**The Politics of Routing**

How Malicious Routing Behaviour Correlates with Freedom

Ben Kendall

BSc Hons Computer Science

[DATE]

Declaration

I certify that the material contained in this dissertation is my own work and does not contains unreferenced or unacknowledged material. I also warrant that the above statement applies to the implementation of the project and all associated documentation. Regarding he electronically submitted version of this submitted work, I consent to this being stored electronically and copied for assessment purposes, including the School’s use of plagiarism detection systems in order to check the integrity of assessed work.

I agree to my dissertation being placed in the public domain with my name explicitly included as the author of the work.

(not sure about that last one…)

Date:

Signed:

Project Supervisor: Dr Vasileios Giotsas

**Abstract.**

In an era of hidden mass surveillance programs that violate human rights, it has become unclear whether a person’s real-world individual freedoms translate into the digital world. The design of the Internet as a global communication network without centralized control, creates challenges for governments who try to restrict freedom of expression. Consequently, governments that suppress individual freedoms tend to exercise tight control over Internet communications to reduce their citizen’s freedom of speech. This report will investigate the distinctions between online and offline freedoms, how different metrics of freedom correlate with nation states and Autonomous Systems (ASes) that participate in malicious routing behaviour and the impacts of their imposed policies.

Contents

[Introduction 6](#_Toc532897284)

[1.1 Chapter Overview 6](#_Toc532897285)

[1.2 Motivation for Research 6](#_Toc532897286)

[1.3 Aims and Objectives 7](#_Toc532897287)

[1.4 Report Structure 7](#_Toc532897288)

[Background Research 9](#_Toc532897289)

[2.1 Chapter Overview 9](#_Toc532897290)

[2.2 The Politics of Routing: Investigating the Relationship between AS connectivity and Internet Freedom 9](#_Toc532897291)

[2.3 Nation-State Hegemony in Internet Routing 10](#_Toc532897292)

[2.4 Quantifying Information Exposure in Internet Routing 11](#_Toc532897293)

[2.5 Schengen Routing: A Compliance Analysis 11](#_Toc532897294)

[2.6 Politically Motivated DDoS 13](#_Toc532897295)

[2.7 Related Work 13](#_Toc532897296)

[Freedom 14](#_Toc532897297)

[3.1 Chapter Overview 14](#_Toc532897298)

[3.2 Defining Freedom 14](#_Toc532897299)

[Malicious Routing 15](#_Toc532897300)

[4.1 Chapter Overview 15](#_Toc532897301)

[4.2 What is Malicious Routing 15](#_Toc532897302)

[4.3 Nations and Autonomous Systems 15](#_Toc532897303)

[4.4 Methodology 15](#_Toc532897304)

[4.5 Correlations 15](#_Toc532897305)

[Trends and Impacts 16](#_Toc532897306)

[5.1 Chapter Overview 16](#_Toc532897307)

[5.2 Policy 16](#_Toc532897308)

[5.3 Case Studies 16](#_Toc532897309)

[Findings 17](#_Toc532897310)

[6.1 Chapter Overview 17](#_Toc532897311)

[Conclusions 18](#_Toc532897312)

[7.1 Chapter Overview 18](#_Toc532897313)

[References 19](#_Toc532897314)

Chapter 1

# Introduction

## Chapter Overview

This chapter will explain the reasons for conducting this research and the potential benefits that may come of it. An early approximation of what could be achieved by the report’s aims and objectives will also be laid out. These are dynamic objectives and may be added to or adjusted depending on how the results shape up. The report’s general structure will also be outlined, and each section explained.

## Motivation for Research

In June 2013, Edward Snowden stole and leaked an estimated 1,500,000 documents exposing the colossal power and capability of intelligence agencies such as the National Security Agency (NSA, US) and their Five-Eyes (FVEY) partners. It was revealed that mass surveillance tools such as “PRISM” [1] and “X-KEYSCORE” [2] provided the capability to collect and search through millions of people’s digital lives. It was also revealed that many Autonomous Systems (ASes) and Internet Service Providers (ISPs) such as British Telecom, Vodafone Cable, Verizon Business, Level 3, Viatel, Global Crossing and Interoute were collaborating with projects such as “TEMPORA” [3] which tapped fibre optic cables and intercepted dataflows. It seemed that the online world was far less private or free than previously realised.

In parallel with the aforementioned revelations, global freedom has been in continual decline for 12 consecutive years [4]. The internet, as an openly accessible and free network, affords freedom of expression, information, religion, identity and trade as laid out by the Human Freedom Index 2018 [5]. Therefore, a decline in internet freedom must be the result of restrictive policies imposed by government, ASes or ISPs. For example, since the Snowden leaks of 2013 and the Investigatory Powers Act of 2016, the UK has dropped 12 places on the Freedom of the Press Index [6]. Restrictions of internet freedom such as these fall under the umbrella term ‘malicious routing’. This report will investigate how these malicious routing policies correlate with an individual’s internet freedom.

## Aims and Objectives

The aims of this report are therefore as follows:

* Determine what it means to have ‘total internet freedom’ and what positive and negative freedoms make up internet freedom.
* Discover the extent to which a correlation exists between a nation’s malicious routing behaviours and the freedom of their citizens.

From the report’s aims, the formal objectives are:

* Form and collect information about each nation’s malicious routing behaviours.
* Analyse and rank nations based on their malicious routing activity.
* Compare each nation’s propensity to engage in malicious routing activity with various measures of their freedom to determine the degree to which they are correlated.
* Consider whether the finding are significant and determine whether propensity to engage in malicious routing activity is a good predictor of freedom.

## 1.4 Report Structure

This report will begin with a review of the relevant existing research surrounding malicious routing. This will help gain a more comprehensive understanding of the current academic reasoning, backgrounds and issues faces in this area of research. The existing research associated with defining and measuring freedom will also be investigated to aid with narrowing the selection of freedom indexes to the most relevant for this topic.

A nation’s freedom can be measured in a wide variety of different ways, each resulting in a different freedom index. Before any research is conducted into malicious routing, the report will cover the various definitions of freedom and determine which indexes are most applicable when correlating with malicious routing. The primary index to be considered will be the Freedom House, Freedom of the Net Index [9]. This index will also function as a prediction for the most closely correlated index and will also help determine whether the best predictor of internet freedom is a nation’s propensity to conduct malicious routing activity.

The main section of the report will focus on the technical aspects of malicious routing in defining its component elements, examining the nations that partake in it and finding any correlations with freedom. This will begin by accurately defining what actions and policies malicious routing comprises of. Then a table of nations that partake in malicious routing will be built, holding information about the activities of each nation, as well as a standardised numerical score for each nation based on the amount of malicious routing behaviour that said nation conducts. Once the table has been created and the ranks calculated, it will then be possible to contrast malicious routing behaviour with freedom to determine if any correlations are present.

Depending on the results from the correlations, there may be clear connections between certain kinds of malicious routing behaviour and freedom. This next section will examine trends seen across the data as well as stand-out and edge cases. This will be followed up with the ‘findings’ chapter that will contain a careful analysis of the results and a critical review of the methods used. Finally, the report will end with conclusions based on the research and a discussion of the limitations and lessons learnt, as well as any possible future work.

Chapter 2

# Background Research

## 2.1 Chapter Overview

This chapter will briefly summarise what has been learnt from existing research papers about closely related topics. The focus is on malicious routing, however some papers regarding the definitions of freedom have also been included to help form a better understanding of how the varying ideas of freedom can be combined to create an index.

Due to the nature of this project, some information, such as the Snowden leaks which predominately came from news outlets like The Guardian, will be found outside of academic papers. In such a case, only reputable sources of information will be used.

## 2.2 The Politics of Routing: Investigating the Relationship between AS connectivity and Internet Freedom

This study, conducted by Rachee Singh et al, aims to find a relationship between the level of Autonomous System connectivity within a single country, and that country’s Internet Freedom [7]. A network topology graph was constructed for each nation using a BGP path simulator to compute AS paths that are compliant with routing policy. Features of this graph were then extracted and applied to various machine learning techniques that tried to predict freedom.

In this paper, internet freedom of a nation is measured using the Freedom House, Freedom of the Press Index [8]. However, while closely related in legislation, the freedom of individuals online is fundamentally different from the freedom of the press, since there are fewer social and economic constraints acting on a single internet user. Where the vast majority of the press operate in a profit-driven environment, in which straying from the overton window could damage sales, an individual internet user operating under perceived anonymity is somewhat relieved from such pressures, and therefore is more likely to share nonconforming or illegal material. Therefore, this report will primary focus on measuring internet freedom with the newer and more closely related Freedom House, Freedom of the Net Index [9]. The actual differences between these indexes will be investigated in more detail later in the report.

The study found that, of all the graph’s features, IP density and path length were the best predictors of internet freedom. Their machine learning algorithms were able to predict a nation’s freedom category (Free, Partially Free, Not Free) with a 95% accuracy. I will follow a similar method when defining the features that malicious routing comprises of. It will also make an interesting comparison to see whether the correlations between AS connectivity and internet freedom mirror the correlations between malicious routing and internet freedom.

## 2.3 Nation-State Hegemony in Internet Routing

This paper researches the extent to which various countries are dependent on the United States and other Western nations to connect to popular internet destinations [10]. In general terms, their results show that underserved regions of the globe are dependent on North America and Europe. In some cases, over 85% of traffic from an independent nation was routed through another country such as the United States. However, they also found that by using Region Aware Networking, they were able to route traffic away from these hegemonies with middle to high success rates.

This is significant since the level of malicious routing that a nation’s citizens are exposed to extends beyond just the country they live in and includes nearby hegemonic nations where traffic is likely to be routed through. It will be worth considering the impact and measurability of this when defining what constitutes as malicious routing. It also brings up the question of whether nations should be judged based on solely their own policies, or whether neighbouring hegemonic entities need to be taken into consideration.

## 2.4 Quantifying Information Exposure in Internet Routing

In close relation to the last paper [10], this paper measures the extent to which communications between pairs of countries are exposed to other countries [11]. They found that, even in physically adjacent countries, there is a high level of information exposure. Typically, even short paths route through at least 3 separate countries. It was shown that the better connected a country is, the more their information is exposed and there is a trade-off between robustness and information exposure. It was found that having many independent routing paths between nations is the features of robustness that directly increases the level of information exposure. This is because internet routing is ‘best effort’ and if there are many alternate paths available, then there is a higher chance one of those paths will be chosen.

When defining exposure to malicious routing, it will be important to include whether the nation in question has many independent paths. With a greater number of paths to choose from, the likelihood of a packets taking an alternative path increases. If these alternative paths route through a nation that performs malicious routing, then the likelihood that the original data packet could be intercepted or observed increases. To quantify this chance, a function that takes a nation’s proximity with countries that perform malicious routing, and that nation’s number of independent paths will be created.

## 2.5 Schengen Routing: A Compliance Analysis

As explored earlier, due to the internet’s best effort approach to packet routing, there is a chance that packets will unnecessarily pass through additional nations before reaching the destination. To try to counteract this, European intelligence agencies developed Schengen Routing. The aim of which is to make sure that when the sender and receiver are both within the Schengen area, their packets are entirely routed within the Schengen area.

This paper [12] investigates weaknesses of Schengen Routing, specifically looking into the compliance of available routes and the amount that any nation uses Schengen compliant routes. The paper found that up to 39.7% of routes within the EU were Schengen compliant and compliance levels for individual countries ranged from 0% to 80%. The choropleth map shown in *figure 1* has been extracted from the report and shows compliance levels by nation within the EU.



Figure 1: Schengen Routing compliance levels

This is a prime example of legislation that helps reduce the exposure to malicious routing. However, this only affects a small proportion of the world, so when quantifying malicious routing, some nations will be subject to unique features that are not applicable to others. Therefore, it may be necessary to assess the impact of legislation such as this for each nation individually.

## 2.6 Politically Motivated DDoS

This paper [13] documents and analyses the reasons behind many of the recent denial of service attacks directed from governments. It documents the nations involved, their expected reasons and the result of the attack.

The records from this paper will be used alongside the DDoSDB [14], a database that records global denial of service attacks, to gauge an idea of the nations involved in orchestrating DDoS attacks. This information will then be used to help define a nation’s propensity to conduct malicious routing, as well as the exposure of other nation’s to malicious routing activity.

## 2.7 Related Work: Freedom Indexes

Measurements of freedom will provide a necessary backbone from which any correlations with malicious routing will be found. There are many various measurements of freedom and freedom indexes available online. For this project, the primary freedom index that will be contrasted is the Freedom on the Net Index 2018 [15]. This is because we predict that malicious routing behaviour will correlate closest with internet freedom.

However, predictions are frequently wrong, therefore other freedom measures listed below will also be analysed.

### 2.7.1 Freedom on the Net 2018

[15] This will be the main index that malicious routing in contrasted with. The index covers 65 countries and 87% of the world’s internet users. It’s divided into 3 main features that are analysed for each country individually:

* **Obstacles to access**

Referring to how difficult it is for an individual to get online.

* **Limits on content**

Referring to top down restrictions on what can and cannot be shared online.

* **Violation of user rights**

Measures legal protections and restrictions on online activity.

### 2.7.2 Freedom of the Press 2017

As used in 2.2 [7], (The Politics of Routing) Freedom of the Press [16] has been used in the past as a good measure of individual freedom and freedom of speech. While it has its limitations, as outlined earlier, its rankings are significantly different from the Freedom of the Net Index and may provide an additional interesting correlation to explore.

### 2.7.3 The Human Freedom Index (*updated for 2018*)

This index [17] focus’ on overall freedom of a nation’s citizens, taking over 100 features divided into personal and economic freedoms. It will be interesting to compare the results from this very broad index, with the more specific indexes mentioned above. It may also provide an interesting analysis to try to find the single feature from this index that correlates best with malicious routing propensity.

## 2.8 Related Work: Data Logs

### 2.8.1 Bad Packets Report (Ongoing)

The Bad Packets Report [18] scans for botnet activity that is based on the original Mirai source code. Mirai’s TCP sequence numbers will equal the value of the target’s IP address. The report records the source nation, IP and AS of Mirai-like packets and publishes them online. The information here will be a useful feature in determining a nation’s propensity to conduct malicious routing.

### 2.8.2 BGPMON (Ongoing)

BGPStream [19] records hijacks, leaks and outages in BGP. The service records the length of the outage and the AS that it occurred in. It’s intended for network engineers to work around outages, however it will also be useful for this report since the affected nations are also recorded. This information will aid in calculating the exposure to malicious routing, although it must be noted that not all BGP outages stem from malicious intent.

Chapter 3

# Freedom

## 3.1 Chapter Overview

Sample text

## 3.2 Defining Freedom

Sample text

Chapter 4

# Malicious Routing

## 4.1 Chapter Overview

Sample text

## 4.2 What is Malicious Routing

Sample text

## 4.3 Nations and Autonomous Systems

Sample text

## 4.4 Methodology

Sample text

## 4.5 Correlations

Sample text

Chapter 5

# Trends and Impacts

## 5.1 Chapter Overview

Sample text

## 5.2 Policy

Sample text

## 5.3 Case Studies

Sample text

Chapter 6

# Findings

## 6.1 Chapter Overview

Sample text

Chapter 7

# Conclusions

## 7.1 Chapter Overview

Sample text

# References

[1] Glenn Greenwald. NSA collecting phone records of millions of Verizon customers daily | US news | The Guardian. [ONLINE]. 6th June 2013. Available at: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. [Accessed 09 December 2018].

[2] Glenn Greenwald. XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. The Guardian. [ONLINE]. 31st July 2013. Available at: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data. [Accessed 09 December 2018].

[3] John Goetz and Frederik Obermaier. “Snowden reveals the names of the peering telecom companies.” Suddeutsche Zeitung, 2 Aug. 2013.  <https://www.sueddeutsche.de/digital/internet-ueberwachung-snowden-enthuellt-namen-der-spaehenden-telekomfirmen-1.1736791> [Accessed 24 Oct. 2018].

[4] Freedom House USA. “Democracy in Crisis.” Freedom in the World Index 2018. 2018 - ongoing (updating)  <https://freedomhouse.org/report/freedom-world/freedom-world-2018> [Accessed 24 Oct. 2018]

[5] CATO Institute. “Human Freedom Index.” The Human Freedom Index – 2018. <https://www.cato.org/human-freedom-index> [Accessed 10th December 2018].

[6] Damien Gayle. “Downward spiral: UK slips to 40th place in press freedom rankings.” The Guardian. 26 Apr 2017. <https://www.theguardian.com/media/2017/apr/26/uk-world-press-freedom-index-reporters-without-borders> [Accessed 20 Oct. 2018]

[7] Rachee Singh et al.  “The Politics of Routing: Investigating the Relationship Between AS Connectivity and Internet Freedom.” Stony Brook University. 2016. <https://people.cs.umass.edu/~phillipa/papers/foci16-final16.pdf> [Accessed 20 Oct. 2018]

[8] Freedom House. “Freedom of the Press Index”. 2018 – ongoing. https:// freedomhouse.org/report-types/freedom-press. [Accessed 12th December 2018].

[9] Freedom House. “Freedom of the Net Index”. 2018 – ongoing <https://freedomhouse.org/report/freedom-net/freedom-net-2018> [Accessed 12th December 2018].

[10] Anne Edmundson et al. “Nation State Hegemony in Internet Routing”. Princeton University. 2018.  <https://www.cs.princeton.edu/~jrex/papers/compass18.pdf> [Accessed 20 Oct. 2018]

[11] Peter Mell et al. “Quantifying Information exposure in Internet Routing”. National Institute of Standards and Technology. 2016. https://ws680.nist.gov/publication/get\_pdf.cfm?pub\_id=925224 .

[Accessed 17 Dec. 2018]

[12] Daniel Donni et al. “Schengen Routing: A Compliance Analysis”. University of Zurich. 2015. <https://files.ifi.uzh.ch/CSG/staff/doenni/extern/publications/Schengen_Routing_A_Compliance_Analysis_AIMS_2015.pdf>.

[Accessed 17 Dec. 2018]

[13] Jose Nazario. “Politically Motivated Denial of Service Attacks”. Arbor Networks. 2016. <http://www.senki.org/wp-content/uploads/2017/10/12_NAZARIO-Politically-Motivated-DDoS.pdf>

[Accessed 17 Dec. 2018]

[14] “Distributed Denial of Service Database”. University of Twente. Ongoing. <https://ddosdb.org/help> [Accessed 17 Dec. 2018].

[15] Freedom on the Net 2018. Freedom House. 2018. Freedom on the Net 2018. Available at: https://freedomhouse.org/report/freedom-net/freedom-net-2018. [Accessed 19 December 2018].

[16] Freedom of the Press 2017. Freedom House. 2018. Freedom of the Press 2017. Available at: https://freedomhouse.org/report/freedom-press/freedom-press-2017. [Accessed 19 December 2018].

[17] Fraser Institute. 2018. The Human Freedom Index 2018 | Fraser Institute. Available at: https://www.fraserinstitute.org/studies/human-freedom-index-2018. [Accessed 21 December 2018].

[18] Mirai-like Botnet. 2018. Bad Packets Report. Available at: https://mirai.badpackets.net/. [Accessed 21 December 2018].

[19] BGPStream. 2018. BGPStream. [ONLINE] Available at: https://bgpstream.com/. [Accessed 21 December 2018].

[20]