community is put before the individual whereas European communities live according to an I-paradigm where the individual is put before the community. An example is given by the use of remittances by African diaspora which have become a large component of financial aid.

1.1.1.3. Information architecture of the colonial era

Another reason for the difficulty of closing the digital gap is given by the observation that the information network today follows the information architecture of the colonial era (van Reisen, et al., Black Holes in the Global Digital Landscape: Interrogating Human Trafficking Trajectories on the African, 2019). During the colonial era information from colonies were transported towards hegemonic centre of the West. This was done through a system of nodes and trajectories. The nodes were used to filter information whereas the trajectories were used to transport the information. This information was then used by the centre of the West giving them an advantage over the local population in the colonies. This is described by Latour (1987) as a new space-time arrangement. Through the space dimension information and goods could flow towards the West, but not back. Through the time dimension this information could be used by the West to turn into information which could then be used to design projects before the local population in the colonies were involved.

Many colonies have already become independent, but this flow of information and the advantages are still the reality of today. There are more cables connecting western nations than African nations essentially showing the data hotspots. This can be seen in Figure 4. Today the trajectories are those of the physical internet connections rather than ships. Information in the form of data is still transferred out of reach of the local population, namely the data centres in Europe, the US and increasingly China to support their commercial interests. Advantages are obtained through data analysis only increasing the global digital divide and making it harder or even impossible to bridge the gap. The benefits of the internet might therefore be one-sided. This is also shown in Figure 5. The map shows that that Africa is has a smaller population than Europe on the internet despite geographically being larger.

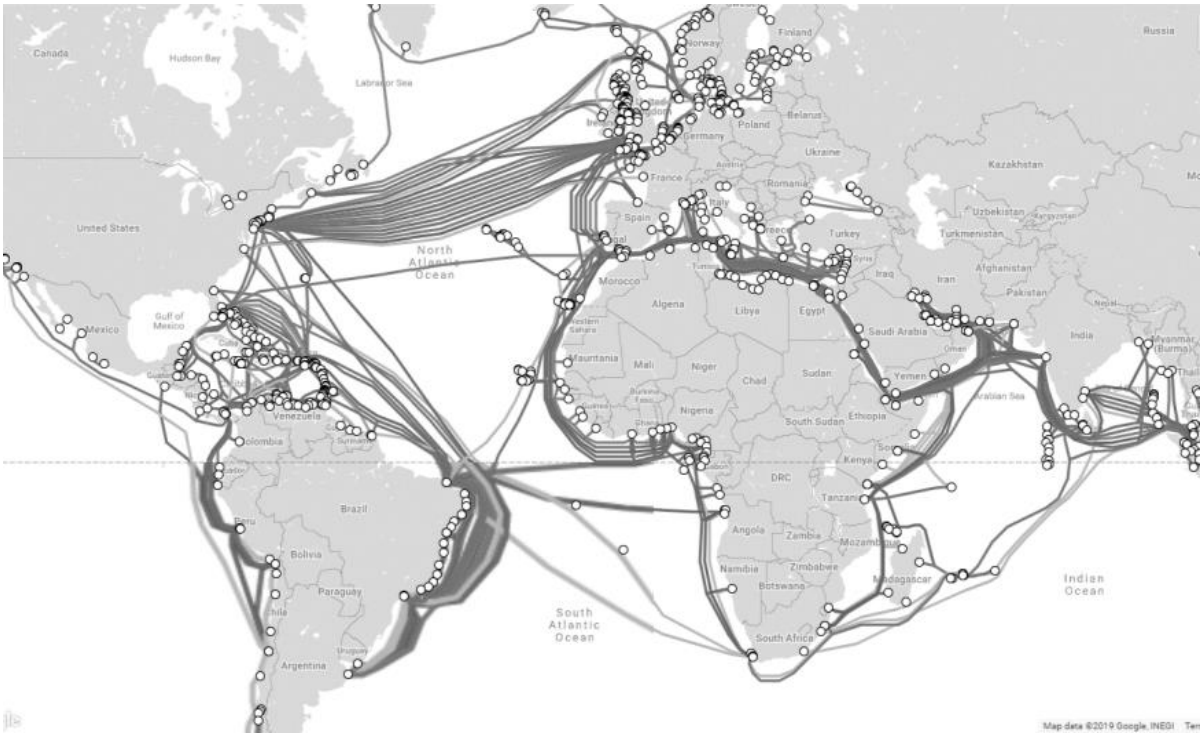

Figure 4: Fiber Optic Submarine Cables (van Reisen, et al., Black Holes in the Global Digital Landscape: The Fuelling of Human Trafficking on the African Continent, 2019)

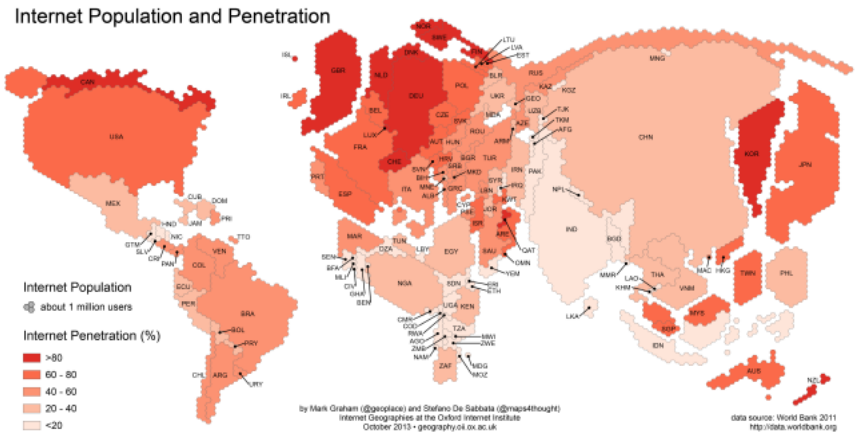

Figure 5: Internet Population and Penetration[4]

The consequence of these realities is that developing nations often have a different architecture of connectivity systems than the West. Sustainable aid should therefore be designed while taking this reality into account. Aid can't consist of plugging in components from the architecture of developed nations into those of developing nations as this will disturb the local balance of systems. Otherwise this can have undesirable consequences.

[4] Desebbata, S., 20 June 2013, *Internet Population and Penetration*, Retrieved from https://stefanodesabbata.com/2013/06/20/internet-population-and-penetration/

1.1.1.4. Human trafficking

A very clear example of this is the usage of ICT to enable human trafficking for ransom. Human trafficking for ransom has emerged in 2009 and was initially identified as 'Sinai trafficking' (van Reisen, et al., 2018). Van Reisen et al. (2018) explain how the expansion of low-cost ICTs have largely enabled human trafficking. Traffickers run their operations using information and networks that have been enabled by ICTs such as mobile phones and mobile transactions. They abuse the situation of the digital divide where they prey on those with less digital capabilities. Many of the victims of human trafficking come from Eritrea where the flow of information is heavily controlled by the government resulting in a black hole. This situation creates a vulnerable group.

1.1.1.5. Black holes and gatekeeping in the information architecture

A black hole is the situation where a local community has no or a weak connection to the information nodes of the information architecture described earlier (van Reisen, et al., Black Holes in the Global Digital Landscape: Interrogating Human Trafficking Trajectories on the African, 2019). This often means that they are excluded from the internet. This has enabled the evolution of another architecture where those residing in a black hole rely on middlemen for information from outside. In the case of refugee these middlemen provide information about where to go for a better future. These middlemen who are active in receiving and passing information can be regarded as gatekeepers (Shoemaker P. , 1991).

Gatekeepers are often seen as a reliable source of information because they are part of the community (Kidane & van Reisen, Collective Trauma from Sinai Trafficking: A Blow to the Fabric of Eritrean Society, 2017). In the case of refugees, these gatekeepers can help to navigate out of the black hole towards more promising nodes. Inside those nodes, there is access to better connectivity which can be used to move further along the network to even better places. This is often done by the youth which also use the nodes to draw support from relatives in diaspora communities during their journey (Dekker & Engbersen, 2013).

Not every middleman or gatekeeper can however be trusted. In the nodes smugglers and human traffickers provide further information about possible destinations and migration routes. This means that those who undertake the journey heavily depend on the information of these gatekeepers in those nodes. This dependency creates the situation where abuse such as extortions, exploitation and corruption of vulnerable groups is possible.

1.1.1.6. Eritrean refugees

These deceitful situations are reality for many Eritrean refugees undertaking the journey towards better nodes (van Reisen, Smits, Stokmans, & Maware, 2019). Van Reisen et al. (2019) describes the difficulties Eritreans endure and explores the role gatekeepers play in this situation. Many Eritrean refugees have fled the country for multiple reasons including

escaping the national service which often could become indefinite (Melicherova, 2019). They rely heavily on gatekeepers of information and these often are smugglers and traffickers. Kidane (2016) shows that the refugee community also heavily relies on social media for information and that the most trusted sources often are relatives. But social media is often inaccessible because use of mobile phones is restricted along the migration route due to technological barriers. Furthermore, the refugees suspect that all phone and internet traffic in Eritrea is being monitored by the government. This causes fear for retaliation against themselves, friends or relatives when communicating. This has created a black hole with severely skewed power relations in favour of the gatekeepers. Gatekeepers often have access to digital means and therefore have more knowledge while refugees only have (limited) access in nodes.

The Eritrean refugees have however sometimes found creative ways to work around the obstructions for digital communication caused by gatekeepers. This provides an interesting new angle and perspective to study gatekeeping. Research about gatekeeping has primarily been conducted from the perspective of the gatekeeper rather than the networks that are gated. No research has been done about circumventing these gatekeepers with digital means, especially not in African context. Researching these digital means can therefore lead to new insight about not only gatekeeping, but also about the information architecture in Africa countries. This information can ultimately be used to find out about the local parameters and equilibrium of the information architecture and how to provide sustainable aid.

1.2. Research objectives and questions

This research will be a case study of gatekeeping in an African context and how digital means are utilized to circumvent gatekeeping. More specifically this research will focus on the Eritrean refugees that travel along the Mediterranean route towards more promising nodes. During their travels they are affected by the many gatekeepers on the route that cause barriers for digital communication. Sometimes these barriers are so severe that it causes a black hole. The refugees have sometimes found creative ways using digital means to circumvent these obstructions. These innovations will be inventoried, categorized according to gatekeeping theory and finally analysed from a technical perspective.

These extreme examples of gatekeeping will provide a different perspective from traditional literature. Gatekeeping has primarily been studied from the perspective of the gatekeeper showing top-down communication from the gatekeeper to the gated. This research will study gatekeeping from the perspective of the gated. Furthermore, this research will also focus on the influence of the new digital means on the communication between gatekeeper and gated. Since social media has made it much simpler to communicate and to retrieve and send information, it is very likely that this communication has altered the balance between gatekeeper and gated.

The primary research question of this case study is:

What digital means for communication are being used by Eritreans to circumvent obstacles caused by gatekeepers?

The sub-questions that follow are:

- What is the context of Eritrean digital communication on the central Mediterranean route towards Europe?
- What kind of gatekeepers and mechanisms are experienced by Eritrean refugees?
- What are the innovations used by Eritrean refugees to circumvent gatekeepers?
- How do these innovations work from a technical perspective?
- Should the concept of gatekeeping be expanded?

1.2.1. Scope

The research will only focus on Eritrean refugees travelling along the Mediterranean route. Countries that have been selected are Ethiopia, Sudan and Libya. The reason is that most Eritrean refugees travel and often reside for a longer period of time in Ethiopia and Sudan. A far smaller number go to other countries such as Kenya and Nigeria. Libya is often where Eritrean refugees embark in order to cross the Mediterranean Sea.

The focus will furthermore only be on digital innovations. It is by no means to be an exhaustive list, but rather a starting inventory of innovations. Due to the time constraints and due to the nature of some innovations there will only be a few that will be explored in depth. Some innovations might need deep technical knowledge while others might need real-time observations in a camp which is not feasible for a thesis. There will also only be a focus on gatekeeping mechanisms that directly influence digital capabilities. Starvation or torturing might be mechanisms but are hardly circumventable by digital means.

1.3. Research Outline

In chapter 2 the theoretical framework will be described. Central is the network gatekeeping theory providing the vocabulary and the four gated attributes which are of importance for this research. Chapter 3 will explain how data about the digital innovations will be gathered and how this data will be analyzed. Chapter 4 will describe the results of the research. These are divided in three sections. The first section discusses the context of the Eritrean digital communication on the central Mediterranean route and Europe using data from the literature, news articles and interviews. The second section will primarily describe the inventory retrieved from literature, news articles and interviews with resource persons. It will also describe the main finding from empirical observations and about digital means used to circumvent gatekeepers. The final section will include a technical analysis of a few technical innovations that have been found. Finally, chapter 7 will discuss the findings and the influence of the innovations on gatekeeping. Chapter 8 will conclude the research and discuss practical recommendations.

Chapter 2: Theoretical Framework of Gatekeeping Theory

In this chapter there will be a discussion of traditional gatekeeping theory and the expansion of Barzilai-Nahon (2009) introducing the concept of network gatekeeping theory. Furthermore, there will be a discussion how this will be used in this research.

2.1. Traditional Literature of Gatekeeping

Gatekeeping has been extensively explored by several disciplines (Barzilai-Nahon, Gatekeeping: A Critical Review, 2009).

2.1.1. Communication theories

Theories have been developed by the communication and journalism fields where gatekeeping is viewed as the process of controlling messages entering the gatekeeper's space. The gatekeepers are treated as a selector that protects the gates. This theory introduces the gatekeeper as the most important filter where their personal control decides what information gets spread. An example is the traditional newspaper editor that rejects an article because he or she personally doesn't like it and/or doesn't see the value. An editor very involved with the environment would for example sooner publish an article about damaging consequences of petrol cars. An editor that also is a car enthusiast might however reject such an article.

2.1.2. Management and technology theories and technology theories

Management theories developed in another direction viewing gatekeepers as those breaking walls and crossing boundaries in order to connect and facilitate (Barzilai-Nahon, Gatekeeping: A Critical Review, 2009). Specialized information is often hard to digest as it requires specialized knowledge. Gatekeepers in such a context are those that are actively involved in knowledge management (Schultze & Boland Jr., 2000). Information that can be retrieved to gain a competitive advantage first needs to be analyzed and digested before it becomes useful. Gatekeepers use their knowledge to select and analyze information to gain a competitive advantage. An example is a market analyst reporting to a CEO what he or she deems most relevant. A more current example would be data scientists using ICT to analyze data. Here again one should decide on the relevancy of information for a report.

2.1.3. Information science theories

Most theories from communication and management fields explore gatekeeping in the context of a profession or organization (Barzilai-Nahon, Gatekeeping: A Critical Review, 2009). Information science also looks at gatekeeping outside of these fields, namely in the community. Theories focus on the identification of gatekeepers and to understand their roles within the community. Other theories primarily look at the gatekeeper fulfilling the information needs and services a community need. Gatekeepers are viewed as agents and much research is primarily done about ethnic communities. Gatekeepers in such a context

are primarily representatives of an ethnic community sending and receiving information from and to the outside world.

2.1.4. Political science theories

Political science theories about gatekeeping have had a very narrow definition (Barzilai-Nahon, Gatekeeping: A Critical Review, 2009). They primarily focused on the political arena, quite literally about the different departments of government where political rivals discuss for example new legislature. Political opponents or allies can release or withhold information whenever it gives them an advantage.

2.1.5. Further advancements

From these theories there have been expansions of gatekeeping and what influences gatekeeping. Shoemaker et al. (2001) have researched what forces determine what becomes news. The research shows how a bigger event is less likely to be filtered by gatekeepers. For example, a person being murdered has a higher chance to become news than a person that was in a minor car accident. This shows the political side of gatekeeping. Livingston and Bennett (2003) show that without many alternatives there is a higher chance of gatekeeping. Much more research has been done about gatekeeping but none of them take the behavior of the gated into account.

2.1.6. Digital advancements

It is very logical that earlier research about gatekeeping didn't focus on the gated. Traditionally one was confined to a few newspapers, radio stations and television broadcasting networks with very limited freedom. There were only a few alternatives and one usually had to pay for them as newspapers weren't free. Furthermore, the barriers for a community to make their own newspaper, radio station or television broadcasting network were very high. One would need a significant amount of finances.

With the internet this has changed. Setting up an own page is very cheap and accessible for many. Furthermore, with social media one can directly reach a massive number of people. A person can now more easily switch from news outlets as it only involves entering another web address or subscribing to another profile or channel. This has changed the dynamics between gatekeeper and gated. The behavior of the gated has become more relevant. This has created a gap in the theory and shows the need for the expansion of gatekeeping theory. This shows the need to research gatekeeping from the perspective of the gated.

2.1.7. Expansion of gatekeeping theory

Barzilai-Nahon (2008) expands the theory of gatekeeping with network gatekeeping theory covering this gap and allowing the analysis of gatekeeping from the perspective of the gated. This is done by a formalization of the definition of gatekeeper and introducing new

constructs allowing for the inclusion of more types of information handling including digital ones.

In her research, Barzilai-Nahon (2008) answers two central questions. The first question concerns the definition of the key constructs network gatekeepers, network gatekeeping, gated and the mechanisms used by network gatekeepers. The second question concerns the identification of network gated and their salience to gatekeepers. This salience is measured by four attributes which will be discussed in further detail in this chapter. These four attributes are hardly static due to the evolvement of these attributes (Barzilai-Nahon, 2009). Network gatekeeping theory can be used to explain these dynamic situations.

2.2. Network gatekeeping theory

Barzilai-Nahon (2008) suggests that network gatekeeping carries three main purposes for information control: guarding the gate from internal information, guarding the gate from external information, an maintaining the ongoing activities within the network boundaries without disturbance. By guarding the gate, a gatekeeper can decide what information leaves and enters the network.

2.2.1. Key constructs

Key constructs are gate, gated, gatekeeping, network gatekeeper and gatekeeping mechanisms. A *gate* is defined as the entrance to or from a network or its sections. *Gated* are defined as the entity subjected to gatekeeping. Being subject to gatekeeping however does not imply that there are no alternatives or that gatekeeping is being forced upon this entity. *Gatekeeping* is defined as the process of controlling information as it moves through a gate.

A *network gatekeeper* is defined as the entity that has the discretion to use gatekeeping mechanisms upon gated. The gatekeeper can also choose the extent of gatekeeping upon the gated. Gatekeepers can be classified through two dimensions: the authority dimension and the functional dimension. The authority dimension represents gatekeepers through the authority scope they have. This can be from micro to macro levels of authority. Functional dimensions reflect the gatekeepers' roles in context of the gatekeeping they exercise. These could be formal and professional designations and positions.

Gatekeeping mechanisms are defined as tools, technologies or methodologies used to carry out the process of gatekeeping. These mechanisms are used to control information. This in turn dictates the interactions between gated and gatekeepers. These key constructs provide a vocabulary upon which network gatekeeping theory can be built.

2.2.2. Salience

The second component is network gatekeeping salience (Barzilai-Nahon, 2008). Salience makes it possible to understand the relationship among gatekeepers and between gatekeepers and gated. Four attributes are used to identify gated and their salience to gatekeepers: political power of gated in relation to the gatekeeper, information production abilities of gated, the relationship between the gated and gatekeepers, and the alternatives in the context of gatekeeping. This is visualized in Figure 6. Each attribute will be explained in further detail.

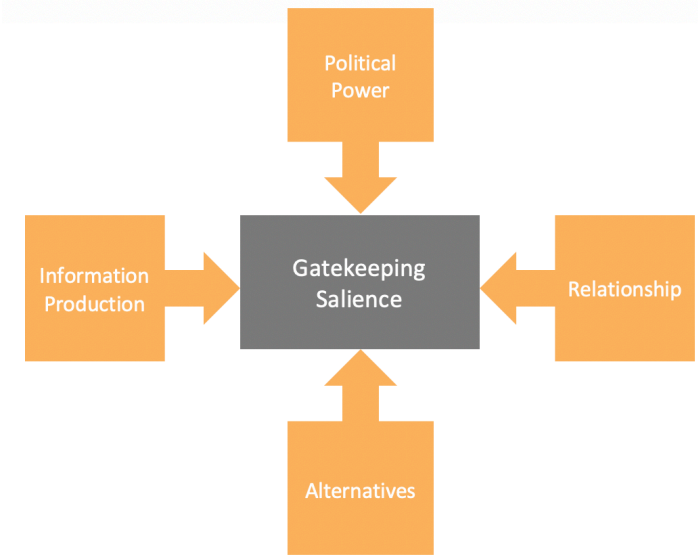

Figure 6: Factors contributing to gatekeeping salience

2.2.2.1. Political Power

Political power has three dimensions (Barzilai-Nahon, 2008). The first dimension involves the ability of one actor to achieve compliance of another actor. This can even be through force. With this ability the actor exerts power to make decisions. The second dimension adds a more subtle definition of power. Decisions are made within a complex situation and in this situation the actor with power also sets the agenda that leads to decisions. They control the context within which the decision is made. The third dimension is even more subtle as it involves the ability to control what another actor thinks shaping and influences one's preferences and awareness. Therefore, political power should be analyzed through decisions, actions and also inactions that influence one's preferences and awareness.

2.2.2.2. Information production

Traditional literature primarily looked at the gatekeeper for information production, but due to the appearance of new methods and technologies this has changed (Barzilai-Nahon, 2008). These new methods and technologies simplify producing information. This empowers and provides the gated with greater autonomy. Technology has also made it easier to spread produced information by for example using social networks.

It should however be noted that these online networks are not as open and democratic as it may seem (Barzilai-Nahon, 2008). Some political, economic and social impediments exist for the gated to reach other users. When using platforms, gated are often still dependent on the gatekeepers' design and policy. Facebook for example still has the authority to enforce censoring rules of governments in each country. Alternatives however provide gated with more power and will be discussed later. Summarized, information production is the process or act of producing content within a network using any multimedia mode.

2.2.2.3. Relationship

Relationship can be examined by different connections (Barzilai-Nahon, 2008). These are direct, reciprocal and enduring contexts. Reciprocity can be researched in different directions including frequency, content, specificity, immediacy, directionality and time or network focus. Other directions are the enduringness and repetition.

Barzilai-Nahon (2008) primarily uses the linkage metaphor projecting on the direct connection between gatekeepers and gated. This emphasizes the enduring relational connection. By having a direct and enduring relationship with a gatekeeper, the gated can negotiate stances. These variables change dynamically as response to events. Having a direct exchange with the gatekeeper enables the gated to change their political power, or the nature of relations with the gatekeeper, and respectively requires attention from gatekeepers.

It should also be noted that the ability of the gated to produce information creates a circulatory effect between gated and gatekeeper. The gated produces information for the gatekeepers while the gatekeepers produce feedback. This feedback is used by the gated and taken into consideration when producing new information. Gatekeepers are also influenced by this information affecting their stances.

2.2.2.4. Alternatives

Alternatives represent an opportunity for gated to decide between two or more courses or propositions (Barzilai-Nahon, 2008). The information economy increased individual autonomy by increasing the things that individuals can do for and by themselves. By providing alternatives for communication that are easily accessible, the autonomy of individuals has grown. This growing autonomy however does not always mean that there is more freedom or power due to the self-regulation of individuals. Another reason is to the strong control of gatekeepers that creates barriers making transferring from one gatekeeper more difficult or even impossible. An example of this is the lack of an alternative for Facebook. An example of self-regulation could be the largest forum that acts as a gateway for information with a strict policy. Although a gated might not agree, they will self-regulate as the access to information is too valuable.

2.2.3. Tiers and classes of gated

Using these attributes, Barzilai-Nahon (2008) created different categories and tiers of gated classes. There are four tiers. Tier 0 represents traditional gated where gated possess none of the attributes and therefore no salience. Tier 1 represents dormant gated classes where gated only possess one attribute. Tier 2 represents potential gated where gated possess combination of two attributes. Tier 3 represents bounded gated where gated possess a combination of three attributes and tier 4 represents challenging gated where the gated possess all attributes. There are several propositions with the main statement being that there is a positive relation to the cumulative number of attributes perceived by the gatekeepers to be present. The more attributes a gated network possesses, the higher to salience towards the gatekeeper. Figure 7 shows the tiers and the class types categorized by Barzilai-Nahon (2009).

	P	I	R	A	Tier	Class type
0					**Tier 0: Traditional Gated** No possession of attributes	Traditional Gated
1			X		**Tier 1: Dormant Gated** possession of one attribute	Captive audience
2		X				Lost voice
3				X		Vagabond reader
4	X					Squanderer Gated
5		X	X		**Tier 2: Potential Gated** possession of two attributes	Exploited apprentice
6			X	X		Demanding user
7	X		X			Potential change agent
8		X		X		Illusive apprentice
9	X	X				Empowered Gated
10	X			X		Vagabond user
11		X	X	X	**Tier 3: Bounded gated** possession of three attributes	Frustrated Gated
12	X		X	X		Influence-Bounded Gated
13	X	X	X			Choice-Bounded Gated
14	X	X		X		Threatening Gated
15	X	X	X	X	**Tier 4: Challenging Gated** possession of four attributes	Challenging Gated

P = political power; I = information production; R = relationship; A = alternatives.

Figure 7: Gated typology (Barzilai-Nahon, Gatekeeping: A Critical Review, 2009)

2.3. Gatekeeping in Virtual Communities

Barzilai-Nahon (2006) used network gatekeeping theory to analyze power interactions between various stakeholders in virtual communities. There are four hubs of stakeholders through which gatekeeping is exercised. Formal regulators, infrastructure regulators, community managers and finally members of the communities. Formal regulators can be any constitutional body, such as the nation state. Laws can prohibit certain activities such as sharing material that is copyrighted. Infrastructure regulators consist of infrastructure providers and service providers. The paper focused on service providers that are responsible for hosting a certain forum. Community managers are those who are responsible for the daily operations of the community.

2.3.1. Tools

The main tools that gatekeepers used are censorship-, editorial-, channeling-, security-, localization-, infrastructure- and regulation mechanisms. The paper focused on information control that is being exercised commonly by community managers. Community managers use tools, technologies and methodologies to delete filter, block or zone content or users. This research primarily looked at what factors may affect the process of gatekeepers and what explanations there are for gatekeeping in virtual communities.

2.3.2. Findings

The results show that certain types of groups experience more gatekeeping than others. Guests are more prone to experience gatekeeping than regular members. Service providers experience gatekeeping due to differences with community managers that are trying to guard the culture of a community. Community members experienced the least gatekeeping. The results also show that gatekeeping could be more or less strict depending on the subject. The more sensitive, the more likely the usage of gatekeeping mechanisms.

The results furthermore show that the history of users also influence the decision whether to delete a message or not. Users of whom messages got deleted in the past were more likely to be censored in the future. The results also show that a user that has not exposed his or her gender is more likely to experience gatekeeping. Additionally, women were more likely to experience gatekeeping than men. Anonymity might seem like it gives users discretion, but the research shows how online permanent members develop familiarity and kinship with other members of the community, despite not using real names.

The research also shows how a gatekeeper can become one of the gated due to exchanging roles of stakeholders. One example is given by commercial information or advertisements. If it is deemed damaging for the community, a gatekeeper might filter this. However, there are differences among gatekeepers and also between the gatekeeper and the community causing the message to be deleted. Community managers play a large role in gatekeeping. They wield a lot of power that can be used to protect as well as harm the gated community. If a community manager can gain personally at the cost of harming the community, the community can get harmed due to members looking for alternatives.

Finally, the research shows the importance of social capital. Cyberspace offers users the opportunity to affiliate with preferred communities. This allows marginalized groups to feel more inclusive. In turn they are more inclined to create a strong social capital and communal core. These two attributes enable them to resist attacks on their communities. Communities with strong social capital and communitarian feelings may become very homogeneous regarding ideas and expressions while oppressing alternatives.

2.4. Gated Eritrean refugees

Van Reisen et al. (2019) have performed a global analysis of the general situation in and around Eritrea using the concept of network gatekeeping theory.

Citizens of Eritrea are classified as traditionally gated (van Reisen et al., 2019). Due to the strict regime, they have no political power. There is no free press and low connectivity limiting their information producing- and distribution abilities. There are no alternatives as the government controls nearly everything including the infrastructure. The government has a monopoly through Eritel.

On the migration route Eritreans are still classified as traditionally gated. Eritreans logically have no political power abroad. To obtain information refugees have to rely on middlemen which can be smugglers or human traffickers. They can sometimes also rely on smartphones, but due to low connectivity this isn't always possible. Camp officials often lack information to be a proper source. The information that refugees produce in turn is closely controlled and disseminated by the human traffickers to specific audiences. The relationship between refugees and smugglers or human traffickers is very distant. Victims of human trafficking rarely have a face-to-face encounter with the persons on top of the organization. The collection of payments and ransom is done in anonymity.

The political power of human traffickers and smugglers is confirmed due to their use of digital technology. This technology is used to organize and run their operations. Digital technology is used to gather intelligence, to facilitate negotiations, facilitate transactions and to coordinate with local authorities. Even government agents can be involved in this process. Finally, the threat of violence is used to keep control of victims.

2.4.1. Innovations

Eritreans have however used digitals means in order to circumvent many gatekeeping mechanisms. This has enabled them to send and receive information where it was otherwise hardly possible. Furthermore, digital innovations have enabled alternatives from these gatekeepers when it comes to communication. Virtual communities could be very important when using these innovations as social networks are often used to spread information. Due to the anonymity of social networks, it is often difficult to see who can be trusted. This is why social capital and community managers are of importance. In this scenario, gated don’t only receive but also send information. Without trust, a gatekeeper can become gated and this shows the importance to further explore the dynamic between gated and gatekeeper from the perspective of the gated.

2.5. Parameters for analysis

In this research, the innovations will be analyzed using the four attributes by looking how they influence the dynamics between gated and gatekeeper. These attributes are political

power, information production, relationship and alternatives. Directionality of information is also an important factor to determine how an innovation is used. A simple model will be used as described in Table 1.

For each innovation it will be analyzed how this influences the four attributes. This will show if and how the innovation has influenced the gated tier. It is also important to see who has the role of gated and gatekeeper and what the gatekeeping mechanisms are. Furthermore, it will be analyzed in what context the innovation is used. The context is subdivided in several parts. First, it's important to know which demographic group is using the innovation. Second, the economic factors need to be taken into account. What financial resources are needed? Third, the technological factor will provide information about the required ICT resources. Finally, the political context should be taken into account. Many African countries have to deal with media shutdowns and have different laws for online communication.

Table 1: Information analysis model

Attributes	**Description**
Gates	What are the gates
Gatekeeper	Who are the gatekeepers?
Directionality	Gatekeeper to gated and/or gated to gated
Political power	How much political power do the gated and gatekeeper have?
Information production	What possibilities for information production does the gated have?
Relationship	What relationship is there between the gatekeeper and gated?
Alternatives	What alternatives does the gated have?
Context	- Demographic; by whom is the innovation used? - Economical; what resources are needed? - Technological; What IT resources are needed? - Political; how do authorities influence the innovation?

Chapter 3: Methodology

This research will be an ethnographic case study. The primary goal of this research is to find out what digital means for communication are being used by Eritreans to circumvent obstacles caused by gatekeepers. The first part of this research will focus on exploring and describing the context of the Eritrean refugees. This includes the situation in Eritrea and along the Mediterranean migration route. Along this route are many areas with low connectivity resulting in black holes. Gatekeeping should be able to be observed more easily in such a situation. This context has therefore specifically been chosen due to it providing an extreme example of gatekeeping. These extremes have in turn caused Eritreans to innovate in order to deal with gatekeeping in black holes. Researching how these innovations influence the dynamics of gatekeeping gives practical insight on the theory and makes it possible to test whether salience is indeed of importance.

3.1. Context

The first part of this research will focus on the context. The context will be studied using research literature, news articles and open interviews with resource persons. These methods will be used to gather information about black holes. With this a rough outline of gatekeeping attributes will be deduced. To get in touch with other resource persons, the method of snowballing will be used. The interviews are ideally done face to face, but due to the dependency of snowballing and the spread of diaspora, telephone calls and even chat apps can be an option. There has already been research about the situation in Africa regarding Eritrean refugees. However, none focuses on the digital innovations. The studies and articles will however provide valuable information about the context regarding the situations throughout Africa about black holes and human trafficking. Both situations are very relevant to analyze innovations in the context of gatekeeping.

There will also be attention for news, statistics about digital communication and the internet shutdowns that have occurred more recently. Searching for relevant keywords and hashtags on Twitter might provide useful information about the behavior in different situations. Especially with attention for the digital innovations, as it is one of the primary tools for communication and because tweets are publicly available. By manually exploring the tweets that have been published during media shutdowns, insight might be given how digital tools were used during the obstruction. All this information will be used as background for the inventorying of innovations for which interviews and observations will be used.

3.2. Gatekeepers and mechanisms

The study of the context will reveal the difficulties Eritrean refugees could face during their journey. Using this study, it will be possible to identify what kind of gatekeepers and mechanisms are experienced by the gated refugees. From there it will be possible to make

an inventory of different innovations used by Eritrean refugees to circumvent gatekeepers. Previous research, social media, semi structured interviews and observations will be used to find out what innovations there are. Resource persons include those that have experience or are part of the Eritrean community and also those that are familiar with innovations in similar context. The interviews, if done face to face or by telephone, will be about 30-60 minutes long.

3.3. Interviews

The interviews with Eritreans will be very informal due to certain effects that can influence the ecological validity. The famous Milgram experiment shows how cues given by authority figures can influence the behavior of research participants. Participants might perform acts that they would normally never do. In the context of this research, this would lower the validity of the interviews and observations as the behavior would be unnatural. Commonalities such as age, similar backgrounds and similar interests between the researcher and participants will be emphasized to gain trust. This will increase the chance that participants will behave more natural and will more easily reveal the use of digital means for communication. This means that the cues that trigger the usage will be natural. This will ensure ecological validity and due to the environment being the natural one, the representativeness of the research is also ensured, although it only being for Eritrean refugees. Representativeness for refugees in general however is not the intention as this research is merely an exploration. There are no artificial triggers and no lab-like environments.

3.4. Innovations

Using this information, it will be possible to describe the architecture and the applications that are being used and to expand the inventory with newly found innovations. The results don't have to be generalizable due to the explorative goal of this paper. This paper is done rather to proof that such innovations occur in this specific context and to give a rough sketch of their workings, rather than to describe in general what refugees all over the world do.

Data gathering will stop when there is repetition of information. The found innovations are by no means supposed to be exhaustive but due to the limited timespan and resources there will be a limit. Each innovation will be analyzed using the model discussed in the previous chapter. A few digital innovations will be analyzed further. The focus will be on why and how they work. This analysis will be done using articles, documents and guides from internet resources. Ideally, the most diverse innovations will be analyzed. From these findings it will be possible how each of the analyzed innovation influences the dynamics of the four attributes for salience from network gatekeeping theory. This in turn shows what the influence is on the tier level of Eritrean refugees in the different contexts and whether gatekeeping theory needs to be expanded.

3.5. Ethics

The main data gathering methods will be interviews and observations. The interviews will be done with resource persons. The preferred method will be in person, but some might be residing abroad. This means that the interview will be done by phone or by a VoIP service. The preferred method of the participant will be used. The interviews will be semi-structured and will have a duration of 30-60 minutes. Persons will be asked if they want to participate and the identity will be anonymized if required. The resource persons will be researchers, activists and journalists with an expertise in the topic of Eritrea and/or digital communication in Africa. These contacts have been gotten through the supervisor of this thesis. These are individuals that are capable of giving informed consent. It is not expected that there are potential ethical threats during the data collection. However, it will be made clear that if the participant has any concerns during the interview that they can stop at any time. There will also be extra care to omit any traceable information such as names and exact locations if they are mentioned in sensitive situations. Each participant will be given a codename to ensure anonymity and once the interviews have been completed any reference that ties the code to the identify will be destroyed. After the end of the interview it will be explicitly said that the researcher can be contacted at any time would there be any questions or concerns about the interview. Since some interviewees might still be migrating, if needed, it will be made clear that no direct help can be given to the interviewee.

The observations will be done using Eritrean participants residing in the Netherlands. These participants will be approached using connections with contact persons familiar with these communities. The observations will be done in the living places from the participants to ensure they behave as they naturally would. Observations will be made for a period of 2 to 4 weeks. Prior to the observations the researcher will give an introduction, introduce the topic of research and ask for consent for the observations. This briefing has been added to the appendix. Due to the threats from the Eritrean regime everything that can be retraced to an individual will be anonymized. Every participant will be given one or multiple codes ensuring that observations can't be traced. As the goal of the observations is to find new innovations, everything that isn't relevant will be omitted minimizing the risk of identification. After the observations have been concluded, the participants will be debriefed with the information that has been gathered to ensure that they will comfortable or would like to omit certain things to ensure safety.

3.6. Data management

The only person having access to the data is the researcher. Digital information will be stored on the personal computer of the researcher secured by password. A backup will be made using SURFdrive[5] which is used by many researchers due to higher security standards than other cloud services. Once the data has been processed, every raw file will and any file having information connecting the participant to a code will be destroyed.

3.6.1. FAIR

Data such as interview notes and transcriptions will be put in the appendix after being processed to ensure anonymity in certain cases. Afterwards they will be stored on SURFdrive. The raw files such as screenshots or copies will be destroyed. Downloading this entire paper will be the only way to access these notes, while SURFdrive will only be accessible for the researchers and supervisors.

Each interview will be stored in the single file that is this research. A backup of separate will also be kept for 2 years by the researcher but won't be published online. Each interview will be named and maybe even split up if it contains information that could easily be retraceable.

The data will be stored using the standard Microsoft Word format. This can be read by most computers and is therefore sufficient in case it ever needs to be accessed. Tables could also be made using the standard Microsoft Excel format. Reusability will only be ensured trough the previously mentioned methods of storage.

[5] https://www.surf.nl/bewaar-en-deel-je-bestanden-veilig-in-de-cloud-met-surfdrive

Chapter 4: Results

4.1. Context of the Mediterranean Route

The first part of the results will discuss the context along the Mediterranean route. First there will be a discussion of the factors that contribute to a black hole. This is important because these factors lead to an increased reliance on middlemen and therefore create situations where gated have less salience. Afterwards there will be a discussion of the three countries along the major route which are Ethiopia, Sudan and Libya. There will mostly be a focus on digital infrastructure and laws to help assess the digital capabilities of refugees. The influence of the Eritrean diaspora will also be discussed as many refugees in Europe still maintain contact with friends and relatives in Africa and often even provide aid in any manner possible. Finally, there will be a short exploration on Twitter to see in social media can reveal the digital methods refugees use to communicate and what barriers there might be.

4.1.1. Black holes in the digital landscape

One of the factors contributing to black holes is the architecture of the digital landscape. Africa is still very underrepresented as there is very low connectivity compared to Europe, other western nations and China. This underrepresentation is worsened by what is called digital imperialism which involves developing applications according to western perspectives and because of data flowing and staying in the West.

4.1.1.1. Information architecture colonial age

As mentioned in the introduction, the digital landscape of today has inherited the shape from the colonial age (van Reisen, et al., Black Holes in the Global Digital Landscape: Interrogating Human Trafficking Trajectories on the African, 2019). A system of nodes and trajectories were developed, and this system was used by the corporations headquartered in Europe to gather information to improve their business. Information travelled using these nodes and trajectories to be analyzed further. This was done with help of agents deciding what information exactly should reach the European centers. This made them very important gatekeepers of information. This information was then used by the European centers to develop further economic, commercial, political and military actions plans for their colonies. An important note is that the local population had no access to this information that was extracted from them.

4.1.1.2. Information architecture today

The architecture of the internet today follows the same pattern (van Reisen, et al., Black Holes in the Global Digital Landscape: Interrogating Human Trafficking Trajectories on the African, 2019). The difference is that internet cables are used instead of ships. Information now flows through these cables to the west where they are stored in data centers and are inaccessible for the local population. The large digital platforms provided by corporations such as Google, Facebook, Microsoft and Amazon represent centralized information

structures (van Dijck, Poell, & de Waal, 2018). These structures cause the information to flow towards the colonial center where it is processed.

This resemblance of current day digital architecture with that of the colonial era causes the benefits of the internet to be one-sided. Due to the geographic and social realities of African communities, they are unable to use these modern-day technologies in ways to empower the African communities. One of the reasons given by van Reisen et al. (2019) is due to the sheer difference in size between Africa and the West which is often misrepresented on world maps. This has been shown in Figure 3 during the introduction.

These maps often represent Europe's landmass larger than that of Africa, while the real geographical size of Africa is much larger than Europe. This gives one of the fundamental challenges for the implementation of communication infrastructures, particularly if information network density is examined. Latency is a large problem because of the vastness of the African continent. Furthermore, many African nations have to deal with legacy equipment and software. These factors pose a problem and cause the big challenge to properly connect the African communication network to the rest of the world. This absence of connection can be seen by the Facebook nodes in Figure 8 and by the global elite corporate structures in Figure 9.

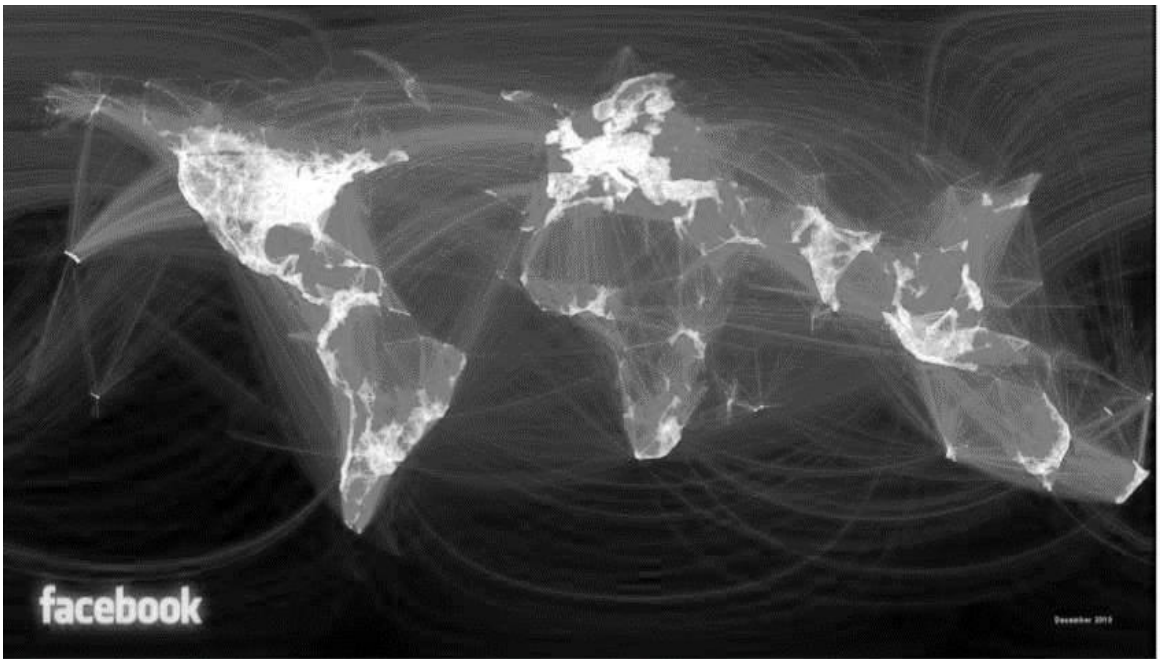

Figure 8: Facebook Nodes (van Reisen, et al., Black Holes in the Global Digital Landscape: Interrogating Human Trafficking Trajectories on the African, 2019)

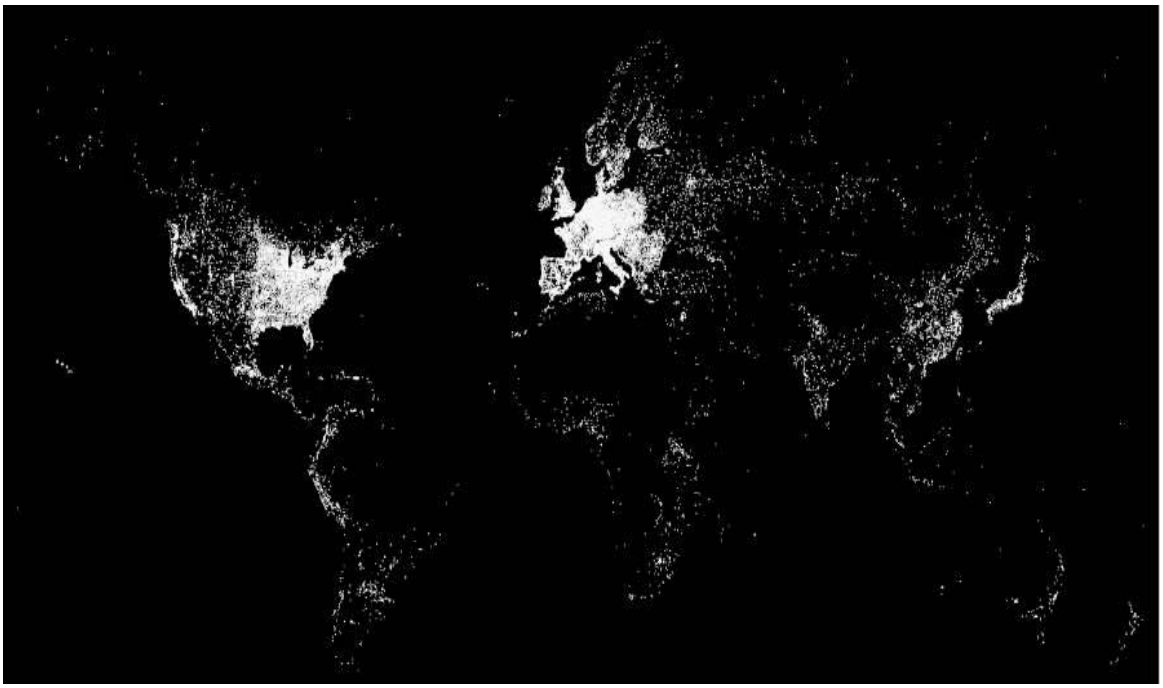

Figure 9: Global Elite Corporate Structures (van Reisen, et al., Black Holes in the Global Digital Landscape: Interrogating Human Trafficking Trajectories on the African, 2019)

4.1.1.3. Imperial perspective to information

The other factor contributing to a black hole is the approach to information. People living in a black hole are seen as objects from which to gather information. This is an imperial perspective. Gathering information is done by monitoring using digital technologies. This one the one hand causes one side to gather and use this information for their own advantage, while the other side is only being used and is at a disadvantage. Communities that produce information are unlikely to use that same information causing a skewed relation in favor of those that are able to use it.

Furthermore, most of the available technologies implicitly incorporate norms, values and ways of doing based on Western epistemology. This essentially can be called digital imperialism where power, authority and influence are extended through digital technologies. This is also depicted in Figure 8 and Figure 9. Everything flows to the hotspots. Solutions given for this imperialism is engineering technologies locally. This will ensure that they reflect the proper local epistemology and serve the local interests.

4.1.1.4. Migration

Van Reisen et al. (2019) argues that this inherent bias of the digital architecture is also inherently potentially harmful regarding irregular migration. Refugees from Africa heavily depend on digital information that is facilitated by smugglers and human traffickers. This is because refugees often reside in black holes of the digital architecture. They have no direct access to relevant information about where to go to increase opportunities and ensure safety.

The middlemen bring filtered information to those wanting to leave bridging the information gap caused by the black hole. The middlemen can therefore be described as gatekeepers.

Gatekeepers use social capital to gain trust of (potential) refugees. They are often part of the community living the black hole and are regarded as a reliable source of information (Kidane & van Reisen, Collective Trauma from Sinai Trafficking: A Blow to the Fabric of Eritrean Society, 2017). The migrants often travel along the trajectories of the information networks towards more promising nodes. In these nodes there are more opportunities. A migrant can prepare and resource their travel along the routes. Greater connectivity along the nodes can be used to draw support of relatives. This support can then be used to move further along to even more promising nodes. During travels however, refugees still come into situations where they must depend on gatekeepers for information. Especially smugglers are traffickers provide information about possible destinations and migration routes. This can unfortunately also provide situations for abuse. These vulnerable situations are arguments for better research of the usage of digital technology in black holes.

4.1.1.5. Empirical observations

Van Reisen et al. (2019) have made several empirical observations about the use of digital technologies in black holes. One example has been observed during a field visit in Masvingo, Zimbabwe. Locals gathered around a building to receive the free Wi-Fi signal of that building. They stood around a fence to pick up the slightest signal. News received through social media was their main source of information.

Extreme poverty is the reason why internet access and even access to electricity is very expensive. Electricity is needed to charge batteries, and this caused charging a phone to be a deliberate action. Sometimes husbands or sons residing abroad in better nodes would provide the families back home with mobile phones and pay for the operating costs. This essentially made them a gatekeeper.

Examples of abuse were also observed by van Reisen et al. (2019). Women in rural villages are vulnerable to grooming through social media as they are desperate for a better future. Another example is the confiscation of phones owned by refugees at gunpoint. This is done to control the flow of information or worse. This leads to vulnerable refugees to be put in deceitful situations with no information on which to base their future actions.

Being entirely dependent on gatekeepers does not provide neutral information. A gatekeeper has their own interest. As has been shown by theory, when there are no alternative sources of information, it enlarges the power of the gatekeeper to determine what information is provided.

4.1.1.6. Summary

Summarized, a black hole is an area where this isn't any connectivity. Factors contributing to black holes are geographical realities of Africa and the digital imperialism. Those residing in such a black hole are dependent on middlemen for information. This makes the middlemen gatekeepers. This establishes a social reality of power relations where the gatekeeper has the upper hand. This shows how the digital architecture has not only created opportunities but also situations where there is in increased dependency on gatekeepers. These situations can cause abuse of gatekeepers towards gated in the form of exploitation, extortion and corruption.

4.1.2. Ethiopia, Sudan and Libya

Ethiopia, Sudan and Libya will be the major focus of this research. These countries are part of the major migration route undertaken by Eritrean refugees. This is shown in Figure 10. A global analysis of the digital architecture will be made for each of these countries. There will be a look at the infrastructure, laws and policies. These factors influence the digital communication. They hardly are exhaustive, but these are major sources that provide a good starting point. This information can be used in the next section to see what gatekeepers and mechanisms refugees experience.

Economist.com

Figure 10: Migration Routes from Eritrea (The Economist, 2017)

4.1.3. Ethiopia

Ethiopia is the neighboring country of Eritrea and lies south of it as shown in Figure 11. The main capital is Addis-Ababa. It counts 105 million inhabitants. Eritrea used to be part of Ethiopia, but Eritrea became independent after a war. Ethiopia and Eritrea have been at war for the majority of time from 1998 till 2018. Recently there have been attempts by the new government of Ethiopia with the leaders of both countries signing the Joint Declaration of Peace and Friendship between Eritrea and Ethiopia (Otieno, 2018).

Figure 11: Ethiopia position[6]

This shared history is probably one of the reasons why most Eritrean refugees remain in Ethiopia. It is one of the first destinations of Eritrean refugees. According to the UNHCR over 160.000 Eritrean refugees reside in Ethiopia. They often stay in refugee camps that aren't adequately equipped and supplied and offer little to no future perspectives (van Reisen & Smits, Inleiding, 2018). This means that refugees can't count on official resources for their wellbeing.

4.1.3.1. Digital architecture

The digital architecture of Ethiopia differs from that of western nations. The penetration of mobile broadband connections is higher than that of wired broadband connections. (Broadband Commission, 2018). 7.1 out of 100 inhabitants make use of mobile broadband connections while only 0.6 out of 100 make use of wired connections. Only 15.4 individuals use the internet. This indicates that inhabitants share internet connections through, for example, public Wi-Fi points or the usage of shared computers in internet cafes.

Ethiopia has a surface area of about 1,104,000 square kilometers and counts about 105 million inhabitants. The GDP lies around 84 billion USD[7]. France has a surface area of about 644,000 square kilometers and counts about 67 million inhabitants. The GDP lies around 2.7

[6] European Comission, 7 August 2019, *Ethiopia*, Retrieved from https://ec.europa.eu/echo/where/africa/ethiopia_en

[7] World Bank, Retrieved 10 January 2020 from https://data.worldbank.org/?locations=ET-FR

trillion. These statistics show the different realities of African and Western-European countries. Ethiopia is twice as large, has nearly double the population, but the GDP isn't twice as large. The GDP of France is over 100 times larger than Ethiopia.

This gives the first reason for a lower penetration of wired broadband connections. Per citizen it is likely more expensive to get a fixed connection as this would need a large amount of cables and electricity. This unaffordability is worsened by the monopoly of the state on internet service (Freedom House, 2018). The state is the sole internet service provider using the organization EthioTelecom. This monopoly has kept the prices artificially high. Recently virtual providers are allowed to operate in an attempt to improve connections with rural areas, but virtual providers are only able to use the EthioTelecom infrastructure (Maasho, 2018). The penetration remains very low in rural areas. Only a handful of signal stations are used to service the entire country. Most Ethiopians can't afford telecommunication devices. This means that it is very hard or even impossible for those in rural areas to get internet at a normal speed. This means that rural areas are very vulnerable to becoming a black hole.

4.1.3.2. Government control on connectivity

The government controls and restricts connectivity using several methods (Freedom House, 2018). Importing of ICT equipment is very strictly regulated using high tariffs and other control measures. Every telecommunication device needs to be registered when a citizen leaves the country via an airport. For cybercafes it is forbidden to offer Voice-over-IP (VoIP) services. Every SIM card needs to be registered before it can be used. This needs to be done with a citizen ID.

Social media and chatting applications have increasingly become popular in Ethiopia. There have however been media shutdowns interfering with the usage of these services. Reasons for media shutdowns are diverse ranging from preventing coup attempts to preventing students from cheating in national exams (Gebre, 2019), (Woodhams, 2019), (NetBlocks, 2019). These media shutdowns are detrimental for local journalists as it limits freedom of press. This is because tools such as chatting applications and social media are inaccessible during such a shutdown. There are also partial blockades where the data connection to such services are throttled making it appear as a malfunction.

The government also targets bloggers to remove politically objectionable content. It is even suspected that they target Facebook pressuring them to remove or block certain posts from political activists. There are also laws limiting freedom of speech online with severe punishments. Examples are content that incite fear, violence, chaos or conflict among people can result in up to three years imprisonment. Another law bans the dissemination of defamatory content which can be penalized with up to 10 years in prison.

4.1.3.3. Summary

Summarized, Ethiopia has relatively low financial resources to invest into their ICT infrastructure. This is probably the cause why mobile broadband connections are more popular and why mobile devices are mostly used to access the internet. Cities are better connected than rural areas. The government has a tight control on the infrastructure through their monopoly and has several laws that restrict what is allowed to be posted online. This limits freedom of speech and freedom of press.

Eritrean refugees mostly reside in rural areas where to connection is very low. These camps are inadequately equipped making it very much harder for refugees. These situations contribute to the factors leading to a black hole.

4.1.4. Sudan

Sudan lies west of Eritrea and shows many similarities in culture. Since the war for independence between Eritrea and Ethiopia, Sudan has been one of the primary locations for Eritrean refugees. According to the UNHCR about 99,000 Eritrean refugees resided in Sudan at the end of 2015 (Crijns, Migratie uit Eritrea, 2018). These are however only the registered refugees. Two out of three refugees don't register and travel directly to the main capital Khartoum. Most refugees reach Sudan via Ethiopia. This is done with help of smugglers or by foot. Ethiopia has a policy where refugees need to stay in camps and if they are detected, they risk getting sent back to the camps.

Figure 12: Sudan position[8]

Some refugees travel to Libya with help of smugglers. Many Eritreans unfortunately get abducted and trafficked before reaching the camps. Even those reaching the camps have to endure several hardships. They still remain under threat of getting abducted because of corrupt local authorities. Furthermore, living conditions are very bad and there is a shortage of food. It is very unsafe and the Eritrean security services are very active. There is also large-scale extortion, intimidation and (sexual) abuse. Refugees are prohibited from leaving the camps. Leaving could result in being deported back to Eritrea. This has been characterized as refoulement which is illegal according to international law.

[8] European Commission, 11 November 2019, *Sudan*, Retrieved from https://ec.europa.eu/echo/where/africa/sudan_en

4.1.4.1. Digital architecture

Citizens of Sudan have to deal with severe economic conditions that limit availability and access to the internet (Freedom House, 2018). One important reason is the severe inflation. This has caused the operating environment for the ICT sector to become more expensive. This has impacted both telecom companies and their subscribers. A month of fixed-line internet costs nearly half of the average monthly income.

Sudan has an even large surface area than Ethiopia with 1,886,000 square kilometers. It counts 40.53 million inhabitants. The GDP of Sudan in 2018 was around 40 billion USD. In 2017 it was 123 billion USD. This shows the rapid economic decline of Sudan. This however does show a similar situation as Ethiopia. Compared to western nations Sudan has to cover a much larger surface area making it very probable that fixed line connections are too large of an investment. This would mean that mobile broadband connections are dominant.

The broadband commission report showed that 0.1 per 100 habitants have a fixed-broadband subscription (Broadband Commission, 2018). This places it lower than Ethiopia. However, 30.5 per 100 habitants have a mobile-broadband subscription. 28 percent of the citizens use the internet. This places the penetration above Ethiopia. This shows that most people are dependent on their mobile subscriptions. A mobile phone subscription for 30GB costs about USD $34. However, it should be noted that because of the high inflation of over 40% that it hard to get the actual costs for internet services. There are additional obstacles for internet due to electricity shortages, especially in major cities. These cities have been subjected to periodic power rationing due to electricity price increases. Most of rural areas have very unsteady or no electricity. Power even gets cut during peak hours.

4.1.4.2. Government control on connectivity

Sudan is directly connected to the global internet through international gateways using five submarine cables (Freedom House, 2018). The government has partial control of the international gateway allowing them to restrict internet connectivity during particular events. There are four licensed telecommunications operators in Sudan, all but one fully owned by foreign corporations. The Sudanese government owns 22 percent of the shares of Sudatel. Mobile corporations are obligated to keep complete records of their customers data. Since 2017 there are mandatory SIM card and phone registrations with national ID. Cybercafes are obligated to download blocking and filtering software to sustain licenses.

The Sudanese government openly blocks and filters websites with content that it considers immoral and blasphemous. The traditional news outlets have had to deal with censorship, confiscations of entire press runs of newspapers and warnings from National Intelligence and Security Services (NISS) agents (Freedom House, 2018). The government is known to actively monitor internet communications on social media platforms and target online activists and journalists during politically sensitive periods. The NISS regularly intercepts

private email messages with sophisticated surveillance technologies. Online news outlets do still cover controversial topics such as corruption and human rights violations.

Sudanese citizens also increasingly rely on online news outlets for their news. Blogging is also popular. Journalists publish anonymously to avoid prosecution. Regular internet users have also become more inclined to self-censorship due to fear of government surveillance and prosecution. WhatsApp is a popular tool to share information due to it using less data. Twitter, WhatsApp and Facebook play a large part as a tool for organizing large scale protests (Freedom House, 2018). Social media also was the main news source for many citizens about the protests with citizen journalists posting videos of police violence and such.

4.1.4.3. Summary

Sudan shows a very similar situation as Ethiopia. Sudan also has relatively low financial resources to invest into their ICT infrastructure. This is probably the cause why mobile broadband connections are more popular and why mostly mobile devices are used to access the internet. Cities are better connected than rural areas. Sudan differs from Ethiopia in the control and prosecution of bloggers and journalists. Sudan is stricter in this regard.

Eritrean refugees must stay in camps or risk getting deported. Camps are often in rural areas which causes refugees to either move to the main capital unregistered or to continue their travels to Libya. This again shows that the factors that contribute to a black hole are present for Sudan.

4.1.5. Libya

Libya is the country from where most of the refugees cross the Mediterranean Sea in order to get into Europe. The situation in Libya is very unstable with multiple parties fighting for control over territories (Human Rights Watch, 2019). This is causing a lot of violence. Libya doesn't have a refugee law or procedure. Eritrean refugees in Libya that try to cross the sea risk getting placed in detention if they get caught. The conditions for those in detention is very inhumane and getting word out of these centers is impossible. The only exception where conditions are slightly better is in the Gathering and Departure Facility (GDF) (UNHCR, 2018).

Figure 13: Libya position[9]

4.1.5.1. Digital architecture

Libya has only two mobile operators, Libyana and Almadar Aljadid. Both companies are state owned. 2.6 per 100 inhabitants have a fixed broadband connection, while 35.4 per 100 have a mobile broadband connection (Broadband Commission, 2018). The situation regarding internet access is very complicated because of the chaos in the country. This has caused all sorts of obstacles for access and furthermore caused violations of user rights (Freedom House, 2018).

In 2017 Libyana deactivated the SIM cards of foreigners showing the power of the provider. In 2015, ISIS also caused disruptions causing mobile and landline service to be distorted in several parts of the country. There have been other power and communication disturbances due to high demand, infrastructure damage, coercion by armed groups and sabotage. The acquisition of SIM cards and mobile phones is relatively easy for citizens as the prices aren't very high.

[9] European Commission, 21 October 2019, *Libya*, Retrieved from https://ec.europa.eu/echo/where/africa/libya_en

4.1.5.2. Government control

There haven't been nationwide blockades (Freedom House, 2018). There have however been blockades for Facebook in several cities including Tripoli in 2018. Partial blockades often are the result of the fighting of rival governments and various militias. Facebook is used by many Libyans as an important news source. It has also been used by activists to organize. Citizens still have to be careful on Facebook because of the chaos in the country. Harassment and threats against journalists and online commentators regularly occur. Many posts are reported by various groups in an attempt to censor. The result is self-censorship. Journalists have faced threats, violence, kidnappings and other forms of violent attacks from militias.

4.1.5.3. Summary

The situation in Libya is very chaotic. There is no real government causing several militias to have their own laws. Internet access is unreliable. Eritrean refugees have to be careful not to get caught by warring militias. Furthermore, the threat of being detained is very severe as it could directly lead to a situation of a black hole.

4.2. Gatekeepers and mechanisms experienced by Eritrean refugees

In the previous section there has been a global analysis of the different situations along the Mediterranean route. In this section there will be an analysis of what gatekeepers and mechanisms were found and their influence on gatekeeping salience. This will be done per country.

4.2.1. Ethiopia

The salience of refugees in Ethiopia is low. They have no political power, no relationship with the gatekeeper and no alternatives. They can however produce information using digital means.

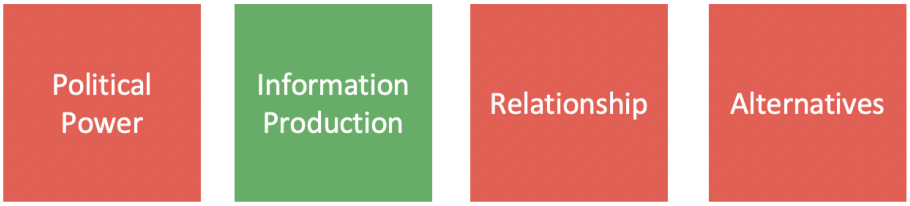

Figure 14: Salience Ethiopia

4.2.1.1. Political power

The laws and penalties for certain content poses a threat for activists and citizens leading to self-censorship. This means that it might be harder for Eritrean refugees, activists and journalists to inform others about camp conditions. It is also difficult for Eritrean refugees to make use of internet services. Due to the mandatory registration SIM cards. It isn't possible to register a SIM card with a refugee ID. Furthermore, such an ID can only be obtained at refugee camps. Many refugees however go directly towards the main capital as registering at a camp can prevent further migration because of the regulations preventing this. Refugees therefore have no political power.

4.2.1.2. Information production

There are several impediments on the production of information. The political impediments are mostly caused by the government. Due to the laws and regulations there is self-censorship of citizens, journalists and activists. Furthermore, due to the pressure on Facebook to remove and block certain posts, information producing capabilities are obstructed. Finally, media shutdowns also cause impediments for information production as websites aren't available. This makes mass communication impossible for all but the government. Journalists could be dependent on bloggers and Facebook posts for information (G. Maunganidze, personal communication, October 15, 2019). Phone calls often do work during a media shutdown, but this can hardly be used to spread news. Media shutdowns are rightly called so because this is exactly what is done. All mass communication methods are immediately rendered useless.

Economic impediments mostly consist of the costs of internet and the availability of internet. The infrastructure of Ethiopia is quite limited resulting in congestion. Furthermore, it lags a generation as it is still using 3G, but 4G might be implemented in the near future (Fick, 2019). This however doesn't change the limited availability in rural areas and might not change the issues of congestion. It also doesn't change the costs which are unaffordable for most refugees. The impediments for Eritrean refugees mostly depend on the place they stay. Internet is better in the main capital, but there are refugee camps in rural areas such as Hitsats. This camp has very bad connectivity (R. Schoenmaeckers, personal communication, September 22, 2019). Electricity is also scarce in rural camps (Dr Kinfe Abraha, personal communication, August 2019).

Social impediments for Eritrean refugees mostly involve the situation in Eritrea of mass surveillance. Even when in Ethiopia, refugees still are afraid of the government listening and often have a habit to avoid this (Dr Kinfe Abraha, personal communication, August 2019). This results in self-censorship and a fear to use digital devices. Furthermore, many are from rural areas and have no digital skill required for the usage of ICT devices.

4.2.1.3. Relationship

The relationship of Ethiopians with the government is quite distant. It mostly has a top down nature where the government is very authoritarian. This is shown by the high number fatalities during protests (Paravicini, 2019).

Eritrean refugees have an even more distant relationship with the government. The government however does provide some resources in order to accommodate refugees. The relationship is mostly built through aid organizations. Refugees can reach these organizations directly in the camps and indirectly through digital means. Digital means are especially useful to reach journalists, activists and friends and family abroad.

4.2.1.4. Alternatives

There are no alternatives to getting internet services due to the monopoly of the government. There aren't any alternatives during a media shutdown either. Furthermore, no real alternative exists for Facebook. There are alternatives to chatting applications such as WhatsApp, IMO, Facebook Messenger and more. Blocking new chatting apps should however be easy for the government. There are no alternatives to registered SIM cards for Eritreans.

4.2.2. Sudan

The salience of refugees in Sudan is low. They have no political power, no relationship with the gatekeeper and no alternatives. They can however produce information using digital means.

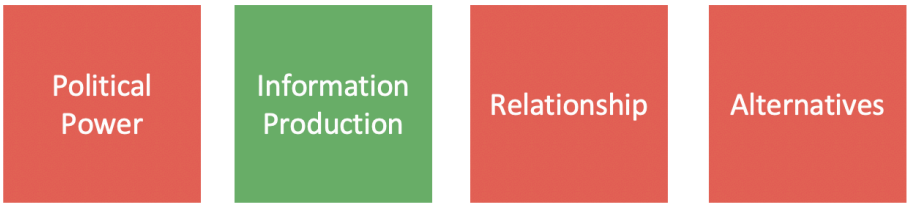

Figure 15: Salience Sudan

4.2.2.1. Political Power

Refugees are very limited due to the laws and regulations in Sudan. Refugees need to stay in camps. Leaving can lead to deportation. In these camps there are often inadequate resources. As a consequence, digital communication is very difficult. Many refugees that enter the country from Ethiopia leave behind their phones. These phones can get confiscated by camp guards in Sudan (Klara Smits, personal communication, August 29, 2019). Furthermore, another obstacle is added due to the recent change that made SIM card registration mandatory. Refugees therefore have very little power.

4.2.2.2. Information Production

Political impediments for information production mostly involve the confiscation of phones by guards in refugee centers. Furthermore, self-censorship occurs because of the tight government control on web content. Journalists also have to be careful making it harder to produce and spread information because of the dangers of the NISS. The government has also shut down the internet during protests adding another obstacle (Human Rights Watch, 2019). Facebook, Twitter, Instagram and WhatsApp have been blocked before obstructing access to information for citizens. This shows the effects of the limits on freedom of speech and press online.

Economical impediments are similar to Ethiopia. Rural areas have limited access to internet and electricity. The costs in the city however seems to be somewhat lower due to higher numbers of penetration for mobile broadband connections. Refugees however face difficulties for getting access to resources. It is unknown how the connectivity in rural areas is, but it is very likely very difficult due to electricity shortages.

4.2.2.3. Relationship

There is no relationship between the government and refugees. The camp officials also have no relationship with the refugees. This lowers the salience of the refugees for the gatekeepers.

4.2.2.4. Alternatives

There are hardly any alternatives to the services being used by Eritrean refugees, especially now that SIM registration has become mandatory. Similar to Ethiopia, no alternatives exist for the social media networks that are used to communicate and retrieve information. Due to the media shutdowns, it is also hard to gain access to chatting apps and social media platforms as there hardly are any alternatives that can't easily be blocked.

4.2.3. Libya

The salience of refugees in Libya is very low. They have no political power, no information producing capabilities, no relationship with the gatekeepers and no alternatives.

Figure 16: Salience Libya

4.2.3.1. Political Power

Eritrean refugees in Libya have no political power due to the nature of the detention centers. The guards in these centers confiscate phones making it impossible for refugees to contact people outside. Furthermore, the different militias prove to be a very real threat and are very unpredictable. Refugees therefore have no political power.

4.2.3.2. Information Production

Due to the lack of resources and devices, it is impossible for refugees to produce information. In the small chance that a refugee can get a phone, there is still fear of surveillance or getting caught. This leads to self-censorship.

4.2.4. Relationship

There is no relationship between the various groups fighting for control in Libya and refugees.

4.2.4.1. Alternatives

Refugees have no alternatives as they forcefully are being detained. They don't have an option at all as there is no access to digital devices.

4.2.5. Diaspora

Eritrean refugees often rely on the diaspora for remittances which is why this group of gatekeepers should also be mentioned. Remittances from the diaspora network play a large role as this is the main income source for refugees. It is very important that remittances can be sent and received. In turn it is very important to have constant communication in order to receive updates about the status of relatives and friends. Since means for communication

and information is retrieved from this network, these relatives and friends can be classified as gatekeepers. The gate is indirect and is a financial gate. Without remittances it would hardly be possible to communicate and retrieve information. The mechanism then is that of providing and withholding remittances and information.

Figure 17: Salience diaspora

4.2.5.1. Political Power

Remittances aren't given without any conditions. Sometimes a relative disagrees with the planned action of a refugee refusing to provide finances. This can influence the decision of a refugee whether to undertake a certain action.

4.2.5.2. Information Production

Without remittances, refugees wouldn't be able to buy phones and data. Through remittances, communities take away some economical barriers which in turn allows a migrating refugee to produce and spread information as well as receive it.

4.2.5.3. Relationship

Eritreans often have a close bond with their families undertaking the journeys. They are often aware due to constant communication. When calling with each other, one often spreads information about what they heard from refugees currently migrating (M., Personal communication, 15 September 2019). This is seen as a moral obligation. Furthermore, like many African cultures, Eritreans live in a we-paradigm. In the we-paradigm community is given primacy over the individual (van Stam, 2019). This means that helping those in the same community will happen a lot faster as it is how one is raised.

4.2.5.4. Alternatives

There are hardly any alternatives to those sending back money. Refugees can't work and obtain money in the mentioned countries and are therefore dependent on diaspora for money. There are however multiple relatives or friends in this network that can provide finances. These can be seen as alternatives.

4.2.6. Summary

The largest gatekeepers are the governments and the camp officials. Refugees officially have to stay in camps where there is hardly any connection. Reason being that these camps are often in rural areas. This can result in congestion when the infrastructure isn't prepared

for this. Furthermore, laws and regulations can increase the severity of an already bad situations. Because of regulations it is very difficult for refugees to obtain SIM cards in both Ethiopia and Sudan. Furthermore, thanks to laws that can cause journalists and activists to be prosecuted there is a lot of self-censorship. Finally, the media shutdowns make it very difficult during political unrest to communicate. These factors contribute to the low connectivity of refugees resulting in black holes. Fortunately, this effect is mitigated by relatives and friends in nodes sending aid either by sending information or by sending remittances.

In general, the refugees have no political power, little information producing capabilities, no relationship with the gatekeepers and have very little alternatives for their digital channels. This means that refugees are traditionally or dormant gated. The mechanisms used by gatekeepers are regulations, laws and media shutdowns limiting the access to digital means.

4.2.8. Exploration of media shutdowns using Twitter

As described earlier, there have been many media shutdowns in all three countries. During such a shutdown there is no incoming and outgoing communication. Sometimes there are ways around these shutdowns if they only partially block access to social media sites. To see what reactions there are on all social media would be out of scope of this research. This is why only Twitter has been researched. The tweets are public making it easier to analyze.

By using Twitter, it will be possible if there is any reaction of citizens, journalists or activists during a media shutdown. This will give insight to how social media is used during such a period. There will be a focus on recent media shutdowns in Ethiopia and Sudan. The most recent media shutdown in Ethiopia was from June 22 to June 28 (Netblocks, 2019). The most recent in Sudan lasted from June 3 to July 9 (Netblocks, 2019).

4.2.8.1. Keywords

For both countries the search will be limited to the periods during the shutdowns. The focus will be on tweets that are about the media shutdown. An appropriate keyword is "media shutdown". A second keyword will be "app", "application", or "Android" since there will be a focus on applications on Android. From there on it is possible to snowball from interesting tweets and accounts containing relevant information about technical workarounds.

4.2.8.2. Results

Searching on Twitter with the keyword "app" and the hashtag "Sudan" with as date between June 3, 2019 and July 9, 2019 revealed tweets mentioning the following apps: Briar, Openobservatory, Socioplanet, Rebtel, Ring Around, Eyewitnessproject and Freech. An interesting hashtag was “internet_blackout_in_sudan". Searching with this hashtag resulted in tweets mentioning more apps, namely Firechat, Hablax, Rebtel and Boss Revolution. Searching for the keyword "VPN" and "hashtag" Sudan revealed that VPN applications are popular during social media shutdowns.

Searching on Twitter with the keyword "app" and the hashtag "Ethiopia" between June 22, 2019 and June 28, 2019 revealed tweets mentioning the Ring Around app and VPN services from Psiphon, Lantern and Tunnelbear.

Searching on Twitter with the keywords "app" and "Eritrea" resulted in tweets mentioning the Ring Around app. Searching with the keywords "Eritrea" and "communication" resulted in tweets mentioning pingo.com, Keku, Boss Revolution, Rebtel and VPN.

This exploration gives an insight about the different kinds of apps used during media shutdowns. Below a table of the found applications or methods and a description:

Table 2: Applications mentioned during media shutdowns

App Name	**Features**
Briar	- Messaging application that works over internet, Bluetooth or WiFi
Open observatory	- Free software detecting censorship, surveillance and traffic manipulation on the internet
Socioplanet	- Social networking and messaging application
Rebtel	- Cheap international calls and unlimited calling
Ring Around	- Cheap international calls and unlimited calling
Eyewitnessproject	- App to record and report human right violations
Freech	- Social networking and messaging application
Firechat	- peer to peer messaging application
Hablax	- Cheap international calls and unlimited calling
Psiphon	- VPN application (bypass blockades)
Lantern	- Proxy application (bypass blockades)
Tunnelbear	- VPN application (bypass blockades)
Pingo.com	- International calling app using VoIP
Keku	- International calling app using VoIP
Boss Revolution	- International calling app using VoIP - Money transferring service

Table 2 by no means represents an extensive list, but it gives a starting point and an indication of the type of apps used. A note that should be made is that the number of tweets about the media shutdown were very limited and mostly came from either journalists or activists. Regular citizens most probably don't use Twitter or even a VPN during a media shutdown. Another note is that most applications are used to bypass blockades and to call using VoIP. The reason most probably being to connect with families and check on them.

4.3. Inventory of innovative methods of digital communication

In this section there will be a description of the found innovative methods. These innovations have been found using Twitter exploration, literature research and interviews. For each innovation there will be a discussion how it influenced the salience between gatekeepers and the gated. A summary is given in Table 3.

Table 3: Innovations and the influence on salience

Innovation	**Influence salience**
Calling 112 during congestion to get internet	+ Information production
Using Psiphon during congestion	+ Information production
Using sharing applications	+ Information production
Using low data alternatives	+ Information production
Sharing credits of phone cards	+ Information production
Using digital money transferring services	+ Information production
Using webmail drafts	+ Information production + Political power
Sending website contents through chatting applications	+ Information production + Alternatives
Black market sim cards	+ Information production
Foreign SIM cards	+ Information production + Alternatives + Political power
Conference calls	+ Information production
Sharing of digital means	+ Information production
VPN	+ Information production
International calling applications	+ Information production + Alternatives
Multiple messaging applications	+ Information production + Alternatives
Deleting messages on chat applications	+ Political power
Using social media to find contact details	+ Information production

4.3.1. Calling 112 during congestion to get connection with internet

This method has been used in Hitsats (Rick Shoenmaeckers, personal communication, 22 September 2019). Hitsats is a rural village with a refugee camp nearby. This camp houses 12,000 to 15,000 refugees. The conditions are very bad. Electricity is very scarce and is being generated using generators running on fuel. Electricity can be accessed through the many outlets connected to the generators against payment. The closest cell tower was in the village and the refugee camp is further removed from the village. There is no direct power line towards the camp. Nearby the camp is an area where NGO's have encampments. Some of these NGO's have Wi-Fi, but the connection is very unstable. The camp itself has no Wi-Fi. It does however get signal from the village through 2G and 3G (H+).

The problem is that making connection to the internet using a smartphone from the camp is hardly possible during daytime. During nighttime it however is. Phone calls using 2G is possible throughout the day and night without any structural issues. The phone needs to be switched from 3G to 2G only using the settings. Screenshots from phones show that there is adequate signal (Schoenmaeckers, 2018).

The local refugees have a method to somehow get a little bit of connection during daytime. To get connection, one uses two smartphones. One phone is running in hotspot mode, allowing the other phone to connect to it. The phone in hotspot modus then repeatedly calls 112 while the other phone tries to load data from the internet by refreshing the Facebook timeline or initiating a call through a messaging application such as IMO or Viber. If a call could be established, it would endure until the end. 112 isn't an emergency number in Ethiopia and therefore it never gets connected. Multiple tries are needed up 20 times before data is loaded. Using this trick, it was possible for refugees to get internet during daytime, essentially circumventing the congestion. Ultimately this enables digital communication allowing refugees to produce information.

4.3.2. Using Psiphon during congestion to get connection with internet

Psiphon is an application that initiates a free VPN connection. It can be downloaded from Google Play. This application has been used in the refugee camp near Hitsats as an alternative to the trick involving calling 112 (Rick Shoenmaeckers, personal communication, 22 September 2019). The refugees connect to the internet using this VPN service tunneling the data from and to the device. The app is officially a circumvention tool in case of social media blockades, but somehow it offers a better connection to those in Hitsats. This also circumvents the congestion during daytime. Ultimately this enables digital communication allowing refugees to produce information.

4.3.3. Sharing applications

Due to the scarcity of electricity and the slow data speed in Hitsats, refugees in the camps have found other ways to download apps. Using sharing applications such as Share.It, C-

Share, All Share and Xender, it has been made possible to get access to the bigger apps (Schoenmaeckers, 2018). Downloading WhatsApp would hardly be possible, but applications can be downloaded and shared through these apps. This enables only a single phone to download the data and then spread it to other devices. This saves data. The applications share the data by establishing a hotspot through which one can send and receive data from phone to phone. This method circumvents the requirement to have a data connection with enough capacity to download applications through Google Play. Doing so increases the information production capabilities as messaging applications can now be used by many more refugees against a cheaper price.

4.3.4. Low data alternatives of applications

Due to the slow data speed in Histats, refugees are more inclined to use low data variants of applications (Schoenmaeckers, 2018). One example is the usage of Opera Mini. Opera Mini compresses data ultimately resulting in less data usage compared to the standard browsers such as the built-in Android browser or Chrome. Another example is the usage of Facebook Lite which uses less data, takes in less size and uses less resources in general. This saves data and battery and ultimately circumvents the requirements of needing enough data and electricity to use the modern web. This increases the information producing capabilities as doing so now requires less data and therefore less money.

4.3.5. Sharing credits of phone cards

Getting prepaid minutes and data is quite difficult for the refugees in Hitsats. Refugees use methods provided by Ethio telecom to circumvent the requirement of having prepaid credits to communicate (Schoenmaeckers, 2018). The first method involves dialing *807*[phone number]#. You enter the phone number that needs to call back. The entered number then receives a text message that informs them that somebody is trying to contact them and to call back to the phone number of the sender.

Another method involves dialing *806*[phone number]*[amount of money]#. Here one enters the phone number of the receiver and the amount of credits that should be sent towards this phone number. This makes it possible to share credits.

Both methods enable the usage of digital communication to produce information.

4.3.6. Using online services to send money

Refugees are very dependent on relatives for money. To send money a person in a node uses services such as Western Union and MoneyGram (D. personal communication, 12 September 2019). Transferring money between Western bank accounts is very easy but sending money to for example Ethiopia is a bit more difficult. One can send money by paying Western Union or MoneyGram and provide them with the details to help identify the

receiver. The receiver can then go to official pick up points of the service and pick up their money.

Money can also be sent using Eritrean middlemen. These middlemen have money in the country of the receiver and offer their services for a price. This allows one to transfer the money without use of a service such as MoneyGram or Western Union. This method is more discrete.

Both methods enable the usage of digital communication to produce information. This is done by financing refugees that can use the money to make use of digital means.

4.3.7. Usage of webmail drafts

The usage of webmail drafts has been used to circumvent surveillance. This method has been recommended by NGO's (Makeda Saba, personal communication, 23 September 2019). This method involves using a webmail client, such as Gmail, Yahoo mail or Outlook. These mail clients allow the use of drafts. Drafts are composed mails that haven't been sent yet to another address. These drafts are often stored in a separate folder. One can communicate using these drafts by writing a draft and leaving it behind on the account. The receiver then logs in and reads the draft and then deletes it. This is done to avoid detection from surveillance of network traffic. Doing so decreases the political power of a gatekeeper as it will be harder to detect and prosecute people. This in turn increases information production capabilities of the gated.

4.3.8. Sending website contents through chatting applications

This method involves copying the text on a website and sending it to a refugee requesting the data (Makeda Saba, personal communication, 23 September 2019). Many modern websites have many modern features and functionalities. These features and functionalities also use a lot of data opposed to simpler websites. This makes it very hard for people in less connected areas with slower data connections to access those websites. This data speed requirement is circumvented by asking a contact in a better-connected area to copy the contents of a website and sending it through a chatting application. This lowers the data requirements to access a website and therefore increases the information producing capabilities and also the alternatives.

4.3.9. Black market or contacts for registered SIM cards

In Ethiopia, Sudan and Libya it is mandatory to register a SIM card before it can be used. This can only be done using a citizen ID. Refugees don't have this ID and therefore can't register SIM cards. To circumvent this requirement refugees often turn to the black market for SIM cards. The SIM cards from the black market are registered under the name of somebody else enabling access to services (H. personal communication, 27 September 2019). There are however issues with these SIM cards. First is that these SIM cards are more

expensive than regular ones. The second issue is that these SIM cards get blocked after a while causing refugees to lose their number and needing to buy another SIM card. Another option to get a SIM card is through friends in the country (Makeda Saba, personal communication, 23 September 2019). These friends can register the SIM card under their name enabling refugees to make use of mobile services. These SIM cards don't get blocked after a while. This enables the production of information.

4.3.10. Foreign SIM cards for messaging applications

The SIM cards bought by refugees on the black market can be blocked at any time. Besides using the black market or friends in the country, another option is the usage of foreign SIM cards for messaging applications (Z, personal communication, 9 October 2019). The SIM cards are from Europe where laws are stricter making it very less likely that a number is going to get blocked. This prevents losing contacts and money. This not only enables digital communication and therefore information production, but also gives alternatives and political power as one is now less dependent on the local network providers.

4.3.11. Conference calls

For a long time, it has been unable for those in Ethiopia to call relatives in Eritrea. This made it difficult for refugees in Ethiopia to communicate with relatives and friends at home in Eritrea. Calling from other countries to Eritrea was possible. This method involves having a third person outside of Eritrea and Ethiopia (D, personal communication, 12 September 2019). This person initiates a conference call with those in Ethiopia and Eritrea essentially acting as a proxy. Using this method, it was possible for those in Ethiopia to reach those back at home. This was done using applications with these functionalities such as WhatsApp or IMO. Whatsapp has only recently added this functionality while IMO has been able to do this for longer. This enabled the gated to produce information and introduced an alternative communication channel.

4.3.12. Sharing of devices and SIM cards

Whenever Eritrean refugees enter another country, they search for fellow Eritreans from the same community (Makeda Saba, personal communication, 23 September 2019). They congregate and often share resources. This includes the SIM cards and smartphones. Whenever a refugee leaves for another country, he leaves behind his device and SIM card which can then be shared with another person entering the country in need of one. This decreases the funds needed to produce information and therefore increases the informatin producing capabilities.

4.3.13. VPN

Ethiopia and Sudan both have had a lot of media shutdowns. During this time, it's nearly impossible to connect to social media platforms. It's also hard to connect to messaging services such as WhatsApp and Facebook Messenger. There are multiple severities of media

shutdowns. One type of media shutdown is the complete shutdown where nothing works. During this type of shutdown, one can't even connect to the web making a VPN unavailable for use. One needs internet connection to connect to a VPN.

There can also be a partial shutdown of social media platforms and messaging applications. These services will be unavailable during the shutdown while other websites are working normally. In this case a VPN can be used to circumvent the blockade and still connect to platforms and applications. But a VPN has limited usefulness because the entire country is affected by the blockade. For journalists this means that even though they might publish stories through a VPN, it won't reach the mass which is the main goal (Golden Maunganidze, 15 October 2019). Furthermore, it is unknown what ISP's do with the usage data and due to the targeting of bloggers and journalists, this would make it dangerous to use a VPN.

Sometimes there is a partial blockade where social media platforms and messaging applications do work, but very slow. This is called throttling. This can also be circumvented using VPN, but people in general are afraid to do so due to fear of surveillance (Golden Maunganidze, 15 October 2019).

The Twitter exploration also revealed that VPN applications are mentioned during the shutdowns, but in general these are free applications and its unknown how many people make use of these applications. In short, while a VPN does take away an impediment for information production, it doesn't remove the political and social impediments of self-censorship and arrests.

4.3.14. Phone applications enabling international calling against lower rates

The Twitter exploration in the previous section revealed how many different phone applications are being used. The popular ones are Ring Around, Rebtel and Boss Revolution.

RingAround App markets itself as the best international calling app for Africa[10]. Using RingAround it's possible for a smartphone user to make international calls over Wi-Fi, 3G/4G and landlines. Users from the same app can call for free with each other over internet. To call to landlines the user has to pay for credits, similar to a prepaid card. Recharging credits can be done using regular online payment methods. Furthermore, the rates for calling are supposed to be lower than using a regular (mobile) provider.

Rebtel is another service with similar features[11]. Features are high quality calls while maintaining low costs. Using this service one can even make subscriptions for unlimited calls to certain countries, such as 12 euros a month for unlimited calls to India. Rebtel claims to optimize international calling by connecting users through local landlines. The service is

[10] Ring Around, 10 January 2020, *Homepage*, Retrieved from https://www.ringaroundapp.com
[11] Rebtel, 10 January 2020, *Homepage*, Retrieved from https://www.rebtel.com/en/

mostly marketed for first-generation migrants that frequently call people from their home country. If the user calls to somebody with Rebtel installed, the call will be free making it cheaper. This differs from WhatsApp as popular messaging apps can't make calls through landlines. Rebtel can also be used to make reverse-charge calls where the person who is called pays for the call.

Boss Revolution is very similar to Rebtel and RingAround. An additional service is sending of money internationally[12]. Furthermore, it's possible to recharge credits of other users. This provides another method of sending remittances and finances communication. First-generation migrants can use this to finance calls for family back home. This ultimately increases the information producing capabilities.

4.3.15. Messaging applications

Eritrean migrants often use many different messaging applications whereas WhatsApp often dominates the Western markets. These applications include WhatsApp, Telegram, Facebook Messenger, IMO, Viber and Signal. There doesn't seem to be a clear reason for this. It could depend on the social environment and what is popular locally (Makeda Saba, personal communication, 23 September 2019). For example, WhatsApp wasn't supported in Hitsats (Schoenmaeckers, 2018).

IMO seems to be very popular, but no reason was given as to why. It has to be noted however that IMO takes far less place than WhatsApp and Facebook Messenger. The installation file of IMO is around 13MB, while WhatsApp takes around 40MB. Furthermore, IMO is more lightweight than WhatsApp enabling it to run on smartphones with lower specifications which are more popular in Africa. Another reason could be due to support for older devices. WhatsApp only supports devices from Android version 4.0.3. IMO might support older devices, but there is no information available about the minimum requirements. IMO did also have support for conference calls before WhatsApp, which might have given it an advantage earlier on while still reaping the benefits now. Furthermore, IMO has the reputation of having a better connection for those with slower internet speed but there is no evidence to back up this claim other than user reviews.

One note to make is that every chatting application constantly releases updates adding functionalities while optimizing existing functionalities. WhatsApp for example didn't support conference calls until 2018. Furthermore, video calling on WhatsApp has become more efficient with data. Due to this fast movement it's hard to compare applications. It's also difficult to see whether applications have been used for historical reasons which are now obsolete. For example, IMO messenger was released as an aggregate for multiple social media platforms such as Skype and Facebook. This functionality has been changed today,

[12] Boss Revolution, 10 January 2020, *Homepage*, Retrieved from https://www.bossrevolution.com/en-us/

but the application has always been lightweight. Facebook only released the Facebook Lite Messenger in 2016, meaning that people that have used IMO for its lightweight might not switch over as their needs has already been met.

In the end these messaging applications give refugees alternatives to better meet their needs and enable refugees to produce information using relatively simple methods.

4.3.16. Deleting WhatsApp messages

One method to avoid surveillance has been the deletion of WhatsApp messages as soon as it was read (Makeda Saba, personal communication, 23 September 2019). This is supposed to avoid surveillance. Using this method, it won't be easily possible to see the communication during a breach of a device. WhatsApp also has the feature of deleting messages for everybody, including the person to whom it was sent but this doesn't work if it's already read. Therefore, it's necessary to delete the message on both devices. This decreases the political power of the gatekeeper as they lose proof for political prosecution.

4.3.17. Using social media to find useful contacts

Many refugees that are migrating get in various deceitful situations. Examples that have been given are the detention camps in Libya and the cases of human trafficking. Another situation is during the crossing of the Mediterranean Sea.

On the one hand the refugees are under threat of the local authorities. On the other hand, the European Union is making efforts to prevent refugees from crossing the sea. This puts refugees in a situation where they can't rely on many people for aid. The only groups remaining are journalists, activists and NGO's.

In deceitful situations, refugees can't rely on any authority to get them out of this. In these cases, refugees often use social media such as Facebook to find activists and journalists that can provide any form of assistance (Cornelia, personal communication, 19 October 2019). Somehow, they are able to get contact details and then start communication with hopes of getting assistance. However, during these conversations' refugees can exaggerate their situation in hope of getting assistance with priority. One always has to be careful of lies and definitely don't make promises (Cornelia, personal communication, 19 October 2019). When refugees then get assistance of anybody, they are sure to spread the story around so that other refugees also know whom to contact. In some cases, refugees memorize and spread phone numbers of certain journalists so that they always know who they can contact (M, personal communication, 14 September 2019). This increases their information producing capabilities as journalists, activists and NGO's can more easily spread information.

4.3.18. Sharing information using the network of communities

Eritreans always share what they know among their communities, it is their moral obligation (M, personal communication, 14 September 2019). Using most of the methods described earlier, Eritreans stay in touch with their communities. Many individuals from these communities share the stories with each other and using this network information gets spread within the community. This combined with the digital communication methods ensures that the community can keep up to date with the latest news. Digital communication in this way has enhanced the communication methods of the communities.

4.4. Technical Analysis

In the previous section there was an inventory of the different methods for communication. Some of these are used specifically due to the situations during the migration towards better nodes. A few of those will be discussed in depth with a technical analysis.

4.4.1. Calling 112

As mentioned in the previous section, this method involves calling 112 in the refugee camp near Hitsats. During the attempt, the user would refresh the Facebook timeline or initiate a call from a messaging app such as IMO or Viber. This call would endure until the connection ended. The exact workings of this method can be revealed by researching the camp conditions and the protocols through which mobile data connections are made. First there will be a look at the camp conditions.

4.4.1.1. Camp conditions

The camp counted over 15,000 refugees. Using internet via an Android smartphone over 3G (HSPA) wasn't able during daytime. It was however usable during nighttime. It was possible to make calls if you switch the mobile connection mode to 2G only in the settings. The nearest cell tower was in the nearby village, but from the screenshots of smartphones of a study about 24COMS it is clear that there were full bars of signal (Schoenmaeckers, 2018, pp. 15-21).

This could indicate that there is congestion. The camp houses about 15,000 refugees nearby a village that is quite small. It is very probable that the mobile network provider didn't account for this camp when setting up the network cell tower. This means that the tower doesn't have enough capacity. From the website of Ethio Telecom it is known that only 2G and 3G connections are available[13]. GPRS is available for mobile internet over 2G while HSPA is available for mobile internet over 3G. 4G has only recently been available in a few big cities. GPRS is too slow for modern websites and applications.

4.4.1.2. Previous research about congestion

Congestion has been researched in a similar scenario where tens of thousands of people were gathered in a relatively small area (Shafiq, et al., 2013). In the research there has been an analysis of congestion and possible solutions were suggested for the providers. The research discusses how cellular network performance degrades during crowded events, what causes this degradation and how they could be mitigated.

Congestion effects can be divided in pre-connection and post-connection phases (Shafiq, et al., 2013). During pre-connection congestion causes connection timeouts and failures. This is because the limited bandwidth of the signaling channel is exhausted when many users try

[13] Ethio Telecom (10 January 2020, *Mobile Internet*, Retrieved from https://www.ethiotelecom.et/mobile-internet/

to acquire radio resources at the same time. These failures are increased by 100-5000 times during congestion compared to routine days, at least in the scenario of the paper. The biggest issue is that there are too many connection requests.

In the post-connection phase, voice network performance degrades causing dropped and blocked calls (Shafiq, et al., 2013). This is 7-30 times worse than on routine days. Furthermore, the packet loss ratio and round-trip time (RTT) degrades causing lower data network performance. Round trip time is the time it takes for a signal or packet to travel from a source to the destination and back again. The degradation was about 1.5-7 times worse than on routine days in the scenario of the paper. The biggest issue here is that there are too many Radio Resource Control (RRC) connections causing the limited radio resources to be exhausted.

4.4.1.3. Radio Resource Control

Looking at the exact workings of mobile networks and the Radio Resource Control (RRC) protocols gives a better idea of what causes congestion. The exact specification for RRC and emergency calls has been recorded in the specifications created by the 3GPP (3GPP, 2019). The 3GPP is a global initiative for creating mobile broadband standards. Members include the Alliance for Telecommunications Industry Solutions (ATIS), the European Telecommunications Standards Institute (ETSI) and China Communications Standards Association (CCSA). As such the biggest manufacturers of mobile devices are a member. This means that it is very likely that all devices conform to these standards, including the standard for emergency calls.

4.4.1.3.1. Cell towers

User equipment (UE) such as a smartphone connects to a network cell tower for internet. This tower has multiple cells that can be connected to for services. There are three types of services offered by cells; limited, normal and operator services (ETSI, 2018, pp. 16-17). Limited services are in case of emergencies on an acceptable cell. Normal services include regular calls and data usage on a suitable cell. Operator services are limited for operators only on a limited cell. Cells are categorized according to which services they offer. Acceptable cells only offer limited services such as emergency calls. Reserved cells offer operator services. Barred cells are not accessible by UE. Suitable cells are used for normal services. Furthermore, there are also distinctions between 2G, 3G and 4G cells. Access to cells can be barred during congestion. This can either be done manually by the provider or could be a built-in feature from the manufacturer. The influence on the 112 method will be discussed later.

4.4.1.3.2. Connecting to a cell tower

When a phone gets powered on it immediately tries to connect to a mobile network through the cell selection and cell reselection procedure (ETSI, 2018, pp. 20-23). The same

happens when switching to a new mobile network by for example travelling or swapping SIM cards. The states and transitions are shown in Figure 18 (ETSI, 2018, p. 20). There are 4 states relevant for this research; “Camped normally”, “Connected mode”, “Camped on any cell” and “Connected mode (Emergency calls only)”. This is shown in Figure 18.

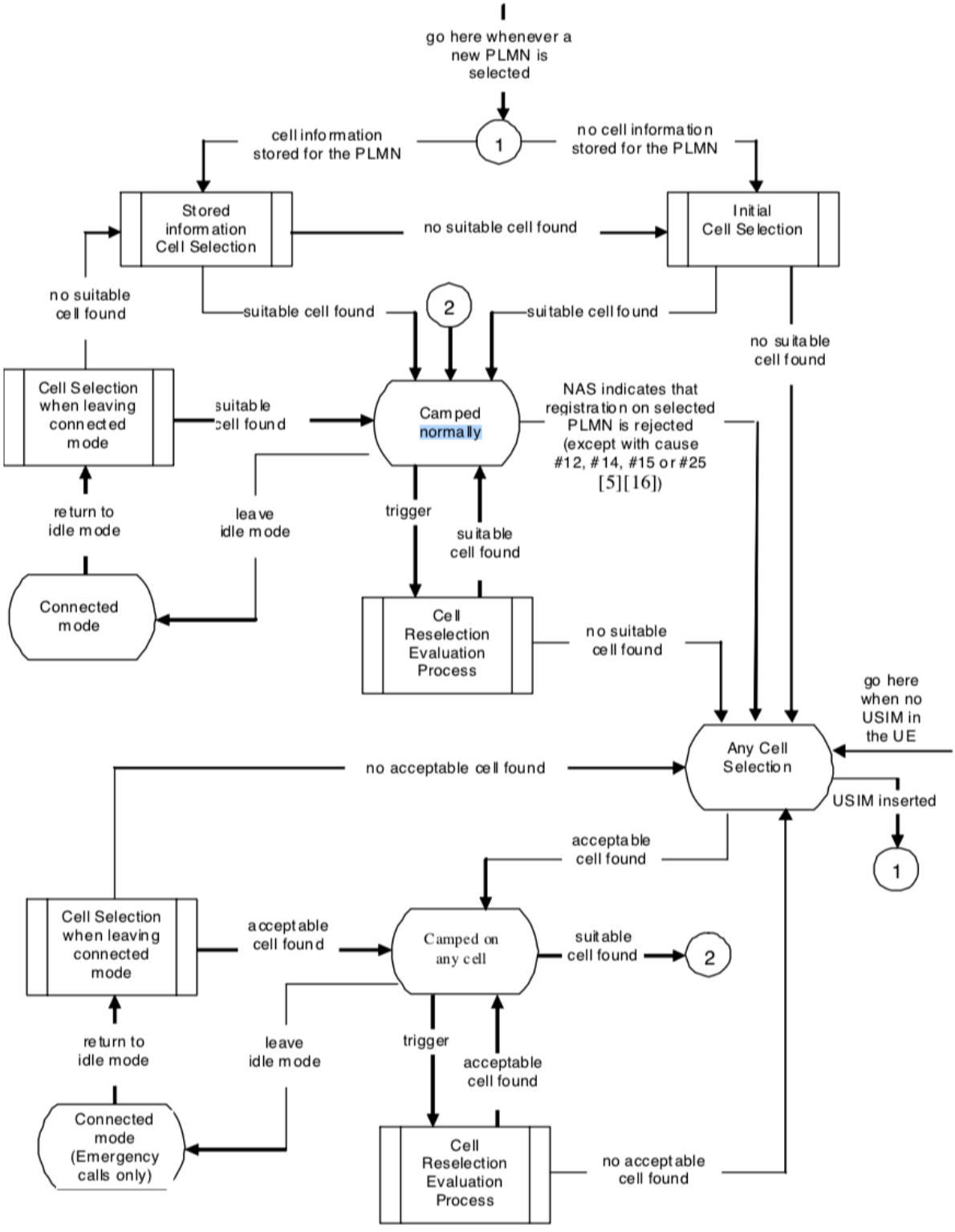

Figure 18: Idle Mode Cell Selection and Reselection (ETSI, 2018, p. 20)

By following the diagram shown in Figure 18 it is possible to see that a phone will reach the state “Camped normally” if a suitable cell is found (ETSI, 2018, p. 20). If no suitable cell is found, it will trigger “Any Cell selection” and if an acceptable cell is found the state “Camped on any cell” will be reached. A phone connected to an acceptable cell in the “Camped on any cell” state will display a warning message. Previous research reveals that phones in the camp of Hitsats didn’t display such a message thus were connected to a suitable cell (Schoenmaeckers, 2018, pp. 15-21). When a phone is camped on a suitable cell, it will reevaluate periodically whether a better cell can be found, but it will never transition from a suitable cell to an acceptable cell unless there is a physical malfunction on the suitable cell. As such a connected phone will remain in a loop where it transitions from the "camped normally" state to the "connected mode" state and back. This is encircled in Figure 19.

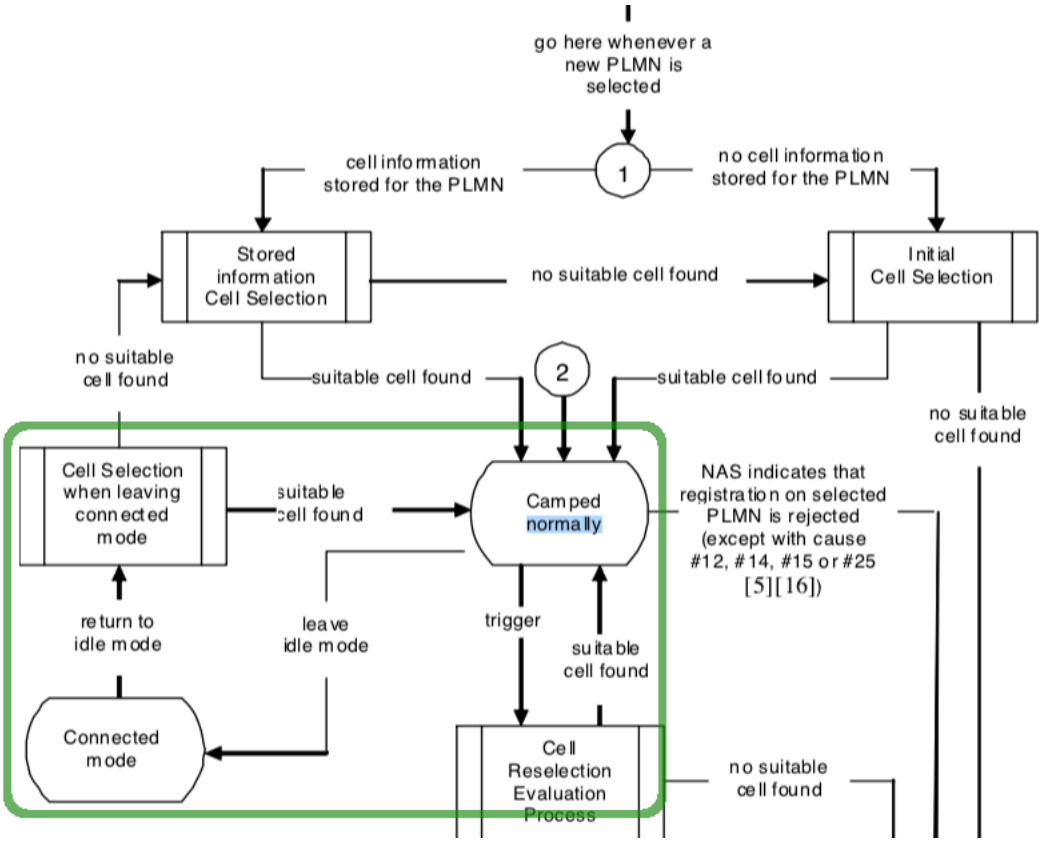

Figure 19: Suitable Cell loop

4.4.1.3.3. RRC States

There is no trouble finding a suitable cell. The issue therefore lies in the attempts for RRC connection states when sending and receiving data. Whenever data needs to be sent or received over 3G HSPA, be it voice call data or internet data, a phone will try to move to the "Connected mode" state by sending an RRC connection request to the cell (ETSI, 2018). There are three relevant RRC states: RRC_IDLE (IDLE), CELL_DCH (DCH) and CELL_FACH (FACH) (ETSI, 2018, p. 57). These distinct states are designed to save energy on mobile devices. A device uses the most energy in the DCH state where high speed data transfer is

possible. Half the energy is used in the FACH state where low speed data transfer is possible, while nearly no energy is used by the radio in the IDLE state where data transfer isn't possible.

The IDLE state indicates that the phone is camped on a cell but does not send or receive traffic. Whenever a call is made or data is sent, the phone will send an RRC Connection Request to the cell attempting to enter the UTRA RRC Connected Mode (ETSI, 2018, pp. 144-146). This can be seen in Figure 20. The E-UTRAN states have been excluded as they are only relevant for 4G. Figure 20 shows that the Connected mode can be reached by establishing an RRC connection via the DCH and FACH states. An attempt via the DCH state is only made if the data size exceeds a certain threshold (Qian, et al., 2010). Otherwise there will be an attempt via the FACH state. The threshold is very low, usually around 15 kbps. This means that only an SMS message, push notifications or something of similar size would be sent and received through the FACH state. Regular websites and voice calls would already require transition to the DCH state. In the DCH state a dedicated high-speed channel is used for data transfer. Lower speed channels will be used if too many devices are in this state.

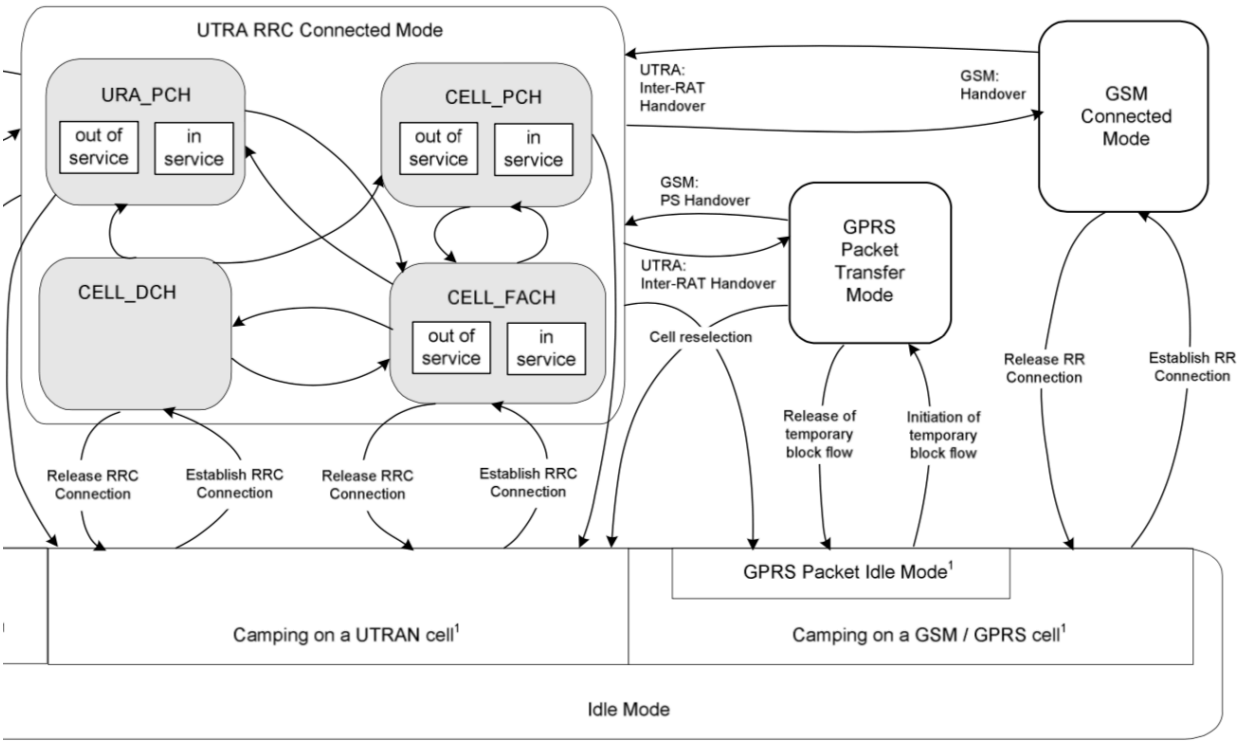

Figure 20: RRC States and State Transitions Including GSM (E-UTRAN excluded) (ETSI, 2018, p. 56)

No data can be transferred without being in the UTRA RRC Connected mode. During congestion, a device can fail to get into this state and therefore will be unable to transfer

data (Shafiq, et al., 2013). However, if connected during congestion, one might still be unable to reach the high-speed channel while in the DCH state.

4.4.1.3.4. Detecting the RRC state on a device

The exact RRC state can be read using an iPhone or a Samsung Galaxy phone running on Android. On the iPhone this is done by dialling **3001 # 12345#** and navigating to UMTS > RRC State. On a Samsung Galaxy this can be done by dialing *#32489#. A test reveals that if data is sent using 3G, the device will go into the DCH state and after a certain amount of time (a few seconds) it will transition into a FACH state and then into other RRC connected states eventually going into an IDLE state. It would be relatively easy to monitor this in Hitsats and it would reveal if the RRC connection request has failed.

4.4.1.3.5. Reaching the DCH State during congestion

The method of calling 112 enabled only a small timeframe during which data could be transferred (Schoenmaeckers, 2018). Examples of the usage were the refreshing of Facebook timelines and initiating calls through messaging applications. Push messages could be received, but upon opening the messages the phone failed to load further content. A push message is usually sent over the FACH connection, but as mentioned earlier, a FACH connection doesn't have enough bandwidth for regular traffic.

It is very likely that the tower has processed the data order and sent the push notification when it had enough bandwidth and computing resources available. This however doesn't work on demand and therefore doesn't enable a user to get RRC connection on demand. Another possibility is that the FACH state is reachable, but that the transition from FACH to DCH can't be made as the channel used during the DCH state is congested. The three points where the transition can be made to DCH are highlighted in Figure 21.

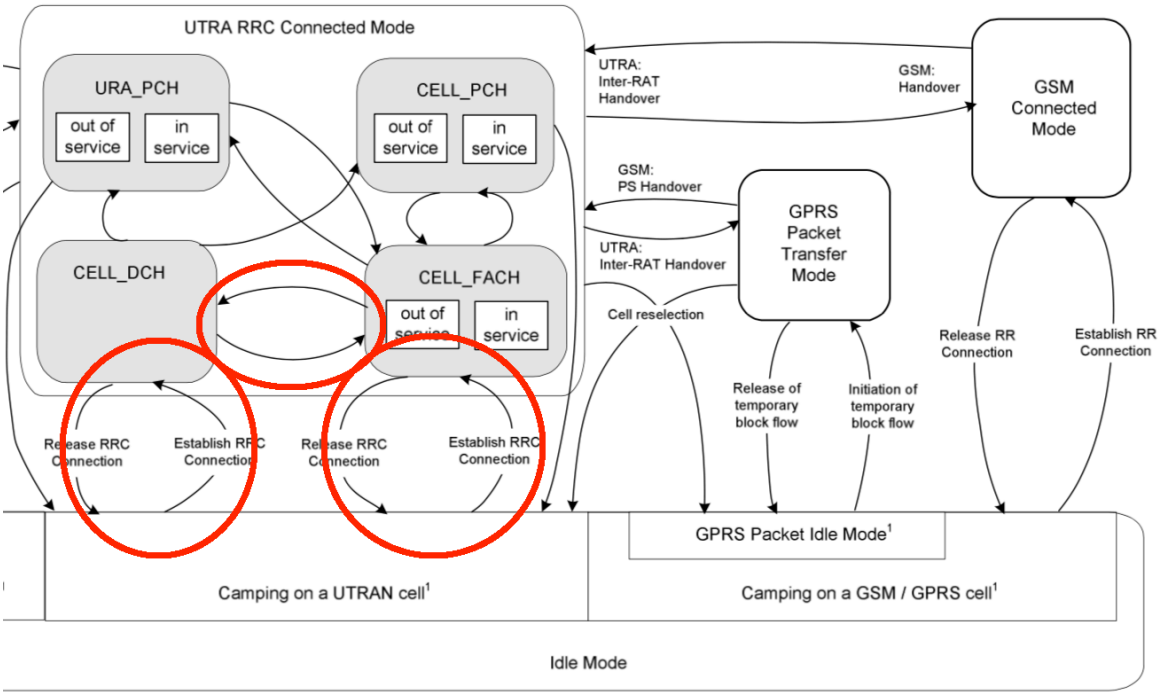

Figure 21: DCH Fail points

4.4.1.4. Does calling 112 cause an RRC connection?

It is clear that an RRC connection cannot be made by the user equipment on demand. Calling 112 somehow triggers something that enables a transition from either IDLE or FACH to DCH. The question is whether this also shows from the documentation and if this explains the method.

4.4.1.4.1. What happens when an emergency call is made?

An attempt to make an emergency calls directly initiates the RRC Connection Establishment procedure (ETSI, 2018, p. 144). Interestingly, the same will happen if the establishment for an RRC connection is made in the Circuit Switched (CS) domain, in other words when regular calls are made. This means that both emergency calls and regular calls will directly start the procedure for RRC Connection. Regular calls however go through an additional check at the RRC Connection Procedure and can't be retried indefinitely because of a certain timer, while emergency calls can (ETSI, 2018, pp. 113-114). This is because the parameter ESTABLISHMENT_CAUSE is set to "emergency call". This indicates that emergency calls can bypass certain checks increasing the attempts made for RRC Connection and therefore increasing the chance that this Connected mode will be reached.

4.4.1.4.2. Alternative transition to UTRA RRC Connected Mode

Another connection route is highlighted in Figure 22. This is the connection via GSM or GPRS with Inter-RAT Handover and PS Handover. These transitions both initiate the RRC Connection Establishment procedure (ETSI, 2018, p. 2158). Certain systems allow for

seamless transitions allowing the UE to immediately move into RRC Connected Mode. Furthermore, when the RRC Connection is established from the Idle Mode, the RRC Connection Request message contains an indication allowing the UTRAN to prioritize the RRC Connection Request from the UE. This further increases the chance. It is easy to check whether this happens. If the phone in hotspot mode switches to 2G when calling 112, this becomes a real possibility. Furthermore, this also indicates that switching a few times from 3G to 2G and back could also be a method that could work to increase the chance for an RRC Connection. Data could also be loaded by switching to 2G via GPRS. It should be enough for smaller messages but will probably fail to connect to larger websites and large Facebook feeds.

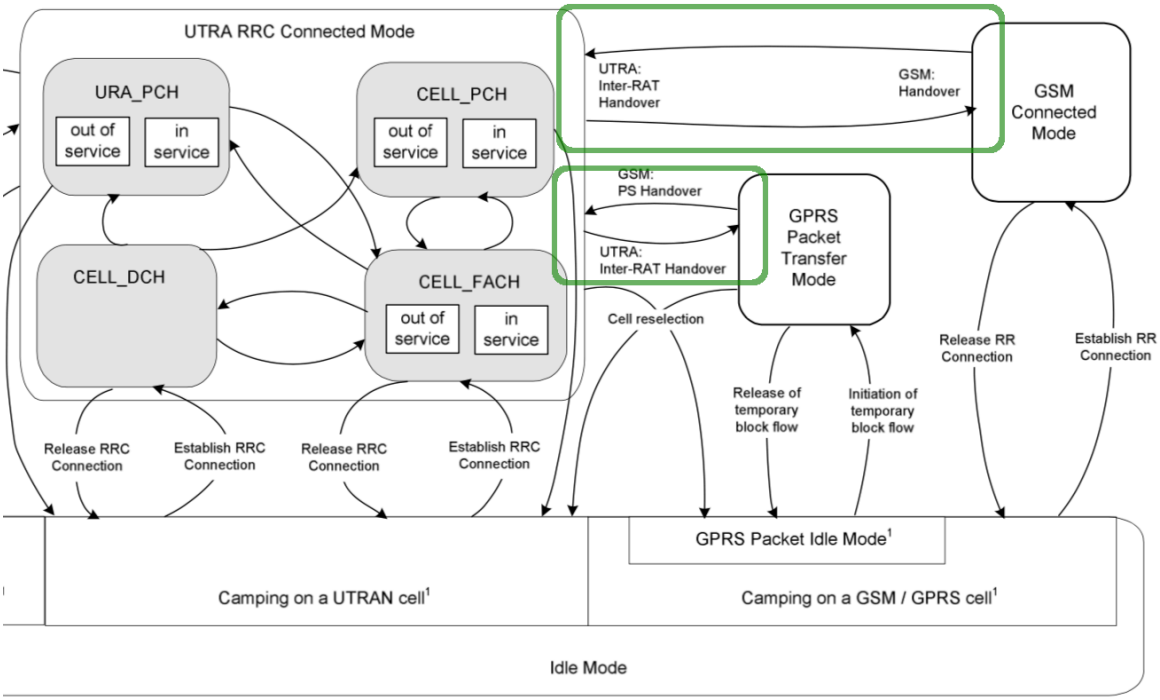

Figure 22: RRC States and State Transitions Including GSM with highlighted transitions (E-UTRAN excluded) (ETSI, 2018, p. 56)

4.4.1.5. Difference regular call and emergency call

Calling an emergency number also works in a slightly different manner than regular calls (ETSI, 2019, pp. 28-35). 112 and 911 will always start an emergency call establishment, regardless whether that is the emergency number of a country. Ethiopia's emergency number neither is 911 or 112, therefore it doesn't connect. The call will always be made in the domain the UE is residing in. Domains can be the IP Multimedia Subsystem Core Network (IM CN), the Circuit Switched Core Network (CS CN) and the Packet Switched Core Network (PS CN). If a certain domain fails, the UE will try to reconnect on another domain. If the call gets aborted, the UE will remember the last tried domain and try it again on that domain. This could indicate that there was a switch to 2G during the emergency call attempt. As shown before, this could initiate an Inter-RAT handover.

In cases of congestion, it is possible that a cell is barred. This prevents connections from being made. This method is called Access Class Barring (ETSI, 2018, pp. 16-22). If this mode is active, SIM cards are assigned to classes. There are 16 access classes. Classes 0-9 are used for ordinary user equipment. Classes 11-15 are used for special services such as emergency services, security services, PLMN staff and public utilities. Class 10 gives an indication whether emergency calls are also barred through a control bit. Each class has a barring factor and if this moves past a certain threshold no new connections can be made with a cell while being member of that class. This can be bypassed if class 10 isn't barred.

4.4.1.6. Summary

Summarized, it is very probable that the main obstacle is getting an RRC Connection. There are less checks resulting in timer countdowns when calling an emergency number increasing the chance of getting an RRC Connection. Furthermore, if during an emergency call the UE switches to a 2G mode, the chances increase further. Essentially calling 112 tries every transition method towards an RRC connection while normal data usually only check a single transition method. However, there is always the risk of getting disconnected due to the congestion in post-connection. Furthermore, while the 112 method could increase the chance of transitioning to an UTRAN RRC Connected State, it doesn't guarantee that enough bandwidth is available for normal data usage. Handovers and connection attempts can still fail due to the severity of the congestion. Finally, these are all merely possibilities. To control this, one would need to be in the camp and monitor the states using the methods described earlier.

4.4.2. Psiphon

Psiphon is a free application on Android formally used to circumvent censorship by utilizing VPN, SSH and HTTP[14]. There are also versions available for Windows and iOS. Psiphon is used in Hitsats to enforce connectivity (Schoenmaeckers, 2018). Psiphon can tunnel the whole device. The main obstacle of getting connection in Hitsats is the congestion preventing an RRC connection. A smartphone only tries to initiate this connection (DCH) when it is actively sending or receiving data, as seen in the analysis of the trick of initiating an emergency call. For example, when loading a website. As soon as a website is loaded, it returns to IDLE mode. A smartphone can also timeout before loading a website staying in IDLE mode.

The way Psiphon could help connectivity might be explained by how a VPN works. A VPN application constantly sends packets of data forth and back from the device to the secure server. This is done to maintain the tunnel connection. This means that a device when a VPN is started, will constantly try to initiate an RRC connection if it isn't possible. This increases

[14] Psiphon, 10 January 2020, Uncensored Internet access for Windows and Mobile, Retrieved from https://www.psiphon3.com/en/index.html

the chance to make an RRC connection as the constant sending of data packets ensures that the device will be first to get a connection when it's available.

When an RRC connection has been made and the device is in DCH state, the VPN will keep sending and receiving packets. This causes the device to stay in DCH state. Only when no data is sent will a device go to FACH state after a few seconds. When the device doesn't send any data while in FACH state, it will finally go into IDLE mode after another few seconds. The timing for state transition depends on the parameters set by a mobile network provider. A device can also still go into IDLE mode due to disconnects and timeouts, but the packets sent by a VPN service are smaller and therefore less likely to timeout as compared to a modern website or picture.

4.4.3. Webmail drafts

The trick is fairly straightforward. Two persons create a webmail account, such as on Gmail, Yahoo or Outlook and share the username and password. Instead of sending emails using two accounts, they have one account. To communicate a person creates an email but never sends it. Instead the person saves it as a draft. The other person then logs into the account and can read the draft after which he or she deletes it. This should avoid surveillance.

4.4.3.1. SMTP and HTTPS protocols

Normally mails are being sent using the SMTP protocol. This protocol enables communication between the sender's and receiver's email servers. This protocol calls for multiple moments of communication by the servers using SMTP commands and replies. This could easily be recognized by a provider, but nowadays many people use browsers or mail clients on their Android phone. Webmail on browsers only use the HTTPS protocol and only the servers, such as Gmail or Yahoo servers, might use SMTP to communicate. The communication from the user to the webmail client is in HTTPS and therefore encrypted. The communication between different webmail clients is in SMTP but can only be seen by the providers on which these servers send and receive traffic. These servers are located on centralized locations. However, due to not sending any mail, nothing will be sent, and SMTP won't be used. Gmail for example uses a HTTP request on their API (Gmail, 2019). This will be registered as regular traffic towards a Gmail server.

4.4.3.2. Traceability

Mails can however be traced and with help of the webmail provider even investigated. Google for example tracks which IP addresses make use of which account. This can be noted by logging in from a new address. If 2-factor-authentication is turned on, Google will ask for a confirmation to confirm if it is the user. This tracking has been used by Google and the FBI during an investigation which revealed the affair of CIA director David Petraeus with Paula Broadwell (Heisler, 2012).

Petraeus set up a dummy account. This account was shared by the two. They never sent each other emails but used the drafts method described earlier. However, they still got caught with help of a misstep and help of Google. Broadwell sent anonymous threatening emails to Jill Kelley through another Gmail account. Kelley asked help from the FBI which traced the emails to their origin. The FBI then got a warrant to monitor this further and uncovered that Kelley was also communicating with a private Gmail account that belonged to Petraeus.

In all likeliness, Broadwell used multiple Gmail addresses from her private network. When logging into an account, Google tracks which IP-address is used to log in. Furthermore, when sending an email, the IP-address can be read easily from the header. When Broadwell sent the email to Kelley, it was relatively easy to get the originating email address by reading the header. The FBI could then monitor that IP-address, with assistance of Google and figure every Gmail account used on that IP-address. Furthermore, it is very probable that emails might be secured by the TLS protocol, but that drafts aren't. Google might therefore be able to read drafts. This made it easy for the FBI to figure out the scandal.

4.4.3.3. Advice

In the cases of usage by NGO's and refugees, it is advised that public Wi-Fi is used otherwise it can still be traced to a single person with help of either webmail provider such as Google or the ISP. A similar trick has been used that is slightly more secure. One could for example write a simple document and then encrypt it using a password that has been shared with the other person. This would add a layer of security. One could then also use cloud services such as Dropbox. Alternatively, one should use a VPN or proxy to send emails making it harder to trace to origin.

4.4.4. Chat applications

Eritrean refugees usually use multiple chat applications. This has many reasons some of which are technical. The first reason is the environment one currently resides in. The dominant chat application often seems depends on the country. But most refugees have multiple application downloaded. These include Telegram, WhatsApp, Facebook Messenger, IMO, Signal and Viber.

4.4.4.1. Influence of environment

Dependent on the country, certain chat applications might be more used. For example, in Ethiopia, Telegram is very popular. It makes sense that Eritrean refugees residing there also use it. While the connection is relatively stable in the main capital, there are still occasions during which the connection seems to get worse (H. Personal Communication, 27 September 2019). It happens randomly and no real explanation can be found. If a particular app seems to have connection issues such as messages taking a long time to arrive, one

switches over to another application. This could be one explanation for the usage of multiple messaging apps.

4.4.4.2. Media shutdowns

There have been times during which the Ethiopian government shuts down the social media. This has had diverse reasons, but during such times apps such as WhatsApp and Telegram often get throttled (NetBlocks, 2019). This means that the connection becomes so slow that it becomes unusable or don't work at all. During these times VPN's are a popular tool to circumvent the blockade. Using a VPN, it is possible to again use the apps, but one has to be careful as it is frowned upon. Furthermore, VPN services can be blocked. It would be easy for an ISP to figure out whether a connection is made using a VPN and which VPN that is. Even worse, with enough power, the provider of a VPN can still be forced to give up information about the user. Blocking all VPN services would however be quite a hard task as it is relatively easy to set up a new server.

4.4.4.3. Resource requirements

Another reason for multiple chatting applications is given by the economical impediments in certain areas. As has been mentioned before, some messaging applications use less data and have less strict system requirements than others and this does have impact. For example, in Hitsats, WhatsApp wasn't supported on many phones causing refugees to use other apps (Schoenmaeckers, 2018). WhatsApp is the most popular messaging application in Europe. If a relative in Europe would wish to keep in touch with somebody in Hitsats through a messaging application, they would be forced to download the application used in Hitsats.

Many refugees use older phones, while also having to pay a lot for data and electricity. This combination makes it hard to download messaging applications. Many Android smartphones already have Facebook pre-installed. This means that a refugee only has to log in to get in touch, while WhatsApp needs additional resources to download the app. Furthermore, Facebook doesn't need a phone number if an account is already registered. This means that it can be used if one has access to Wi-Fi, while other messaging apps need a phone number and therefore a SIM card. Facebook furthermore offers a lightweight version of its application called Facebook Lite.

Facebook Lite uses less data and takes less space making it more usable on Android phones with lower specifications. Table 1Table 4shows how much space of the internal storage an application took on a Samsung Galaxy S7 Edge after installation. The size often depends on the specifications of the phone it is installed on. Nevertheless, this simple comparison shows that Facebook Lite takes significantly less storage space than all other applications.

Table 4: Internal storage used by messaging applications on Android

Application	Version	Size (MB)
WhatsApp	2.19.308	45,59
Telegram	5.12.1	48,42
Viber	11.8.1.1	150
Facebook	247.0.0.42.116	152
Facebook Messenger	241.0.0.17.116	95,73
Facebook Lite	172.0.0.11.116	1,90
IMO Messenger	2019.6.31	56,48
Signal	4.49.18	60,86

Another use of messaging application is accessing webpages that use a lot of data. Some refugees reside in areas with lower connection speed and higher data rates. Most webpages are built for western markets and use frameworks that implicitly assume western connectivity. In simpler terms, they assume a cheap and fast broadband connection and use more data. Due to the size of modern webpages, it is nearly impossible for people in areas with slower connections to make use of them. It either takes a long time to load or doesn't load at all. This could largely be due to elements of a large size, such as high definition images or due to heavy usage of JavaScript, advertisements or flash content. In the case of GPRS connections over 2G, it already becomes unusable even in Europe. Furthermore, data is a lot more expensive. A person in the refugees' network can be asked to copy the text content of the website and send this over a chat application. This causes a significant reduction of data while still maintaining most of the information.

4.5. Using a foreign number

When using a black-market SIM card there is always the possibility of the number being shut down. The contacts of the refugee won't be able to reach the refugee anymore without him getting a new SIM card and informing them. Due to the scarcity of money, data and maybe even electricity, this is quite an expensive endeavor.

SIM cards from the EU can't be shut down without a good reason. As long as somebody is using a SIM card and loading prepaid credits, it will remain active. Using a foreign SIM card isn't possible without having the SIM card itself, but one can still use the number. This is done by using the European number when setting up a messaging application.

For example, when setting up WhatsApp, the user gets prompted to enter his phone number. WhatsApp will then send this number a text message with a code, or alternatively

call the number and play a message with a code. This code needs to be entered into WhatsApp and then it can be used. A refugee can ask a friend or relative living in the EU to simply buy a SIM card, put it into a device and simply relay this code while the refugee sets up WhatsApp on his own phone. WhatsApp doesn't physically need a SIM card in the phone to be set up, only the code. This trick has been used before to use WhatsApp on a tablet because WhatsApp isn't available on a tablet through the official Google Play store (Black, 2018). Sideloading and registering with a number on a phone was a trick to get it working on a tablet.

Chapter 5: Analysis

Should gatekeeping theory be expanded? The theory of gatekeeping has traditionally assumed top-down communication. Gatekeepers would process information for the gated and the gated had no influence on this process. The gatekeeper had been defined as an authority such as a journalist, news editor or news agency that makes the decision what information should be published. This information is then published using traditional mediums such as newspapers, radio and television. Publishing through these mediums would require a larger scale organization and capital before it would be possible to reach many. The audience of these mediums had a passive role. Communicating with the gatekeepers was quite difficult as there were no direct channels.

5.1. Network gatekeeping theory

Barzilai-Nahon (2008) expanded traditional theory with network gatekeeping theory. The important expansion involved attributing the salience of the gated for the gatekeeper. Salience is measured through political power, information production capabilities, relationships and alternatives of the gated. The expansion of these attributes makes it possible to analyze whether internet has changed the dynamics between gatekeeper and gated. Barzilai-Nahon (2006) has shown how the internet influenced the gatekeepers on a virtual forum. Due to the availability of alternatives, gated have a higher salience resulting in the limitation of gatekeeping mechanics available to gatekeepers.

5.2. Gatekeepers and mechanisms

The situation of the Eritrean refugees represents an extreme situation with many black holes where gatekeepers use mechanisms to control information. Without internet the situation would be very simple. The refugees would have to rely on camp officials, middlemen, governments and possibly NGO's for information. The information would be spread using newspapers, spokesmen and maybe radio. Contacting family and friends would hardly be possible because refugees would have to have a phone and a phone number.

From the results it became clear that the internet had had its influence. Using smartphones with internet, refugees were able to get their own information. But gatekeeper mechanisms also evolved with the internet to try and control the information, even from the internet. This is why certain methods were used by refugees to circumvent these mechanisms.

5.2.1. Governments

The largest group of gatekeepers are governments and authorities. Authorities can confiscate any digital device of refugees upon entering a camp. This instantly causes a refugee to be traditionally gated. No communication is possible, and the authority controls all information entering and leaving a camp.

Governments can cause also barriers by not investing in adequate infrastructure for refugees. Bad infrastructure can hinder communication of refugees making it harder to communicate with the outside world. This is especially true for camps near rural areas with inadequate infrastructure. This could cause congestion in the case of larger camps. Refugees can hardly use internet and circumventing methods such as calling 112 or using a VPN have to be used to increase chances of connectivity.

There can also be obstructions by implementing to laws penalizing publications of information which can cause harm as defined by a government. These laws cause self-censorship on social media, blogs and websites due to fear of surveillance. Not only refugees, but also citizens become more conscious of what they post online. This also has a negative effect for journalists and activists as this self-censorship causes there to be less information from the people. Furthermore, if requested by a government, Facebook might delete certain publications. This example shows how surveillance had an adverse effect for the gated and decreased their salience by increasing the political power of gatekeepers.

Finally, there are media shutdowns imposed by governments. These can be full shutdowns or partial shutdowns. During a full shutdown, no information can travel within, enter or leave the country. This essentially creates an artificial black hole and there is no way to circumvent this in Africa due to geographical properties and sparse population. Applications such as Firechat initiating a peer to peer mesh network through Wi-Fi hotspots and Bluetooth depend on densely populated areas. A partial shutdown often only blocks social media, including Facebook, WhatsApp and other platforms.

This can be circumvented by using a VPN, but the general population often is unaware of this method or fearful of using it due to surveillance. In terms of communication effects, there might be little difference between a full and partial shutdown. The method does however show that governments have implemented methods to censor the gated. This implicitly shows that mass communication from the gated to the gated exists and is something that is unwanted in some scenarios. This indicates two-way communication between gated.

5.2.2. Family and friends sending financial resources

The second large group of gatekeepers are the friends and relatives of refugees. This group can also be seen as gated as governments also withhold information from them if they censor the refugees. They often reside in the better-connected node. To communicate refugees, need digital means and therefore financial resources. These are often obtained through means of remittances enabled by the digital money transferring services. These remittances are sent by those in the better-connected node, essentially making them a gatekeeper.

These gatekeepers don’t only want to send information, but they also want to receive information from those currently migrating in order to keep the whole community up-to-date. This created a circulatory effect showing that communication travels in both directions. Refugees pass on information about the situations they reside in and the relatives and friends pass on information that they gathered from within the nodes from fellow diaspora. These in turn again pass it on to their relative and friends that are migrating along the trajectories and nodes. It shows a very similar situation as in the colonial age where information is sent to the bigger nodes in order to be processed and then again used locally in the colonies. This shows horizontal two-way communication between networks of gated people.

5.2.3. Journalists and activists

Activists and journalists are the third group of gatekeepers. In general, there isn’t much attention for the difficulties Eritrean (and other) refugees face when migrating towards the West. Journalists and activists are mostly responsible for publishing information about the happenings during this migration. These journalists and activists are largely dependent on information from refugees about the situations they face. Refugees often contact these journalists and activists by means of digital communication. WhatsApp, Facebook or any means through which they can be reached are used by refugees to make contact.

Without this bottom-up communication, it would be very hard for journalists and activists to publish their stories as they would lack information. They simply are dependent on the information of the gated. Journalists and activists are also active on Facebook which is a primary news source for many refugees. This builds social capital which gains the trust of refugees. This does however mean that the work of said journalist or activist needs to be satisfactory. If one would only report negatively on refugees and as consequence worsen the situation of the refugees, they would most probably not be contacted and would not get any information of the refugees.

This essentially shows that communication from the gated with the gatekeeper is important. By publishing articles, the gatekeeper builds social capital and with that a relationship with the gated. Using the information gained from the gated, the gatekeeper acts as a proxy that filters and publishes articles that could be useful for the gated. This also shows some sort of circulatory effect indicating two-way communication between gatekeeper and gated. This wouldn't be possible without the modern digital means facilitating communication and accessible mass media.

5.3. Summary

Traditional gatekeeping theory only assumed top-down communication. With the internet and particularly social media this has changed. The extreme situation of the refugees has shown that the internet has enabled two-way communication both between gatekeeper

and gated and between gated. Governments do not like the increase salience and have developed new gatekeeping mechanisms to limit this. Refugees and citizens have however found methods to circumvent this. This has been done using resources of other networks of gated in the form of diaspora and sometimes even using resources of other gatekeepers in the form of journalists and activists.

Chapter 6: Discussion

In this chapter there will first be a discussion of the meaning of the results followed by a discussion why these results matter. Then there will be a discussion of the limitations followed by recommendations for future work and practical actions.

The research has shown the importance of digital means to circumvent gatekeepers. As expected, Eritrean refugees face many situations where gatekeepers use gatekeeping mechanisms to limit the flow of information. Digital means have however introduced methods to circumvent these mechanisms. The research has shown how refugees can use digital devices to send and receive information about where to go. They also use it to fund their migration. The internet has changed the dynamics between gatekeepers and gated. It has also changed the dynamics between gated. Thanks to digital means using internet, gated are no longer fully dependent on the channels guarded by gatekeepers to send and receive information. In black holes however, there is very low salience. This makes it is very easy for gatekeepers to still completely control information.

6.1. Interpretation of results

The results have several implications for network gatekeeping theory and fractal theory.

6.1.1. Foundation given by network gatekeeping

Previous research about traditional gatekeeping has always been from the perspective of the gatekeeper. This research looks at gatekeeping from the perspective of the gated. Network gatekeeping theory has given the foundation for this by introducing gatekeeping salience. Using this framework, it became clear that political power is greatest asset of gatekeepers as information production has become more accessible and because many alternatives exist. This is shown in the research by the many innovative methods used to avoid surveillance or used to circumvent barriers. Examples are the mandatory SIM registrations, using webmail drafts and using foreign SIM cards.

6.1.2. Fractal theory

Fractal theory shows how the slightest differences between nations can have a very large impact on the development of a nation. In the case of Africa, it means that the colonial past, geographical differences and cultural heritage can have an impact on the development digital means. This is shown in this research by the different internet infrastructure compared to western nations and its influence on gatekeeping. Information still follows the same pattern as the information architecture of the colonial age. This is done today by social media networks.

Africa is very large, geographically seen. Much larger than usually depicted as shown in the introduction. This means that a cabled infrastructure would be far more expensive compared to in Europe. This difference is amplified due to the difference in population

density. Europe has a very dense population making internet infrastructure cheaper. This is also why mobile broadband is more popular in Africa. It's harder and more expensive to get the same coverage in African countries as in the West. This is a large contributing factor to black holes. This also causes the susceptible environment for refugees.

A large problem is the orientalism of the developed applications and websites. They all implicitly assume a western connectivity standard making it unusable for regular citizens in Africa. This is also shown in Hitsats where there have been difficulties using applications, such as 24COMS, which would work very well with western infrastructure, but didn't in rural African context due to the amount of data and speed needed to load high definition videos. There does however seem to be change as Facebook for example is making lighter variants of their applications and because entrepreneurs start building their own applications. These entrepreneurs are sometimes members of diaspora using their capabilities to help those back home.

The cultural heritage is why refugees are able to migrate towards the west. This has been shown in previous research which states that African communities live according to the we-paradigm were resources are not owned individually, but communally. This might also be the cause why there are so many remittances and other forms of help from diaspora. Without this, it would be impossible for refugees to circumvent gatekeepers as many methods depend on the resources of a community. African nations also seem to want to have a tighter control on information. This is indicated by the many laws that lead to surveillance.

6.1.3. Information bubbles

One surprising observation is the lack of attention of the more mainstream media. Immigration is a hot topic today with parties divided between allowing refugees access or providing shelter in the region. In Europe it is especially about the refugees crossing the Mediterranean Sea in what sometimes look like lifeboats. While there is attention of this influx of refugees, there is little attention about the journey they made.

The mainstream media publishes very little about the hardship refugees endure and even less about the dire camp conditions. There is however enough information available online about this. This is very interesting because it could indicate that while internet allows for two-way communication, it requires an active will of gated to do so. It also indicates that while the internet has made it possible to find alternative news sources and therefore increased the salience, that gated might not utilize these possibilities. This could be due to the trust the mainstream media has built and with this a relationship with the gated. This shows the danger of a too large platform. In turn this platform can be used for gatekeeping and create information bubbles by use of filters.

6.2. Implication of results

This research has used the foundation given by network gatekeeping theory to explore the gatekeeping Eritrean that refugees experience and how they circumvent this using digital means. This research builds on the existing evidence that the internet has changed the dynamics between gatekeeper and gated. The internet has enabled new resources for the gated to increase their salience. This research explores how Eritrean refugees have used the new resources to increase their own salience. With this it provided examples that can be used to give direction to future research. While previous research about gatekeeping has mostly been conducted from the perspective of the gatekeeper, this research is conducted from the perspective of the gated. This has led to the proposal to expand gatekeeping theory with two-way communication. Gated aren't passive entities, but rather try to increase their salience if it is too low.

The results of the research should be taken into account when creating policies for refugees. It shows how gatekeeping influences the flow of information and how gatekeepers even try to limit information exchange through internet. It also shows how refugees circumvent these attempts and with that indicate areas for improvement. Especially when providing aid, one should be aware if and how this influences the situation of the refugees. The infrastructure of Africa is unique, and this should be taken into account when developing solutions. Failure to do so might worsen situations in black holes where middlemen can be corrupt. A good example besides human trafficking is the surveillance. Thanks to digital means gatekeepers have increased their political power and abused this power. Digital solutions should specifically be developed with the alternative African infrastructure in mind rather than western standards.

6.3. Limitations

This research merely explored the different innovative methods in the context of the migration along the Mediterranean route. This list is not meant to be exhaustive and it is very likely that these methods will change with time due to the ever-changing infrastructure in Africa. It was beyond the scope of this study to investigate every route leading to the Mediterranean Sea, but it is suspected that little countries could be more extreme.

The ecological validity has been ensured by approaching participants and finding similarities rather than speaking from an authority's manner. This created familiarity making it easier to find out about the cues that were the cause for using certain innovative methods to make connection. If the approach had been in an authoritative manner, the refugees might have produced "correct" answers rather than true answers. Due to the nature of these innovations, the action fidelity would be nonexistent in an experimental context, which is also why observations were the preferred method of gathering information.

These innovative methods are representative for the specific situations but are hardly generalizable. While many interviews and observations were made, the number of refugees that participated was very limited and moreover might have a bias because those that were reachable were those that showed ingenuity. They might not represent the general population. Generalizability has however not been the goal of this research. The identified innovative methods merely provide a starting point on which to build future research.

6.4. Recommendations

This research indicates two-way communication between gatekeepers and gated and between gated. Further research is needed to establish whether this also is the case for other communities of gated. This can be other refugee groups from other parts of the world, but other possibilities could be in a political environment where political groups negotiate policies and exchange or withhold information.

Future research could also further investigate what difficulties refugees face in certain specific camps. There are many refugee camps in Africa, and each has their own difficulties. By investigating these camps, it could be possible to see a pattern of how gated try to access and spread information. This will provide insight how to better facilitate this. An interesting angle would be how orientalism creates barriers for refugees due to implicit western specifications.

Chapter 7: Conclusion

The main question of this research was what digital means for communication are being used by Eritrean refugees to circumvent obstacles caused by gatekeepers. The short answer to this question is the internet. The internet has enabled the creation of social media platforms that facilitate accessible communication. The internet has also enabled the creation of financial services that can be used for remittances. Finally, the internet has enabled refugees to publish their own information with help of social media platforms and chatting applications. These platforms have also made it easier to contact journalists and activists. With help of the right journalist or activist, their story can even reach larger audiences.

The list of digital means has been recorded in Table 5. Especially the method to use emergency calls, Psiphon, webmail drafts and a foreign SIM stood out. These are irregular methods that are used due to the unique context of the Eritrean refugees. Using these innovations, the gated refugees were able to either increase their salience with the gatekeeper or to circumvent them. Political power seems to be the hardest to increase for Eritrean refugees. This is no surprise as the largest gatekeepers were governments. Surveillance remains a large barrier due to the risk of imprisonment. Many innovations are facilitated by resources of diaspora in better connected nodes.

Table 5: Digital means to circumvent gatekeeping

Innovation	**Influence salience**
Calling 112 during congestion to get internet	+ Information production
Using Psiphon during congestion	+ Information production
Using sharing applications	+ Information production
Using low data alternatives	+ Information production
Sharing prepaid credits of phone cards	+ Information production
Using digital money transferring services	+ Information production
Using webmail drafts	+ Information production + Political power
Sending website contents through chatting applications	+ Information production + Alternatives
Foreign SIM cards	+ Information production + Alternatives + Political power
Conference calls	+ Information production
Sharing of digital means	+ Information production
VPN	+ Information production
International calling applications	+ Information production

	+ Alternatives
Multiple messaging applications	+ Information production + Alternatives
Deleting messages on chat applications	+ Political power
Using social media to find contact details	+ Information production

7.1. Summary and reflection

Network gatekeeping theory has laid the foundation that can be used to research gatekeeping after the widespread adoption of the internet. This is especially important as the widespread usage of smartphones has enabled the widespread usage of internet. Many Eritrean refugees flee their country and undertake a large journey from the Horn of Africa across the Mediterranean Sea into Europe. They are very dependent on information during this journey and for this they rely on middlemen and increasingly on the internet.

The analysis of the context has revealed the many difficulties Eritrean refugees face during their migration. This was analysis primarily conducted through the analysis of previous research, interviews and news articles. While news articles and previous literature did provide some insight, little research was done and published about the digital infrastructure making it hard to find out much. Previous research and news articles have been written from a humanitarian perspective, rather than a technical one.

The interviewees were all very knowledgeable about the political, social and economic context, but not the digital context. These are reasons that make it hard to extract technical details to gain insight of the digital infrastructure and innovations. Nevertheless, by combining information it was possible to get adequate insight and identify the possible gatekeepers and other barriers.

The results showed that gatekeeping potentially creates a black hole where corrupt middlemen can cause serious harm in the form of trafficking for ransom. From the context it became apparent that refugees often rely on relatives in better connected nodes for information and resources.

Due to the explorative nature of this research, the innovations are not generalizable. It is however very possible that refugees of other countries at the very least also make use of digital means to circumvent gatekeepers during their journey. This would be something that could be a topic for future research. Furthermore, many African nations have a shared colonial heritage and the influence is still visible today. Western corporations still reap benefits from the information architecture.

7.2. Future research

This research indicates the expansion of gatekeeping theory with two-way communication. Digital means have enabled this. Future research can check whether this is also the case for other refugees coming from different places, such as the Middle East. Other possibilities can be in an entirely different setting such as the political arena where a party communicates with their followers. For example, how does internet outrage influence the agenda of political parties?

Future research can also focus on other methods through which the salience can be increased. Especially political power is hard to increase when dealing with larger entities such as governments. While social media applications have made it easier, it should also be researched how these same applications can limit the salience. As described earlier, Facebook profiles are often targeting for censorship. This makes it very relevant to seek methods through which people can still publish information but remain anonymous to avoid political persecution.

This also raises the question whether messaging applications such as WhatsApp are really that safe to use. Signal for example uses encryption that is touted to be the most secure. Weak points need to be researched. Other than safety, it should also be usable. The application takes a fairly large size similar to that of WhatsApp. This might make it expensive for those that need it the hardest.

7.3. Practical recommendations

Several innovative methods have been researched in this paper. This has provided valuable insight. This has led to the practical recommendations given in this section.

Refugees have used the method to call 112 to increase connectivity. The technical analysis shows that there is congestion and that calls in general bypass certain checks that could increase the chance to gain connectivity. Another possible method that is less intensive could be switching from 2G/3G mode to 2G only and then switch back to 2G/3G mode after refreshing the feed or trying to make a data call. This is however no long-term solution. The situation in Hitsats is very difficult as every solution such as free Wi-Fi access points require direct power which isn't available. Remote off-grid solutions should be researched as this is the biggest hurdle.

Refugees use digital money transferring services. This is an important resource for money. When developing policy, this should be kept in mind. It might be useful to even facilitate this as it can increase the wellbeing of refugees as camps are often inadequate. It however could also provide incentives for traffickers. Future research could focus on safe and secure methods to transfer and carry financial resources.

Finally, refugees make use of internet to find and send information. This is expensive for them and sometimes even impossible to the resources required by websites. Modern websites require newer smartphones and a fast data connection, both which aren't available to refugees. When developing websites containing information that is useful for refugees, it should be made so that it has a very small size. This means that there should be no expensive JavaScript elements, no high-resolution images and that there should be no tracking or any other functionality that unnecessarily uses data. The smaller the site, the better.

There should also be a smaller chatting application as an alternative for Facebook lite as Facebook doesn't have a good reputation when it comes to protecting privacy. Ideally this should also work in less connected areas. For Hitsats and similar situations these applications could make use of peer-to-peer mesh networks using Bluetooth and Wi-Fi hotspots where only a limited number of phones actually connect to the internet. This would however mean that refugees must be persuaded to turn off their mobile data connection.

Webmail drafts have been used to avoid surveillance but the scandal involving Petraeus has shown that it might not be as safe as thought. While drafts are better than directly sending emails, they can still be traced. If possible, it should be used in combination with a VPN service. Furthermore, it is wise to not use an account for too long as it increases the chance of detection. Drafts also aren't encrypted. Instead of drafts, it would be better to communicate using encrypted messages.

7.4. Contribution

This research explored the extreme situation of gatekeeping that Eritrean refugees face during their migration to the West. Most gatekeeping literature has been conducted with the gatekeeper as the focal point, this research deviates by putting the gated as the focal point. This approach has revealed how gated have used digital means to circumvent gatekeepers. This has primarily been done by increasing the information producing capabilities through the use of social media platforms. This has shown that gated aren't passive, but rather also interact with gatekeepers and their mechanisms. This has led to the suggestion to expand gatekeeping theory with two-way communication.

Chapter 8: Bibliography

3GPP. (2019). Retrieved November 8, 2019, from 3GPP: The Mobile Broadband Standard: https://www.3gpp.org

Barzilai-Nahon, K. (2006). Gatekeepers, Virtual Communities and the Gated: Multidimensional Tensions in Cyberspace. *International Journal of Communications Law & Policy*.

Barzilai-Nahon, K. (2008). Toward a Theory of Network Gatekeeping: A Framework for Exploring Information Control. *Journal of the American Society for Information Science and Technology, 59*(9), 1493-1512.

Barzilai-Nahon, K. (2009). Gatekeeping: A Critical Review. *Annual Review of Information Science and Technology*, 1-79.

Black, M. (2018, April 6). *How to Install WhatsApp on Tablet.* Retrieved from Tech Advisor: https://www.techadvisor.co.uk/how-to/google-android/whatsapp-tablet-3517280/

Boss Revolution. (2019). *Call, Top Up, Send Money Around the World - Boss Revolution*. Retrieved from Boss Revolution: https://www.bossrevolution.com/en-us/

Broadband Commission. (2018). *The State of Broadband: Broadband catalyzing sustainable development.* ITU, UNESCO.

Broadband Commission. (2018). *The State of Broadband: Broadband catalyzing sustainable development.*

Broadband Commission. (2019, May 24). *Home*. Retrieved from Broadband Commission: https://www.broadbandcommission.org/about/Pages/default.aspx

Crijns, M. (2018). Mensenrechten in Eritrea. In M. van Reisen, & K. Smits, *Eritrea en Eritrese Vluchtelingen* (pp. 99-108). Dutch Central Agency for the Reception of Asylum Seekers (COA).

Crijns, M. (2018). Migratie uit Eritrea. In M. van Reisen, & K. Smits, *Eritrea en Eritrese Vluchtelingen* (pp. 109-123). Dutch Central Agency for the Reception of Asylum Seekers (COA).

Crijns, M., & Smits, K. (2018). Nationale dienstplicht. In M. van Reisen, & K. Smits, *Eritrea en Eritrese Vluchtelingen* (pp. 91-96). Dutch Central Agency for the Reception of Asylum Seekers (COA).

Dahir, A. L. (2018, February 24). *In a continent dominated by WhatsApp, Ethiopia prefers Telegram*. Retrieved July 15, 2019, from Quartz Africa: https://qz.com/africa/1214381/in-a-continent-dominated-by-whatsapp-ethiopia-says-yes-to-telegram/

Dahir, A. L. (2019, June 18). *Ethiopia's tech startups are ready to run the world, but the internet keeps getting blocked*. Retrieved July 15, 2019, from Quartz Africa: https://qz.com/africa/1646789/ethiopia-tech-startups-hurt-by-social-media-block-internet-shutdown/

Dekker, R., & Engbersen, G. (2013, October 18). How social media transform migrant networks and facilitate migration. *Global networks, 14*(4).

Ethio Telecom. (2019). *Mobile Internet* -. Retrieved November 8, 2019, from Ethio Telecom: https://www.ethiotelecom.et/mobile-internet/

ETSI. (2018, October). *ts_122011v150500p.* Retrieved from ETSI: https://www.etsi.org/deliver/etsi_ts/122000_122099/122011/15.05.00_60/ts_122011v150500p.pdf

ETSI. (2018, July 1). *ts_125304v150000p.* Retrieved November 9, 2019, from ETSI: https://www.etsi.org/deliver/etsi_ts/125300_125399/125304/15.00.00_60/ts_125304v150000p.pdf

ETSI. (2018, Januari). *ts_125331v111800p.* Retrieved from ETSI: https://www.etsi.org/deliver/etsi_ts/125300_125399/125331/11.18.00_60/ts_125331v111800p.pdf

ETSI. (2019, July). *ts_122101v150700p.* Retrieved from ETSI: https://www.etsi.org/deliver/etsi_ts/122100_122199/122101/15.07.00_60/ts_122101v150700p.pdf

Feedom House. (2018, November 1). *Freedom on the Net 2018 - Ethiopia*. Retrieved July 6, 2019, from Freedom House: https://www.refworld.org/docid/5be16b1a4.html

Fick, M. (2019, August 30). *Ethiopia to install 4G network ahead of telecoms liberalization*. Retrieved from Reuters: https://www.reuters.com/article/us-ethiopia-telecoms/ethiopia-to-install-4g-network-ahead-of-telecoms-liberalization-idUSKCN1VK1KB

Freedom House. (2018, November 1). *Freedom on the Net 2018 - Ethiopia*. Retrieved July 6, 2019, from Freedom House: https://www.refworld.org/docid/5be16b1a4.html

Freedom House. (2018, November 1). *Freedom on the Net 2018 - Sudan*. Retrieved July 15, 2019, from refworld: https://www.refworld.org/docid/5be16af713.html

Freedom House. (2018). *Libya Country Report | Freedom on the Net 2018*. Retrieved from Freedom House: https://freedomhouse.org/report/freedom-net/2018/libya

Gebre, S. (2019, June 13). *Exam Cheats Cited in Three-Day Internet Shutdown in Ethiopia*. Retrieved July 10, 2019, from Bloomberg: https://www.bloomberg.com/news/articles/2019-06-13/exam-cheats-cited-in-three-day-internet-shutdown-in-ethiopia

Gmail. (2019). *Users.drafts/ create | Gmail API | Google Developers.* Retrieved November 12, 2019, from Gmail: https://developers.google.com/gmail/api/v1/reference/users/drafts/create

Heisler, Y. (2012, November 16). *General David Petraeus used clever Gmail trick during affair | Network World*. Retrieved from NetworkWorld: https://www.networkworld.com/article/2223513/general-david-petraeus-used-clever-gmail-trick-during-affair.html

Human Rights Watch. (2019, June 19). *Sudan: End Network Shutdown Immediately*. Retrieved from Human Rights Watch: https://www.hrw.org/news/2019/06/12/sudan-end-network-shutdown-immediately

Human Rights Watch. (2019). *World Report 2019/ Libya | Human Rights Watch*. Retrieved from Human Rights Watch: https://www.hrw.org/world-report/2019/country-chapters/libya

Kidane, S., & van Reisen, M. (2017). Collective Trauma from Sinai Trafficking: A Blow to the Fabric of Eritrean Society. In M. van Reisen, & M. Maware, *Human Trafficking and Trauma in the Digital Era: The Ongoing Tragedy of the Trade in Refugees from Eritrea* (pp. 317-345). Bamenda: Langaa.

Kidane, S., & van Reisen, M. (2018). Trauma van Eritrese Vluchtelingen. In M. van Reisen, & K. Smits, *Eritrea en Eritrese Vluchtelingen* (pp. 125-132). Dutch Central Agency for the Reception of Asylum Seekers (COA).

Latour, B. (1987). *Science In Action: How To Follow Scientists And Engineers Through Society.* Harvard University Press.

Livingston, S., & Bennet, L. W. (2003). Gatekeeping, indexing and live-event news: Is technology alerting the construction of news? *Political Communication*, 363-380.

Maasho, A. (2018, May 23). *Ethiopia opens telecoms sector to limited competition*. Retrieved from Reuters: https://www.reuters.com/article/ethiopia-telecoms/ethiopia-opens-telecoms-sector-to-limited-competition-idUSL5N1SU3A1

Melicherova, K. (2019, May 9). Retrieved June 7, 2019, from https://www.indepthnews.net/index.php/the-%20world/africa/2673-exodus-of-eritreans-in-post-peace-era-continues

NetBlocks. (2019, June 24). *Ethiopia internet shutdown continues following reported coup attempt*. Retrieved July 15, 2019, from NetBlocks Mapping Net Freedom: https://netblocks.org/reports/ethiopia-internet-shutdown-continues-following-reported-coup-attempt-xAG4DmBz

Netblocks. (2019, June 27). *Ethiopia partially restores internet access days after blackout following reported Amhara coup attempt*. Retrieved from Netblocks Mapping Net Freedom: https://netblocks.org/reports/ethiopia-partially-restores-internet-days-after-amhara-coup-attempt-blackout-V8xxlo8k

Netblocks. (2019, July 9). *Sudan internet shows signs of recovery after month-long shutdown*. Retrieved from Netblocks Mapping Net Freedom: https://netblocks.org/reports/sudan-internet-recovery-after-month-long-shutdown-98aZpOAo

NetBlocks. (2019, June 11). *Total internet outage identified in Ethiopia.* Retrieved from NetBlocks: Mapping Net Freedom: https://netblocks.org/reports/total-internet-outage-identified-in-ethiopia-gBLkVoA4

Otieno, D. (2018). *After making peace, Ethiopia and Eritrea now focus on development*. Retrieved July 2019, from AfricaRenewal: https://www.un.org/africarenewal/magazine/december-2018-march-2019/after-making-peace-ethiopia-and-eritrea-now-focus-development

Paravicini, G. (2019, October 31). *Ethiopia says at least 78 people killed in protests last week, number could rise*. Retrieved from Reuters: https://www.reuters.com/article/us-ethiopia-politics/ethiopia-says-at-least-78-people-killed-in-protests-last-week-number-could-rise-idUSKBN1XA21S

Psiphon Inc. (2019). *Psiphon | Uncensored Internet access for Windows and Mobile.* Retrieved from Psiphon: https://www.psiphon3.com/en/index.html

Qian, F., Mao, Z. M., Wang, Z., Sen, S., Gerber, A., & Spatscheck, O. (2010). Characterizing Radio Resource Allocation for 3G Networks. *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement* (pp. 137-150). Melbourne: IMC.

Rebtel. (2019). *Cheap International Calls and Unlimited Calling | Rebtel.com*. Retrieved from Rebtel: https://www.rebtel.com/en/

Ring Around App. (2019). *Ring Around App*. Retrieved from Ring Around App: https://www.ringaroundapp.com

Schoenmaeckers, R. (2018). *Secondary Migration and Mobile Phone Use in Hitsats.* Tilburg: Tilburg University.

Schultze, U., & Boland Jr., R. (2000, September). Knowledge management technology and the reproduction of knowledge work practices. *The Journal of Strategic Information Systems, 9*(2-3), 193-212.

Shafiq, M. Z., Ji, L., Liu, A. X., Pang, J., Venkataraman, S., & Wang, J. (2013). A first look at cellular network performance during crowded events. *ACM SIGMETRICS/international conference on Measurement and modeling of computer systems* (pp. 17-28). Pittsburgh: ACM.

Shoemaker, P. (1991). *Gatekeeping.* Newbury Park, CA: Sage.

Shoemaker, P. J., Eichholz, M., Kim, E., & Wrigley, B. (2001, June). Individual and Routine in Gatekeeping. *Journalism and Mass Communication Quarterly, 28*(2), 233-246.

Strebe, D. R. (2011, August 15). *File/Gall–Peters projection SW.jpg - Wikimedia Commons*. Retrieved from Wikimedia Commons: https://commons.wikimedia.org/wiki/File:Gall–Peters_projection_SW.jpg

Strebe, D. R. (2011, August 15). *File/Mercator projection SW.jpg - Wikimedia Commons*. Retrieved from Wikimedia Commons: https://commons.wikimedia.org/wiki/File:Mercator_projection_SW.jpg

The Economist. (2017, May 25). *Migration from Eritrea slows*. Retrieved from The Economist: https://www.economist.com/middle-east-and-africa/2017/05/25/migration-from-eritrea-slows

The World Bank. (2019). *Ethiopia*. Retrieved from The World Bank: https://data.worldbank.org/country/ethiopia

UNHCR. (2018, December 6). *UNHCR - First group of refugees evacuated from new departure facility in Libya*. Retrieved from UNHCR: https://www.unhcr.org/news/press/2018/12/5c09033a4/first-group-refugees-evacuated-new-departure-facility-libya.html

United Nations. (2017, July 31). *Mobile broadband subscriptions on track to hit 4.3 billion in 2017 – UN report | UN News*. Retrieved 6 8, 2019, from UN News: https://news.un.org/en/story/2017/07/562562-mobile-broadband-subscriptions-track-hit-43-billion-2017-un-report

van Dijck, J., Poell, T., & de Waal, M. (2018). *The Platform Society. Public values in a connective world.* Oxford: Oxford University Press.

van Reisen, M. (2017, March 10). International cooperation in the digital era [Oration]. Leiden: Leiden University. Retrieved from https://openaccess.leidenuniv.nl/handle/1887/51670

van Reisen, M., & Smits, K. (2018). Inleiding. In M. van Reisen, & K. Smits, *Eritrea en Eritrese Vluchtelingen* (pp. 9-15). Dutch Central Agency for the Reception of Asylum Seekers (COA).

van Reisen, M., Gerrima, Z., Ghilazghy, E., Kidane, S., Rijken, C., & van Stam, G. (2018, January). Tracing the Emergence of ICT-enabled Human Trafficking for Ransom.

van Reisen, M., Maware, M., Stokmans, M., Nakazibwe, P., van Stam, G., & Ong'ayo, A. O. (2019). Black Holes in the Global Digital Landscape: The Fuelling of Human Trafficking on the African Continent. In M. Van Reisen, M. Mawere, M. Stokmans, & K. A. Gebre-Egziabher, *Mobile Africa: Human Trafficking and the Digital Divide* (pp. 3-32). Bamenda, Cameroon: Langaa RPCIG. Retrieved November 12, 2019, from Submarine Cable Map: https://www.submarinecablemap.com

van Reisen, M., Maware, M., Stokmans, M., Nakazibwe, P., van Stam, G., & Ong'ayo, A. O. (2019). Black Holes in the Global Digital Landscape: Interrogating Human Trafficking Trajectories on the African.

van Reisen, M., Smits, K., Stokmans, M., & Maware, M. (2019, June 5). The (un)intended role of gatekeepers of information in human trafficking in the Digital Era.

van Stam, G. (2019). Method of Research in a We-Paradigm, Lessons on Living Research in Africa. In *Molecular Logic and Computational Synthetic Biology* (pp. 72-82).

Woodhams, S. (2019, July 15). *Ethiopia's leader promised to protect freedom of expression. But he keeps flicking the internet kill switch*. Retrieved from CNN: https://edition.cnn.com/2019/07/15/africa/ethiopia-internet-shutdowns-old-regime/index.html