THE DARK WEB

FOR THE RATIONAL

linkcabin

I dedicate this book to the late Heather Heyer, Barnaby Jack, Aaron Swartz and Jo Cox.

ABOUT THE AUTHOR

My first name is Jack. I am a security researcher who is interested in many subjects not only limited to IT security. I aim to make positive changes in the world for the vast amount of people and not a small pocket of people. This book was written while I was in university and also after I graduated.

Website: https://itsjack.cc

Twitter: https://twitter.com/linkcabin

ABOUT THE COVER

The cover was made by selecting all of the client side code from a popular ‘dark market’ forum and appending it into the image of the ‘Silk Road’ camel commonly associated with the famous ‘Silk Road dark market’ which was run by Ross Ulbricht. The code is appended by using a hex editor, which is then later viewed by an early version of MS paint which renders the appended client side code into a distorted form. This was then copied and stretched to produce the background of the cover, essentially providing a visual representation of the HTML/CSS/JS code from the ‘dark market’. The ‘Silk Road’ camel was then put on top of the distorted background.

CONTENTS

PREFACE

The ‘dark web’ is a common phrase that’s used to describe parts of the internet that supposedly is mysterious, full of terrors, that are too dark to describe to the many. The most common stories on the ‘dark web’ are usually drugs, hacking, paedophilia, red rooms, hitmen and guns. For journalists, the dark corner of the internet is a fantastic opportunity for internet hits and for an interesting story to write up, but, it is not completely true. Many parts of this mysterious place are a misconception developed by many to sell products and also to sell stories, in reality, it’s sadly less sexy than most would think. The loose definition of ‘dark web’ or ‘deep web’ is a website that is not indexable by search engines, such as Google or Bing, most sites disallow access to some pages to be indexed, but very few allow no content to be indexed. Throughout this book I choose to put ‘dark web’ under quotations, I believe it is an incorrect term given to describe the network and therefore decide it needs to be highlighted as incorrect. I also wish to highlight through this book that I use ‘TOR’ as the way to display The Onion Router project, although many from the project use Tor, there is no real difference, I am simply more comfortable with TOR as I think it’s correct. It’s little, but I’m sure someone will take note of it, in conclusion the official way to write it, is Tor. The main reason for me describing this as a loose description is that it is also impossible for search engines like Google or Bing to correctly index some pages that are deemed in the ‘dark web’, as you require other technologies to access such a page, technologies like TOR. Many web resources on the ‘dark web’ are depict the ‘dark web’ as a hard to reach place that only a few know how to reach, making it an attractive story and something that many people will seem interested in knowing. It is in actual fact very easy to access some ‘dark web’ sites through software known as TOR, or more precisely, the TOR browser. TOR stands for **T**he **O**nion **R**outer, a project which was initially released in 2002. It is freely available to download and builds on top of the Firefox browser to allow you to access ‘onion’ sites. In 2015 on August, the term ‘dark web’ reached its peak in interest on Google, this looks to be mainly because of the release of the film ‘Deep Web’ which aims to tell of the story of Ross Ulbricht, the alleged owner of infamous drug site Silk Road. This story alone has produced a vast amount of interest towards the ‘dark web’, what it is and why people use it.

I think the ‘dark web’ is misunderstood, it isn’t dark, and it isn’t even a web. It’s arguably a group of projects which initially attracted various users, who can be indeed paedophiles and drug salesman, but can also be spies and journalists. The ‘dark web’ can help in alleviating censorship in totalitarian regimes to every day citizens, it can also help paedophiles escape justice. There are many different variants to what the media broadly calls the ‘deep’ or ‘dark’ web. A better term could be ‘anon-web’, the aim for users of a network to be anonymous and untraceable, allowing freedom of speech to thrive. But as I discuss in later chapters, complete anonymity is something relatively questionable, so would be a

slightly inaccurate term. This area of work is more political than technological, many projects around this area of work exist, but are depicted as ‘dark’ or ‘deep’ to produce the idea of being undesirable or unreachable. The argument that is currently in question is how far we can allow freedom of speech in technology, libertarians wish for anyone to be able to view any information they wish without intervention from other third parties. This is of course a fundamental belief in libertarianism and has been previously crushed with the internet, where censorship and manipulation is quite prevalent in various areas of the world. Many like the idea of freedom of speech when it is seen positively, removing censorship barriers from dictatorships, allowing communication through revolutions and allowing journalists to do their job safely and securely. The trouble that many have, is sadly, freedom of speech doesn’t just have positive points, there has to be an appetite of how much freedom you give people to ensure there is some level of order. This argument is why so much energy is put upon this subject, do we accept the consequences of having a much freer society where people do not need to worry about their opinion being ‘incorrect’ or a society where users must be analysed, tracked and searched to ensure that sections of society are kept safe in some manner. The issue of it being technological means many generations of users don’t understand the issue, much like the internet, which is still hardly understood by many in American or UK political parties. With this hurdle in place where technical points are missed, many do not look at the core question of the subject, which is freedom of speech. Instead, we refer to such a network as ‘dark’ or ‘deep’ a mysterious, warped place, where only the worst of society go to.

The ‘dark web’ can also been seen in a similar light to what happened with cryptography in 1990’s, known as the ‘Crypto Wars’, where America produced restrictions on the access of strong cryptography. This ‘war’ was very much on intelligence agencies being able to *decrypt* any communication or data. This ‘war’ almost re-emerged in Britain when David Cameron decided to make a speech advocating backdoors in cryptography, this later came to no avail. The main reason why nothing further was done in regards to backdoors in cryptographic products was most likely because of fears of attack vectors on businesses being widened because of backdoors. The misunderstanding of the technical points by politicians means security in general, not just cryptography, is therefore sometimes attacked. An argument again exists in the ‘crypto wars’ which is similar to the ‘deep web’ on freedom of speech, and what various parts of the world think of it. The aim of writing this book is to identify really what is what many call the ‘deep’ or ‘dark’ web, why many people are wrong with many points that are made against the mysterious network and shed light on many intricate parts of such a system. This book obviously cannot be completely conclusive, there are various projects in regards to anonymous networks which all have different solutions. I want to be able to provide an overview of an increasingly important place on the internet that in my view is misunderstood, many technical features of anonymous networks are exploring ideas that could be introduced for the security of everyone around the world on the internet. TOR is the largest project in anonymous networks and there I only reference others networks such as I2P. The TOR network is relatively mature and will be the only focus in this book, other anonymous networks will hardly be touched upon. I decided to write this book in this way because many individuals don’t take too much notice of other anonymous networks such as I2P due to how extensive TOR is. I do not wish to cast these projects adrift, I am simply writing about the most popular network to ensure people can refer to this book easily. There are parts of this book which become fairly technical and may be hard for a non-technological reader to follow, the terms and the ideas made in this book can be researched with relative ease and are not too deep if one wishes to completely follow. There is enough content which is intentionally not technological, this is the core idea of this book, to provide people with little knowledge of technology to understand somewhat, what the

'dark web' is. The issues that arise from anonymous networks like TOR do not involve exclusively technological issues, there are many moving parts to the network that can be interesting to every day citizens of the world. One other thing I wish to mention is the amount of events happening while I write this book, at the end of writing this book I am suddenly hit with the news another child pornography site has been taken down by the name of 'Childs Play', the largest site of its kind, far outperforming 'PlayPen' which is referenced in this book. It shows the disturbing trend that more and more users are finding these pockets of hidden services to which they register and take part in. Elysium, another child pornography site was also taken down while I was writing this book. In regards to drug markets, the main marketplaces taken down were 'AlphaBay' and 'Hansa'. I actually write in parts of this book how big AlphaBay is, but should be noted it has now been taken down, I do point this out at points but do not do this at every point. This writing project took me around half a year and shows anarchic and ever-changing the largest anonymous network is, the only think I can tell you, nothing is static on the 'dark web'. This can be true of the internet, but the 'dark web' changes so often, it is so isolated, that many may not even know the changes that have happened. The internet is surveyed more, it is far easier. I have extensively researched in this book and hope nothing is incorrect, if you do notice something that is incorrect you can contact me to notify me what I got wrong.

I wish that this book allows readers of all technological ability to at least learn one thing from not only anonymous networks but other subjects I discuss. I think it's important that people from technology backgrounds immerse others with knowledge that allows for better decision making, at this moment of time I do not think this is the case. Many may read this book and see it is quite centred on America and the UK, this is simply because I live in the UK, and am far more aware of the politics of my country. I have also provided a large amount of references to other countries which I label oppressive but hardly touch upon issues in westernised countries such as my own, this is not my intention to assume my country has the best model in regards to censorship/privacy/free speech, I do have the view that many countries outside of the European block are increasingly using far more restrictive measures than one would see in Europe. This is, of course, a view of my own. I try to fray away from imposing too much of my views on subjects discussed in this book, but it is impossible to explain a subject in detail without certain views being outlined. I guess it is for the reader to take their own views and decide what they think, which is what most authors would prefer, instead of completely spoon feeding a reader. I am not a natural writer, I come from a technology background, security specifically. There will be mistakes, in fact I can guarantee there will be issues with my grammar. I apologise for this, but I am still learning the process of writing, I hope my mistakes do not distort the ability to read this book well, I've taken a large amount of time and put considerable effort to produce this book. I've had an issue with how the 'dark web' has been portrayed for some time and decided to take a challenge this year, to write a book. Something many attempt, but a considerable portion never fully commit. I can understand why, it can consume your thoughts and your life for many hours in the day, it can also be lost some weeks where you never think about it. At times, I thought this book would never be finished, but I'm relatively happy that I got it to a point where I'm happy with a release. The research for this book was not only from court documents, articles and films that I was looking at, but some chapters I have put my own research into the book. There is an endless amount I could discuss, but you do not wish to drown a reader with information which is aimed at all levels. Hopefully, I have achieved this somewhat.

CHAPTER 1

THE BIRTH

The most popular anonymous networking project by far has already been given to the reader, the TOR project. The TOR project was, like the internet, at first a military project where many parts of TOR was developed under DARPA. The project later developed away from the US military and became a non-profit organisation, where funding came from a number of sources like the EFF but also still notably the US government. In 2013, Alex Hurn from The Guardian highlighted how the US government were increasing the funding of TOR, giving a staggering $1.8m to the project [1]. The US government has been the highest donor to the project for the majority of the projects life, which leaves many privacy advocates uncomfortable and cynical in the projects intentions. TOR, in 2017 is ultimately the most popular choice in regards to anonymous networking software, it is regularly maintained and has a slew of donations that allow it to continue growing. I2P is an alternative to TOR, the difference being it has significantly less funding and less developers. It is a little bit more mysterious than TOR due to the developers only being known by computer “handles” (Alternative names) and it being much smaller in organisation. The project does not have regular funding organisations like TOR but rather one off donations from organisations who support open source software or individuals who believe in the project. An I2P lead developer, ‘jrandom’, went AWOL in 2007 but the project continued and still has builds developed in 2017[2]. I2P may have far less resources and publicity when it comes down to anonymous networking but still has some interesting concepts for developing privacy for all and evading censorship. Users of the projects TOR and I2P often have sites available on both platforms, I2P is by no means a hobby project and has genuine users utilising its network every day. These two projects are the most well-known ‘anonymous’ networking projects that are still active in 2017, these two are lumped into the ‘dark web’ terminology by the media even though you would require different software to access ‘I2P’ sites or ‘Onion’ hidden service sites (TOR Websites). There are also other anonymous networking projects of course, but I feel these two are the most important out of the long, long, long, yes long list of anonymous networking projects out there. Due to the amount of funding TOR has, it is very well known compared to its alternative, I2P, it has been used by many journalists to evade capture and films are also referencing the software, although please, don’t make me list them. I2P has a more focused base of users who believe in privacy and freedom of speech, there are very few news pieces that refer to it in any context of ‘dark web’ or anything at all. These two projects are inter-connected only by the goal of the projects, to produce anonymous networking which aims to evade censorship and manipulation from third parties. They are in no way able to be connected in

anyway, and therefore cannot be defined as a ‘web’. Primarily these projects try to keep an individual’s identity to themselves, the identity of a user can be powerful when you are aware of their online habits. People act differently online to how they do offline and it is seen by some that absolute anonymity is required to keep people safe.

The term for ‘web’ is also technically incorrect for TOR, when used in the ‘dark web’ context. Research has been produced on the ‘dark web’ which provides some answers for this networks interconnectivity. The research was produced solely on sites that use the ‘.onion’ domain, the ‘.onion’ domain is an indicator of TOR project. ‘onion’ is a top level domain specific to the TOR project, it is much like other top level domains like ‘.com’ and ‘.org’ but can only be routed correctly through the TOR network. If someone was to enter an onion domain on a normal browser with a normal network configuration, it would simply reply with a DNS error. Onion top level domains allow access to hidden services within the TOR network, essentially, websites with an onion domain that can only be accessed through TOR. These hidden services are what many define as the ‘dark web’, although, it can get rather confusing. It seems everyone has a different definition for what ‘dark web’ means, mostly down to misunderstanding of anonymous networks. For the basis of this book, we take the assumption that the ‘dark web’ is a collection of hidden services not limited to TOR but all anonymous networks that can only be accessed through an anonymous network. What the researchers found in this study is that 87% of ‘onion’ sites do not link to another onion site at all, which is completely different to the internet or the idea of a ‘web’ [3]. This makes the majority of ‘dark web’ sites isolated in some manner, but not in-accessible. Large portions of onion sites are posted on what many call the ‘clearnet’. ‘Clearnet’ is essentially another term for the internet, although this can also be debated, we will refer to ‘clearnet’ as traffic which is not within an anonymous network, which is easily crawled by search engines. This can be confusing for many I understand, as we also have the term ‘deep web’ which is used by many, but I am going to be simply lumping this into ‘clearnet’ in this book for simplicity. You can learn about the definitions of all from the internet, although, you may get confused by how different many portray some of the words. In this book there is only anonymous networks and no anonymity networks. There are devoted sites for updating and showcasing onion links on the ‘clearnet’ allowing many to have knowledge of drug marketplaces and such, there are very few useful resources within TOR that give you good updated links to accessible sites. Most search engines that are within the TOR project have dead onion links, where a link has been submitted and either the onion address has changed or the administrator has taken it off of TOR.

‘Isolated dark silos’ is a term introduced by the researchers as a more accurate description, which is a true characterisation of how the ‘dark web’ operates in my opinion. The TOR project has ‘onion’ sites which are chaotic; many are experimental and others are constantly changing. The idea that it is a ‘web’ is quite incorrect, there are very few, which is highlighted in this study that actually link with each other to make a ‘web’. This isn’t primarily due to how TOR is designed, but more of the mind set of onion site administrators. The content that some hidden services have are minimal, most are experimental or not responding and so therefore don’t link with others. Many hidden services also are simply self-serving, there is no reason to link outside because everything is simply available on the hidden service that they have developed. The erratic nature of TOR onion sites allows for many scams to take place. There is a vast amount of downtime on many hidden services, even popular ones, this depicts how unstable the ‘dark web’ can be. With popular drug marketplaces, when reviewing the uptime of the marketplaces available on the ‘dark web’, there is not one that is 100%. There is a common misconception that hitmen are available on the ‘dark web’, which allow individuals to scam

TOR users often, the idea that there are hundreds of hitmen who develop websites for jobs on the ‘dark web’ is quite simply, ludicrous [4]. Individuals less aware of what the ‘dark web’ actually contains fall for hitmen scams, to which many posing as hitmen services are law enforcement. There are numerous examples of individuals being scammed by fake hitmen services on the ‘dark web’ mostly due to people buying into the idea that criminal gangs utilise crypto-currencies for payment in hits, an idea that is mostly facilitated by the media. Even Ross Ulbricht, the ‘Silk Road’ owner, allegedly wanted to hire a hitman and was scammed, it was carried out by law enforcement who faked the murder of the target. The fluid network landscape of the ‘dark web’ means individuals who use the ‘dark web’ should be cynical to dish out varying amounts of trust to others, as it is so easy to be scammed. But of course, many do not.

The constantly connected internet or ‘web’ has very different properties currently than what these researchers define as the ‘dark web’, this does not mean it will not change, but as of right now it is isolated by the chaotic development of onion sites which go up and down often. What is interesting to note is how the internet or ‘web’ and the ‘dark web’ have a very close relationship, the popular ‘clearnet’ site Reddit has forums that have user reviews on various dark sites such as the infamous drug site ‘AlphaBay’ and suppliers that are available on these markets. Large portions of information that many would think are secret are openly available to many on the internet. Other portions of Reddit are also devoted to ‘Darknet’ markets overall, containing information on ‘Dream Marketplace’ and ‘Hansa’ too (other marketplaces available on the ‘dark web’). The main reason for ‘dark web’ sites not requiring links to other pages is because they advertise on the internet, the isolation is a current feature of the ‘dark web’ because there isn’t a thorough way of indexing ‘dark web’ pages. In fact, the TOR project would rather it wasn’t possible to index hidden services so easily and is beginning to make design changes where it will not possible to crawl through the ‘dark web’ so easily. Many hacking forums, drug markets and fraud shops that are accessed through the ‘dark web’ using an onion domain can also be accessed through the internet or as some refer to it, ‘clearnet’. This is entirely down to the hidden service operator’s discretion, there is the ability to have users access through domains like ‘.com’ and ‘.onion’, although the security benefits of TOR hidden services won’t be carried onto ‘clearnet’ visitors. This is sometimes due to members not particularly trusting ‘dark web’ software such as TOR or administrators wanting to appeal to wider audiences, some criminals aren’t as technological but still may want to access to the services these provide. There is a worry from many criminals and users of fraud shops and hacking forums that using TOR or other anonymous networks makes you a much larger target than rather using traditional cloaking technologies like a VPN. This is certainly up for debate, anonymous networks rely on a high number of users in the network to make it hard to differentiate between identities. If there are a small pool of users in an anonymous network, it becomes much easier to understand the behaviours and activities of an individual. What is quite obvious is that these anonymity networks are far from perfect, I2P still prefers to be labelled in beta in its development. TOR is also not perfect either, participants of these projects have been arrested, sometimes for simply operating a ‘Tor Node’ as is the case for Russian Maths instructor Dmitry Bogatov [5]. These arrests leave many wary of utilising such networks because they may be targeted by authorities from their country, although, people using TOR overall has increased significantly. Many reading should note that Dmitry Bogatov was arrested for operating a ‘Tor Node’ or ‘relay’ as it is commonly described, this is very different from actually using the network, although again criminals have of course been arrested for their activities within the network. The ‘dark web’ looks to be in its infancy and therefore isn’t as connected as many may think, there are small pockets of organised groups and individuals who utilise this platform for their own, but there are certainly considerably more who are less organised. If and

when it does develop into something more mature is a valid question, the technology for anonymous networks is certainly advancing, but the culture around it is full of individuals who want to access the ‘dark web’, not enrich it at this time.

TOR technology requires volunteers to generously donate ‘servers’ that allow traffic to pass through in some way, be it transferring information to another ‘relay’ or having the responsibility of protecting the user or server (This discludes the event that the user requests a network resource outside of the TOR network, to which an exit node must request, we’ll talk more on this later on). The system is similar to the internet in which it requires ‘nodes’ to route traffic but is done in a way that the internet, does not. TOR has the main aim of keeping individuals identities hidden, for this to be possible the system is designed to ensure that both points of a connection do not know the address of one another. TOR uses ‘nodes’ to pass information between a *client* and a *server*, these nodes are used as a go between and these nodes only know who they are sending to and who they are receiving information from. With these nodes in the middle of a connection between a user and a server, both the server and client will only talk to a node and not to each other. Nodes is a common term used in networking, this is the term I’ve first started to use for people with a networking background to understand, nodes are commonly understood as ‘relays’ in TOR.

These nodes that are in-between the user and the host are donated and administered by volunteers who believe in the TOR project. One ‘node’ or ‘relay’ is specifically tasked with being the last ‘relay’ in the chain, if a user requests a resource which is outside of the anonymous network, these nodes, which are known as ‘exit relays’ will communicate outside of the TOR network for the user who requested the resource. There are some risks for operating what is called an ‘exit node’ or ‘exit relay’ which is one of four types that can be in-between a user and a host. These exit nodes are essentially connecting to services on your behalf and providing the front face of any connection TOR may have, this includes an address. Although IP addresses of three types of nodes are publicly listed by the TOR project, exit nodes get the rough deal as many users doing illicit activities will use TOR and exit nodes are the end destination, thus, connecting to the service that is requested. An ‘exit node’ will be the last place before a network request reaches its destination and so therefore servers will identify the illicit activity being from the exit node address. Volunteers who run ‘exit nodes’ have far more chance in being arrested, as was the case for an individual William Weber in Austria [6]. These exit relays also get a fair amount of legal complaints thrown at them, to where their IP addresses are accused of various amounts of abuse. These volunteers are the life and blood of TOR, if they did not provide donations in resources the project would fall down completely. These are the people that pass vast amounts of information through the TOR network and have no idea what it is (hopefully). It could be encrypted state secrets shared by the military, a whistle-blower sharing vital exposing documents or terrorists outlining their next attack. These nodes are not maintained by criminals to my knowledge, but mostly people with a libertarian or anarchic political stances who strongly believe in freedoms of an individual, to which ‘state oppression’ as many would describe it should be minimised. Criminal gangs utilise TOR much like the US government, but unlike the US government do not seem too inclined to provide money to the operation. Many could say that these volunteers that own these precious resources and maintain them are being exploited by many who are technologically proficient to be aware of the power of the TOR project and are using it for the wrong purpose.

The aim for many anonymous technologies is to be somewhat decentralised, a single point could be an interesting attack vector for governments and organisations around the world who wish to keep anonymous networks quiet or inoperable. TOR currently has a sufficient amount of relays and

donations to uphold the vast amount of traffic that it currently processes, but it may not be enough if TOR traffic increases. The main issue with decentralised technologies is enforcing order, you are providing levels of trust towards volunteers or people who wish to donate resources to the projects cause who you do not know are trustworthy. There is the possibility that if a user requests a 'clearnet' site which doesn't use SSL/TLS (The padlock on your address bar "https" instead of "http") on TOR, the chosen 'exit relay' would be able to log down or view what request someone was doing, essentially allowing them to snoop on requests that aren't encrypted. This isn't a conspiracy of some sort, this can be confirmed in TORs own 'legal FAQ for relay operators'. It states the question "Should I snoop on the plaintext traffic that exits through my Tor relay?" to which a condensed version of the answer reads "No. You may be technically capable of modifying the Tor source code or installing additional software to monitor or log plaintext that exits your relay." [7]. Some may think this is theoretical, no relay would do such things, but it has been documented by a researcher named "Chloe". Chloe was able to identify TOR exit relays which were logging down traffic and attempting to login to a page. The researcher specifically setup a server which would show credentials in plaintext allowing bad exit relays to log down the correct credentials, if anyone tried to login it would allow Chloe to identify what she called "BADONIONS" [8]. Onions are commonly referred to TOR due to The Onion Router name. The TOR project tries to identify malicious relays that are manipulating traffic or are misconfigured which could endanger the user, but they are unable to deflect passive attacks, of which this is, to an end user. There is indeed research into passive attacks against users in the TOR network, but I have yet to see concrete research toward exit relays. This sort of attack is minimal in regards to a thoughtful, educated criminal in regards to TOR, as anyone who understands security would not request a 'plaintext' or unencrypted site on the TOR network. The reason for highlighting this attack is that I have discussed how I don't think criminal gangs donate resources to the TOR cause, but governments and hackers may want to donate resources to disrupt or utilise TOR in some way, it is not simply the case that donating relays are for the good of the network, sometimes it can be that relays are introduced for the worst reasons for the network.

The amount of exit relays that allow users to stay anonymous within the project is quite small, at the time of writing this there are 868 servers that have policies that accept being an 'exit relay'. There are only 7397 relays overall within the TOR network, my issue is not the question of resources, as many of these servers have a vast amount of resources, but rather how many individuals are actually donating resources. As stated earlier, anonymity networks require to be decentralised with no single point of failure, therefor the trust must be put to the generous donators of a project. The lack of vast numbers in volunteers, or rather donations in resources provides TOR with a weakness. Many network providers do not like to host TOR 'exit nodes' or even sometimes other types that TOR requires, this is mostly due to the barrage of abuse complaints that many TOR operators receive. The countries that are actually relays providing some access to users is fairly western based, with no real diversity when it comes down to server location (although this does not include 'bridges'). An ideal decentralised network would have servers in all countries around the world, but due to the improper advancement in some countries network infrastructure, lack of cheap network infrastructure overall in some countries, the TOR relay network is primarily based in Europe and the US. There also issues with laws around the world that are not in the west, with the internet being heavily restricted or surveyed in non-western countries. This lack of diversity can be confirmed by watching TORFlow, this interesting website allows you to see the flow of traffic on the TOR network and is developed by uncharted software [9]. The 'dark web' is not a strong robust system to which criminals thrive, but an isolated, at times anarchic, ever-changing system which cannot fully be predicted, although criminals do thrive in it. It just so happens

that many groups that utilise such a service are able to thrive within these conditions, mostly due to the hard work and dedication of volunteers and expertise of TOR employees. The project itself discloses it prefers server resource donations rather than donations to servers, the need for new relays provides far more security, dependent on the owner of the relays of course [10].

There has been much talk of different types of 'relays', to which one has been described already, an exit relay. Another type can simply be just a 'relay' where a relay operator has decided it does not wish to be an exit relay through its policies and simply wants to act as a middle relay, between the first and last relay. It is possible to be not only an exit relay but also a middle relay. A middle relay is the default responsibility that a relay must perform, a requirement if you wish to be a relay within the TOR network. You can choose not to be an exit relay but you are given the responsibility of being a 'guard relay' through being a stable relay which has been known for a while, once achieving the 'guard relay' responsibility the possibility of taking the 'middle relay' role decreases due to the possibility of attacks an active state could take. Essentially there are different responsibilities that can achieved by being a relay in the TOR network, primarily being a middle relay, to which you pass on the information given to another relay. I have categorised them as being types of relay but they do have the possibility of overlaying in certain circumstances, obviously not within the same circuit (or chain, as I've previously described it). A relay can only become an 'Entry Guard' relay after 8 days, minimum, a guard relay has the responsibility of interacting with the user. They are named the guard relay due to them protecting the user's identity when the user enters the TOR network. There is a level of trust that a guard relay has, it will see the IP that you are connecting from to TOR and therefore it can potentially know where you're located if you are not using a VPN. There is many who discuss how if you are worried about entry guards you should disable the use of them in your TOR configuration, this would be a poor idea as this would greatly diminish your chance of security in the anonymous network. If you simply rely on any relay to enter you into the TOR network every time a circuit is built then you have a higher chance in having a nefarious relay. TOR specifically gathers and gives the responsibility of being an 'entry guard' to a few in the total network who prove to be stable amongst other factors, while it is true that a guard relay can still be nefarious, only a few are selected for a TOR user allowing less possibilities of an organisation owning a guard relay, middle relay and exit relay in the same circuit. We have a middle relay which passes information on from a previous relay, essentially the middle man of the network (don't confuse this with a man-in-the-middle attack), we also have an exit relay which talks to outside anonymous networks for a user and we also have a guard relay which is used to hide the user's identity and is the first in the circuit. We also have a special type of relay which I have not previously discussed. All these relays just described have information which is available for public consumption, anyone can know what entry, middle and exit relays are on the TOR network. There are websites devoted to listing all ~7,000 relays, to which allows literally anyone to know if someone is connecting to TOR conventionally, be it governments, universities or other organisations that might find it interesting to know who connects to TOR. This is how many 'clearnet' services can decisively block traffic from the TOR network, as all the exit nodes are publicly listed for them to see. The reason why many block traffic from TOR is due to the amount of abuse that is given to a service, this also hurts legitimate users using the TOR network though. For highly authoritarian states, the use of TOR and other anonymous networks is sometimes forbidden due to fear of dissent. Many states which have a very authoritarian government block IP's that are in this public list to ensure users cannot connect to the network. This is where bridges come in, the last type of node I will describe that's within the TOR network. You can choose to be something completely different from a normal relay, you can be a bridge relay, these bridges are not publicly listed and have to be requested. These bridge relays allow individuals to

circumvent censorship as they are not publicly listed on the TOR network, you can request for them in multiple ways to ensure you can reach the TOR network. In a later chapter, we discuss these further and see how governments actively try and seek these specific relays. There is far more that I could cover on these relays and how they work within the network, but for now I think this an acceptable amount of knowledge that is required for this book. You can learn so much from the TOR projects blog posts on its relays and the unlimited amount of papers that cover the anonymous networking project. Relays are essentially the building blocks of the TOR network, without them there wouldn't be any 'directory authorities' as there would be no nodes. These different types of relays all have really important jobs in keeping peoples identities safe from adversaries of anonymous networks, paradoxically these relays can be from these exact adversaries at times.

CHAPTER 2

MEDIA

Everyday there is another news story on the ‘dark web’, due to the name utilising the word ‘dark’, it is not associated with many things positive. There are a multiplicity of sites that are horrific on the ‘dark web’ and on the ‘clearnet’, what is sadly unclear to people is how close these two actually are when it comes to content. A Livestream which provided viewers with content of rape [11] was on the ‘dark web’ according to many media outlets, how these vile individuals first shared this content though was not through the ‘dark web’, but through a ‘normal internet chatroom’ [12]. This point was less bold when writing up these articles. The fact this was first advertised on the ‘clearnet’ is a fairly normal practice, I’ve previously discussed how ‘dark web’ markets are advertised online due to the lack of good indexing sites online which people access regularly. Instead, these ‘dark web’ markets use ‘clearnet’ sites to promote their sites, allowing the onion domains to be easily discovered. When ‘onion’ site (hidden service) operators wish to share content or promote their site, they must initially provide this bridge where people are aware how to find such content. This was also one of the reasons the infamous ‘Silk Road’ marketplace alleged owner was captured, revealing trails of information through the ‘clearnet’ [13]. Everyone will have some other identity in the ‘clearnet’, when these two identities are found and can be correlated, TOR or anonymous networks can no longer help. Operational security is one of the most important factors for someone operating under the ‘dark web’, especially an individual running a hidden service which is under law enforcement surveillance. The issue with operational security is that it is very easy to get it wrong, we all have flaws, all have made mistakes and revealing our identity is much easier than many may think. Most hidden services on anonymous networks are not mature enough to completely rely within its own network to advertise and sufficiently withhold its economy (be it drugs or other illicit products), this is assuming of course, that someone is selling something illegal. Therefore there is this requirement to create a bridge between what people call the ‘dark web’ and the ‘clearnet’. The reason for providing content such as livestreams via the ‘dark web’ is that it can provide the server and the client far more anonymity compared to the internet by design, its purpose is to keep individuals within the network anonymous. Live streams require content to be interactive, a scripting language called JavaScript is likely to be used in livestreams. Interactive content has the risk of removing anonymity from an individual viewing the content, something not commonly discussed in the media.

The media pursues the idea that anonymous networks only promote ‘dark’ activities, there is very little coverage of legitimate business that goes on under the ‘dark web’ such as bitcoin services. Bitcoin services can be used by people who are, yes, criminals, but also crypto-currency enthusiasts and dark web enthusiasts. It is of course true that many undesirable things occur under anonymous networks,

and many surveys have detailed and confirmed this theory [16][17]. But these surveys also point out something interesting too, terrorism and child porn are not the highest at all by a long stretch. In fact, a large portion of the 'dark web' is blank or default pages. One interesting element on surveying hidden services on their subject matter is how much TOR traffic actually passes through to hidden services. In 2015, TOR asked volunteer relays to log anonymous data for analysis. What was found in 2015 was around 3% of TOR traffic passes to hidden services, or 'onion' sites [14]. That's right. 3%. The majority of requests are not hidden services, we can confirm this further by looking at TOR metrics [15]. This is not conclusive evidence that the anonymous project is largely innocent, as other protocols that are utilised by chatroom and file sharing software are not 'hidden services', the statistics simply inform us that only small percentages of users utilise the ability to view 'hidden services'. Nefarious behaviour is quite obviously high in anonymous networks by its nature, but the actual use of 'hidden services' shows a large disconnect in the medias understanding of anonymity networks. This misunderstanding from the media is evident in regards to the hacking community in general due the subject being mostly technical. Many journalists obviously do not have any previous knowledge in the subject, and so put trust in advisors or subject matter experts who may not be particularly clued up as many may think.

Because of this gap in knowledge, anonymous networks have slowly become the bogey man when it comes down to safety on the internet. It's a great seller for getting more money out of concerned business people, that you can't see the hacker. Public opinion is distorted due to this gap in knowledge, to which politicians follow suit in the aim to finally control the seemingly anarchic internet, in which cooperation is required from nearly every state in the world. Anonymous networks and the internet overall like many things, are not as black and white as people would like to think, the issue of trying to keep people safe overall from criminals, paedophiles, terrorists and extremism is not a one policy solution. It requires significant cooperation from at least the majority of countries around the world. The fear from many in regards to anonymous networks is that it is not regulated in any manner, which is true to some extent, as the networks are usually designed to withstand censorship. TOR is actually heavily reliant on a small number of nodes to keep everything afloat, if these particularly important nodes were to exit the network all at once (a possible cooperative law enforcement takedown) then the network would essentially be broken for hours, or possibly the foreseeable future. TOR puts a considerable amount of trust on servers called *'directory authorities'* to which aid people to reach the network. In 2014, it seemed to the project that these were under threat of some sort [21]. While the network is not regulated as in regards to the internet, where you can send abuse complaints to have something taken down, it is fragile enough in some regard for it to disappear. The idea that this secret network is impenetrable is a fallacy, the technology that is integrated into most anonymous networks make common surveillance tools relatively challenging, although surveillance is not impossible through at least the TOR network. The TOR network is a hardened version of the internet, requiring less trust on both sides of a connection, a client and a host. The issue remains though that the infrastructure that supports this network is relatively straight forward and does not require further technological advancements. Like much of the internet, these parts in infrastructure are in theory, possible to take down and shut down the TOR network. The issue is rather political than technological, where the issue of freedom of speech is called into question in not only one, but multiple countries.

The media rarely touches on the fact that these anonymous network projects, particularly TOR, are used to exchange secrets. This is what they were designed to do and not just for whistle-blower's, states use this technology to transfer securely information or to mask themselves. This is why the US government has put a considerable money in it previously. These networks, like many things that are

useful, are abused by criminals, but they are also very helpful to intelligence agencies and activists. Intelligence agencies wish to ensure that they are able to identify individuals who use the network for criminal use, but also wish to use it themselves, which produces a catch 22 for them. This is most likely why directory authorities have not been shut down, as of writing there are 9 directory authorities which are within Europe and America. These locations mean the TOR network is obviously possible to shut down, although it is likely to be very hard to do so due to local countries laws. The problem for law enforcement and many who look at anonymous networks is that it is simply not only a technical issue, but is also very politicised. The basic argument of privacy from the state, splits many, not only from fringe groups who believe in absolute freedoms, but liberals and progressives too. The subject is also very active on the internet overall, the question of how much regulation and intrusion should a state take to protect its citizens from adversaries. Anonymous networks and internet regulation is not the first subjects to be simplified by the media, but has made the debate very skewed, tolerance of freedom on the internet has slowly diminished. The idea that "*I don't have anything to hide*" has made people not follow the tightening of the internet overall, whether right or wrong.

The term 'Dark Web' has been simply attributed to networks that are anonymous, usually decentralised to which users are harder to track. This to me and many is quite strange, the feature of being theoretically untraceable is not particularly 'dark' but rather an innovation in developing possible future networks. The internet itself is gradually becoming militarised, which many have conceded [18], anonymous networks main aims are privacy. These anonymous network projects also have technologies which keep people safer on the internet, the constant reference to being 'dark', to me, is quite insulting to their efforts. The misunderstanding of anonymous networks by journalists makes it harder for many to see anonymous networks as an appealing prospect for the future of the internet, let alone to experiment or use it. Anonymity or the right to not be tracked doesn't always have negative connotations, it is not only criminals who should want to remain private or anonymous to some extent in their online life. The '*right to be forgotten'* initiative by the EU paved the way for this realisation that much of our content online is damaging to our own safety or security and needs to be regulated in some manner for the future of our children and ourselves. Identities online are being inscribed to a human face from the day people are now born, from parents sharing baby pictures on Instagram publicly, to schools becoming more active on social media. The activity that many do online can be attributed to a physical human due to the lack of understanding in operational security. Many security considerations are taken when choosing a password but very few talk about the issues of having just one username. Usernames are an important identifier in attributing a person to an identity [22], many choose relatively similar usernames if they have multiple. With the constant output of information in regards to someone's activities and identities throughout their lives, you create a timeline of events in someone's life. This can be evidently problematic in the safety of not only children but anyone on the internet; routines, places and relationships are logged. Anonymous networks are aimed to keep people anonymous, most hidden services do not reveal usernames, or censor parts of them. Anonymous networks are designed to make it hard to track both parties in the connection and many hidden services have a similar goal. Whether in the long run this is correct to do so, still remains a large question in today's society.

There are numerous examples of real tragedies that occur due to the lack of removal features on sites, especially in regards to social media. The right to be forgotten can be perceived as a right that can manipulate history for large corporate individuals to ensure they are only seen in a positive light, or a law that could facilitate victims of online abuse, like revenge porn. Revenge porn and shaming of

individuals is rife on the internet because of how lawless the internet can be, an argument is that anonymous networks can facilitate this further for individuals posting content. The question is what anonymous networks facilitate and how content is moderated on such networks to a safe degree, currently, these networks are unmoderated completely, which helps keep many secure, but can also hurt victims of abuse rather than the perpetrators.

There are some good things that come from anonymous networks that the media does not touch on, as I have discussed these networks can currently work well both for victims and perpetrators, but only one side of the coin is discussed, the criminal aspect. This criminal aspect, especially in regards to drugs is highlighted numerous times and is seen as dangerous. One of the most reported and high profile cases of drugs on anonymous networks, namely, TOR, is 'Silk Road'. The first marketplace really to facilitate the sale of drugs on scale for a long portion of time, online, adding the security of being 'anonymous'. The market since then has grown considerably and is becoming increasingly competitive [19], the 'dark markets' have removed the street aspect to many who wish to buy drugs. Buying drugs from the streets can be dangerous in many ways; producing relationships with gangs, not understanding the quality of the drugs and unreliable consistency. Online 'dark markets' have made sellers online provide good customer service, good quality drugs which are reliable. These features are becoming more and more ingrained in 'dark market' communities as vendors fight for customers. This can only be good for the safety of many individuals who choose to take drugs, which many see as inevitable, the experience of taking drugs has become much cleaner due to such markets cropping up online it is argued. Although, I have seen no research papers giving any evidence of this. Because of the high security that 'dark markets' enforce online, the identities of individuals around the world are safe from intimidation and the exchange of money is much easier due to middle-men, this can also include the delivery of the drugs as well. With no knowledge of each other's real identity, the trust in such systems increases, which is shown in The Economists article. Many have realised that these anonymous networks provide a safe alternative to the purchase of drugs, including students from the UK [20] who have decided to choose these 'dark markets' as their main supplier. The technical challenge of accessing such content has been eroding for a while, even purchasing bitcoins is becoming relatively simple. Students are obviously a target market for many drug suppliers, what many, including the article from the Independent concludes, is that markets on the 'dark web' can make it safer for people to experiment with drugs. Whether you agree with taking drugs or not, it is surely a good thing that individuals can shop around for what seems like the best quality, reliability and choice for the sake of the individuals' health. When purchasing drugs in real life, you must acquire trustworthy contacts and remain known to these individuals, you may not consistently get quality drugs, something you cannot review like on an online platform, where reviews are important to vendors.

Reddit has increasingly become a source for some journalists in understanding the internet or anonymous networks, this is highlighted with a Metro article published online in 2015 [23] to which the author sources a Reddit thread entitled "What's your deep web story". The article produced by the journalist does not challenge the possibly of these stories being untrue, in fact, much of the language used portrays it as fact. In the article, the journalist writes "but what actually happens when you go 'off piste' into the parts of the internet". The blind acceptance that mysterious users from Reddit are providing truthful stories is dangerous and damaging, it further erodes the idea that anonymous networks can be *potentially* innocent. But this idea of there being 'red rooms', dangerous parts to the 'dark web', are already well within the majority of people who actively use the internet. The media is misrepresenting many parts of anonymous networks and blindly following sources which cannot be

trusted. There are a huge amount of articles dedicated to highlighting listings from ‘dark web’ stores, most likely from the popular marketplace “AlphaBay”. These listings cannot always be trusted, even when a user on the site has a very high score. I’ve crawled various marketplaces which are deemed to be on the ‘dark web’ and many have substandard or poor product listings, especially in regards to fraud and malware (commonly people misuse the term virus). From simply visiting one of the more popular marketplaces you can see the quality of many of the items on sale are files which are being reused and have been commonly distributed most likely through the ‘clearnet’ as well. Fraud guides with titles all in caps advertising vast riches screams fake or poorly made. As someone who regularly analyses malware it was interesting to see a listing of a very old malicious tool named ‘Blackshades’ which is widely available on the internet. The user was attempting to sell this admittedly for a very low price, but was relying on the purchasers of his item to have no real idea about the marketplace in regards to malicious software. Blackshades operators had been taken down and the actual software is mostly inoperable, it is heavily detected by anti-viruses and is very outdated compared to other malicious software that has subsequently been leaked. Users still persist in giving this user a positive review, most likely because they think they possess something of worth that is dangerous, when in reality they have been scammed somewhat. This charade is quite common on the ‘dark web’ and in the media, where an item or hidden service is sensationalised, for little or no reason except that it is simply on the ‘dark web’. The forbidden place where one must not go, an idea that skews many perceptions of anonymous networks. This type of blind trust towards a seller is also evident with the media, which accept that either listings are vetted or are just simply true, when in fact, marketplaces on the ‘dark web’ can be manipulated very easily, and fraud is rife, even with a review system in a place. With this blind trust, every few months a media outlet pushes a story on how terrible listings are on the ‘dark web’, when some of these listings may be fake or not that special. Credit card fraud, phishing, malware, and online identities are all sold via the internet as well as the ‘dark web’.

As I’ve discussed earlier, sometimes blindly trusting a source is best for the media to be able to sell a story, especially as traditional media is fading and new online media sources are popping up with energetic, alternative reporting. In an article from The Daily Mail [24], they discuss the findings they have found on the ‘dark web’, most likely from browsing to a popular site which indexes onion sites. Nowhere in the article do they discuss the legitimacy of such sites like many would on the ‘clearnet’ and quote users who pose as Hitmen. This lack of real investigation makes the dark web seem like a chaotic dangerous place, when in reality it’s full of people who want to buy and sell drugs and get high. There are no actual verifiable reports to my knowledge of hitmen being bought on the ‘dark web’, which have subsequently killed an individual. The way the ‘dark web’ is treated in the media is something similar to how the media treats spies or hackers, with this fake pretence that everyone goes a long with, even though many know this is indeed a fake representation of the subject matter. Why do this? To sex up the story is the only thing I can think of, technology can be quite a boring subject if one is not interested in it. To write that a hitmen is available on the ‘dark web’ will at least drive views from some individuals. Many media articles want the user to feel like they are inside the dark web and that the article author has put a lot of effort into investigation, the reality is much different. Most articles describing listings are poorly researched, while there exceptions to this, the large majority simply visit a ‘dark web’ indexing site and register to these marketplaces. Most ‘dark web’ marketplaces are not closed communities and allow anyone to register as long as they are accessing it through TOR, there may be select communities which are closed communities, but these are not what the media is highlighting. The specific marketplaces that the media usually trawl through allow anyone to go on, the invite only marketplaces usually rarely appear or not at all.

As these hidden services which commonly service the drug trade are open to anyone, they can also be open to manipulation. Law enforcement or well-resourced actors could potentially register an endless amount of accounts to which they would purchase items from an account controlled from them too. Users who have purchased an item can leave reviews from the seller, giving a user much like on eBay, a positive, negative or neutral score. This bumping up of a user's score allows for someone to achieve a reputation by simply owning other accounts. I am over simplifying this for an example, but it is possible to make users on such marketplaces seem far more reputable than maybe they are. This can lead to scammers and law enforcement stings. The services that are provided, especially for drugs users are not impenetrable in regards to purchasing. These marketplaces are much like any other marketplace available online, ripe to abuse if someone has enough energy and time. To me, these gaping vulnerabilities in such a marketplace mean you cannot report correctly whether these items are real or not without purchasing them, this itself provides a risk of being incarcerated. With this endless campaign of showing usually unverifiable products leads to misleading or misinformed articles that produce views to users that are not accurate to what currently is on the dark web. Politicians and journalists are unable to understand or get to grips with the mechanics of anonymous networks and refer to anonymous networks as 'dark', what is clear is that not all content from the 'dark web' is criminal or morally wrong. Anonymous networks have many applications that are useful to everyday users, one emerging attribute that is becoming commonly important is the requirement for sufficient privacy. As a society we have progressively become more comfortable in publishing moments of our life, even if some parties cannot consent (such as a very young child) to the public. Experiments and advancements in technologies within anonymous networks can potentially provide answers for helping in giving more privacy to people online, giving people truly *the right to be forgotten*. What's evident by many reports online is that people think these anonymous 'dark' networks are impenetrable, impossible to taking down. This is simply not the case, in fact, most anonymous networks are fragile in some manner. A level of trust must be put upon some element in connecting users together, whether it be peer to peer based or a more centralised design. Specifically, the TOR network has trusted 'directory authorities', without these special servers the network would not be able to function correctly. What is worrying for the TOR network is that these special servers are located exclusively in the US and Europe, the most important aspects of this anonymous network are not diverse in server location at all.

CHAPTER 3

DARKNESS LIES EVERYWHERE

In 2013, the UK Prime Minister David Cameron ordered intelligence agencies to break up the ‘dark web’ [25]. The main aim was to get rid of child abuse online, but this aim, is as many will probably have guessed is not as easy as David Cameron giving orders. There is a presumption that online content on the ‘dark web’ is considerably worse because of the amount of freedom given to operators who run hidden services. While it is of course correct, as I’ve previously outlined, that the ‘dark web’ has some awful content, so does the internet. In fact, technically the ‘dark web’ is connected to the internet, but you need to access this content in a specific way, dependent on the anonymous network. The internet itself is rife of abuse, be it credit card fraud, human trafficking, paedophilic content or extremist content. It is not radical in my opinion for me to state that anonymous networks are sometimes used as a scapegoat for the ills of the internet, to me this mostly stems from the frustration many have that abuse sometimes is hard to remove in a stateless network system (the internet). Large amounts of cooperation from various organisations in different countries must work together to reduce the amount of *classic* abuse on the internet, such as malware, child pornography and credit card fraud. It is of course inevitable that different states have varying amounts of tolerance toward different subjects and many states may be less stable than others in regards to corruption.

This is not to dispute that there is some horrific content on the ‘dark web’. These networks have a fair share of content which is much harder to be taken down traditionally, like the content from the internet can. It is frustrating that the mechanics of the TOR network mean it is near impossible to take down, but not all attacks (if someone is willing to attack) are preventable when running a hidden service. The idea that the ‘dark web’ is being used as a scapegoat is quite a strong statement to make, but large quantities of abusive content can be found online simply due to the amount resources that the internet offers, such as free web hosting. The amount of unique .onion addresses daily is averaging around 60,000 [26], do note that some services have multiple unique onion addresses. If we take in contrast just how many .com domains are registered in a single day in 2015 (222k) [27], the ‘dark web’ is a small but growing network that is currently dwarfed by the internet. The ‘dark web’ is of course a more concentrated network which largely facilitates criminality in conjunction with hidden services, as I stated earlier, but the sheer size of the internet overall means abuse is obviously much higher. The argument

would be that it is much easier to take down abusive content on the internet than on the ‘dark web’, which is true. The issue is, as many have discovered with internet piracy, is it is much like the game whack-a-mole. The amount of freely available resources on the internet is high, open to be abused by people like paedophiles wishing to distribute content. The amount of freely available resources on the ‘dark web’ are scarce, in which resources like image uploading sites which are freely available are usually sporadic in uptime, and may disappear within a few days. The reliability to provide openly available resources like image uploading on the internet makes a far more fruitful option than choosing a questionable unknown image service on the ‘dark web’. Servers which adhere to web requests for content cost money, requires technical expertise of some sort and hours of work. It also requires a person to have knowledge (dependent on what you’re doing) of “bulletproof” web hosting providers, or have sufficient confidence that your payment details won’t lead back to you. Some groups such as extremists or paedophiles have very few people who are able to do these activities well and so are far more restricted than many may think, some are not very technological at all [28]. This is not to say that these groups are completely unable to perform such activities, Eric Eoin Marques, the owner of Freedom Hosting allowed child pornography on the Freedom Hosting service [29]. Freedom Hosting was the most notorious in providing hosting for child pornography through TOR and was fairly successful at this operation until attacked with a trivial well known flaw in web applications. To be hacked by such a well-known attack can highlight that even experienced network administrators who facilitate the distribution of child pornography through TOR still have a lack of knowledge in some technical areas, such as web application security. The main point to be taken from this is that most abusers of the internet and ‘dark web’ would see it far more beneficial to abuse an open service on the internet than spend large amounts of time and money to setup a service of their own. While this is not always the case, the main indication to me is it is far easier to abuse open services on the internet.

The internet has its fair share of abuse just like anonymous networks, apart from these abuses are masqueraded by the huge quantities of activity that isn’t abuse. The Internet Watch Foundation found 57,000+ URL’s on the internet which had child pornography in it in 2016, most worryingly is that this content was not found on broken states networks, but rather hosted predominantly in Europe [30]. Interestingly, the foundation provided numbers for ‘hidden services’ as well (hidden services on anonymous networks), in which they were able to identify 41 in 2016, previously in 2015 it was 79. It is unfair to comment that there is far fewer hidden services than URL’s that contain child pornography, as it is much harder to be taken down and therefore is far more dangerous in regards to damage to overall society. It is fair to comment that the internet and the ‘dark web’ are not polar opposites and in fact, have far more in common than people may have thought, especially in regards to content. Another highlight from IWF’s 2016 report is that they discuss how much of the ‘dark web’ hidden services link to internet image hosts to host content, “Hidden services commonly contain hundreds or even thousands of links to child sexual abuse imagery that’s hosted on image hosts and cyberlockers on the open web” [30]. This partly agrees with my theory that there is far more resources openly available on the web to abuse without the cost of hosting or the technical expertise that many in these groups do not have. It is also rather savvy in some regard to exploit a currently running service, as it becomes much harder to track or find the original author of such content, be it an image or text.

Identities and details are reportedly sold and passed across the ‘dark web’ all the time and this is also true on the internet as well. Pastebin, which has been around since 2002 allows users to anonymously post text content to the site, this can range from code to links to various other content. The service is primarily used as a place to dump account details and show announcements from hackers, it has also

been host to personal details such as social security numbers and credit card information (Note, Pastebin is compliant in removing such content). There have been numerous cases which have identified Pastebin as an entry point to downloading private information or revealing information [31], including the hacking of the now French president, Emmanuel Macron [32]. There are offshoots of this service available on the 'dark web' but none have really lifted off due to poor uptime or reliability, this is the same on the internet, there are many alternatives to Pastebin but it is by far still the most popular. Much of the content that is posted to Pastebin want people to take notice, this is something that the 'dark web' was not designed for. Most posts that are intriguing are people advertising credit card fraud services, account dumps and piracy. Pastebin provides a platform that is heavily monitored not just by journalists but also threat intelligence companies. This platform among other alternatives ultimately is exploited heavily to advertise services and reveal personal information about people that most people would associate with the 'dark web'. Pastebin has higher traffic than most UK supermarkets according to Alexa, with the global ranking impressively set for Pastebin at around 1,021. Like many openly available resources on the internet, they are abused by many for various activities that I have previously listed. Pastebin has done well to remove much of the abusive content on its site, but again the situation is quite like whack-a-mole, where regulation of such content is hard to do. Arguably you could say Pastebin is the frontline of hacks where details are shared almost instantaneously, most likely pasting a sample to prove authenticity and wanting to sell the rest of the details to the highest bidder. Although there are platforms on the 'dark web' for such a thing, you gain a wider audience by utilising not only Pastebin but other sites such as forums that are available mostly on the internet. Bank details specifically are not as active as people would assume on the 'dark web' than on the internet. The Telegraph reported in 2016 of a particular site which was selling 100,000 UK bank details [33], becoming one of the largest available credit card fraud sites openly accessible to anyone who has an internet connection. The website which reportedly held such a large amount of UK bank details was openly available from a normal browser with no restrictions on registration to the service. In my personal experience I see a rise in these type of services and see mirrors of services available on the 'dark web' with very few credit card fraud shops solely relying on the 'dark web'. A lot of fraud is directed in criminal forums where many exchange information and rely on invitation only entry, this allows members to feel safe from law enforcement and newbies. These forums are not inside the 'dark web' but available to view on the internet, where they use exotic top level domains in the hopes of evading abuse complaints.

Information is exchanged by criminals on some best practices to take when administering infrastructure. One vital part of an online criminal's enterprise is registering domains for whatever reason they need it for, in this example I will be referring to credit card fraud shops. These credit card fraud shops allow you to buy bank details of innocent citizens captured in various ways and are sold at very low prices *(*$5/45, although I see some for much lower) [34]. In 2010-13 there was a surge of exploiting the .su domain, which was the reserved top level domain for the Soviet Union, an official blamed the reason for being unable to remove abusive content in a timely manner down to "weak Russian Legislation" [35]. The .su domain is not in the 'dark web', and can be accessed simply through a web browser much like entering a domain which uses the .com extension. From 2013 a new trend began to emerge that criminals were easily able to exploit, the mass of new generic top level domains. Everything from .xyz, .dance, .fun, .webcam, .top, .click and more were being introduced and allowed to be registered. With such a huge influx of new domains available it was only time before they were tested to see which were most susceptible to abuse [36].

Criminals do not simply lurk in the areas in which people call the ‘dark web’, there are plenty of places on the internet where criminals can thrive easily with little to no intervention from law enforcement. Criminals can and do actively exploit parts of the internet for their advantage, for example, the domain name system which has become bloated and susceptible to large amounts of abuse. One interesting group that has facilitated abuse greatly on the internet is a group labelled the ‘Russian Business Network’ [37], this network had been able to utilise ‘bulletproof’ web hosting services (taken down in 2007). As many may have guessed ‘bulletproof’ web hosting services ensure that if abuse complaints are made, content will remain online and no action will be taken on the individual. Many use ‘bulletproof’ web hosting to host servers for malware, host credit card fraud shops and pharma content. This criminal network had a diverse portfolio of abusive material on the internet, at one time in an analysis by a researcher, 406 different servers were used with 2,090 domains to push such content [39]. A lot of the network infrastructure used by this group was not exploited at all, ISP’s would be fully aware of what they were hosting for such a group. The owners of this infrastructure are according to WHOIS located within Russia and Panama, this could be fake, so should be taken with a pinch of salt. The Russian Business Network is presumed to have most members located in Russia, where crime of this nature isn’t investigated as harshly as some westernised countries. In 2017, there are many groups who not only know ISP’s that can be used for abuse, but ISP’s that can be exploited easily. This diverse network of individuals utilised the internet to profit by exploiting people in various different ways, they were aware of how the internals of the internet worked and were able to be quite successful for a while. Threats like this group appear on the internet often, maybe not to a similar scale as ‘The Russian Business Network’, but reveal that it might not be the ‘dark web’ that is the largest threat to people on the internet. While many associate the ‘dark web’ as a safe haven on the internet for criminals, there are temporary safe havens across the internet and not only in eastern Asia.

These safe havens are connected to the internet, they are able to have these safe havens mostly due to the ingenuity from the criminals. There are many exotic ways of evading IP’s getting blacklisted, but commonly it involves rotating a pool of IP’s. It can be also the actual internet service provider that allows such content on their network, in which criminals do not have to exploit the internet service provider (ISP) at all, rather the ISP complies with such requests from a criminal. There have been many different types of ISP that look away from abusive content which can range from DDoS attacks to other nefarious content. It is not only in countries commonly associate with bulletproof services (Russia or China etc.). In 2009, the FTC in the US shutdown a provider called ‘3FN’, which in FTC’s press release reportedly hosted not only malware and phishing sites, but child pornography as well [38]. The idea that only the ‘dark web’ has awful content is obviously quite untrue, the amount of abuse on the internet is high. This is because of how the internet is designed. These providers who have tolerance for such abuse take a huge risk in accepting such content but do it for profit, there are many groups on the internet that need infrastructure to be able to exploit people in many ways and will pay a high price to have network infrastructure that isn’t blacklisted and can withstand abuse reports. The problem is having to accept that other countries have different laws. The internet has connected countries all around the world to where nearly anyone can speak to who they wish (dependent on how tolerant your country is of free speech). Countries which believe in privacy and liberty will naturally have a disjointed relationship with more militant partners in the world, many countries do not wish to be appearing to be censoring their citizens. There are other countries which are connected to the internet which have dictators, their citizens having their activities followed on the internet like hawks. These stark differences mean cooperation can sometimes be difficult, especially when it comes down to abuse that other countries may not constitute as abuse. In the TOR network and many anonymous networks,

reporting abuse is not possible, which is why many see anonymous networks as problematic. Content that is on TOR can withstand these abuse reports because the location of such content is hidden, you must go through relays to communicate with a host on TOR. 'Bulletproof' hosts and anonymous networks have similar qualities to them. Anonymous networks like TOR mean abuse reports are not possible, allowing content to remain as long as the host is up, relying on the host of the content to be responsible for what is allowed. 'Bulletproof' hosts use a variety of tactics to keep content online on the internet, they may ignore abuse reports or simply change the network infrastructure to evade abuse reports. One of them is regarded as dangerous and another is not mentioned often within the media, both are as equally as dangerous as the other and should be treated so.

The abuse or exploitation of the internet does not require a lot of knowledge or planning, this was evident when Microsoft's Xbox Live service and Sony's PlayStation network was taken down by a group who named themselves the Lizard Squad [40]. The group exploited the fact that most home routers had poor security configurations, usually using default passwords to login to administration accounts [41]. It is also something to note that they used an internet service provider in Bosnia and did not utilise the 'dark web' to advertise their services at the start of their rise to fame. The group was famous after the 25th of December for launching large scale DDoS attacks, an attack that essentially drains the resources of a host. This resource can be bandwidth, memory and even hard disk space on a server. This type of attack means that innocent users of a service are unable to view the service because it is preoccupied trying to fulfil requests from an attacker. This type of attack is not very complex in being setup and can be relatively hard to thwart, dependent on the experience of the attacker. Most of these hackers did not come from the 'dark web', they came from forums that could be accessed from the internet relatively easily. It is however correct, as stated in a Daily Mail article, that the hackers communicated 'using the dark web' [42], but not as some may think. Many criminals, hackers and terrorists will utilise TOR to mask their true IP, much like a proxy or a VPN. This interestingly, does not mean they don't use services to communicate that are available on the internet in coalition with TOR. There is much evidence that members of Lizard Squad used services like Skype, Tinychat and XMPP. One interesting piece of evidence is a YouTube video of a conversation taking place with a "Poodlecorp" member and Vinnie Omari, an alleged member of Lizard Squad [43]. A childish affair which fully displays the maturity of many members of these supposedly feared groups shows active use of communication through the 'clearnet'. The hacking group 'Lizardsquad' also created a service essentially providing DDoS for hire, allowing anyone to subscribe to their services and attack a target. This service was later hacked, and the database leaked [44] and distributed across many forums. I was analysing Lizard Squad at the time and got my hands on the database that was leaked, the administrators that were in the database had their IP's logged, many of these IP's were TOR exit nodes. This confirmed my suspicion that they utilised TOR to mask their identity, but didn't use TOR completely to specifically talk over the 'dark web'.

The overlapping of these two shows the blurred lines sometimes between anonymous networks and 'clearnet'. Anonymous networks usually aren't restricted in what they can access, the majority of outbound traffic is to what many call 'clearnet', although I'm not the biggest fan of the term. Anonymous networks and the internet overall interact often, many see anonymous networks as closed off and hard to reach, but are in fact very open armed in regards to communicating with the internet. The main aim as I've previously discussed is to ensure the privacy of the client, the user who wishes to communicate with a service. The problem that these hacking groups that took down Xbox, Microsoft and many others have is the fact that they have very large egos. Two members actually went on Sky news to discuss

the attacks in which they showed their faces on TV [45]. The pomposity of these members shows that individuals who exploit the internet are not always anonymous dark figures in a corner, they can be loud arrogant kids who understand some flaws in today's networks.

This group not only used hacked home routers, but also used Googles infrastructure, exploiting the use of coupons and the ability to use hacked credit cards. The cloud is a buzzword in businesses now, where everyone must use the cloud to provide 'scalability' and 'flexibility'. Because of these attributes of the cloud, groups like Lizard Squad, but not limited to, have utilised cloud technology to attack other infrastructure [46]. The group attempted to attack what had been masking them, the TOR network itself, but clearly misunderstood the technicalities of the anonymous network and the consensus system it had in place [47]. The group attempted to fill the TOR network with a bunch of new relays within the network [48], in the hope to make a statement of how someone could potentially deanonymise someone on the TOR network by controlling large amounts of relays. This was a classic case of trying to undermine a peer-to-peer system through what many call a 'Sybil Attack' [49]. The first problem that the attack had was it were blatantly obvious what they were trying to do, adding over 3,000 relays in one day to the TOR network. The second issue that the group probably didn't account for was that relays are not instantly trusted when entering the network, they go through phases to which they become trusted [50]. The third and final issue is that these relays were created from fraud and would not last very long, the second issue required that these relays must be within the network for 6 days to at least begin to make some difference in the network. Google would have been able to recognise the credit card fraud and would have shut these servers down, but before they could, it was made plainly obvious that relays were meant for harm and were removed from the network. Accounting for less than 1% of the network if they had stood, would have most likely not have made a huge dent in the anonymity of the users of the TOR network, if any at all. The arrogance of Lizard Squad was shown in this attack to be an undesirable characteristic. Sharply introducing so many nodes to which most were blatantly named with "Lizard" in them was a bad move, the attack could have proven somewhat useful if it wasn't for the groups volatile nature. Although the attack was very small and would have never properly altered the network, it could have been a poignant reminder of how anonymous networks could be fragile in some circumstances.

Not only is the 'dark web' full of criminals, paedophiles and terrorists but so is the open web, 'clearnet', 'surface web' or internet (so many terms I give up). The amount of abuse on the 'dark web' is high for how small the network is compared to the internet, but large problems are still apparent on the internet with groups like the Russian Business Network and 3FN openly facilitating the host of child pornography and more. The internet has so much abuse, young teenagers have been able to exploit it sufficiently to cause outages in major corporations. The interesting point is when the Lizard Squad group attempted to attack the TOR network with the flood of relays that it decided to add to the network. The TOR network had a system in place which should be noted for future security considerations for the internet, a reputational based system didn't help on this attack because they were already identified, but ensured deanonymising users would not be possible for this group. This case shows why I think much of what anonymous networks develop is interesting for the future of the internet, it is where innovation and new ideas grow and experiments like this could help millions in the future. While anonymous networks have worrying default stances on content removal, the internet also has areas where content is difficult to remove. The judgement that the 'dark web' is a safe space for many we want to catch, can be completely correct for some of the areas we have discussed on the internet.

CHAPTER 4

PRIVATE COMMUNITIES

Private communities are areas of our online world that can be quite worrying, but can be also quite liberating. Most people want to make sure that everyone has a voice on the internet, they are able to freely demonstrate freedom of speech without having fear on their subject matter. The issue with freedom of speech arises with extremism and criminals who wish to divide and exploit individuals, they aim to rip up the fabric of society for ideological or financial reasons. Private communities can range quite significantly in size, subject matter and the ability to stay private. One thing that the 'dark web' and anonymous networks can facilitate, are private communities and do it well. This became evident when the operator of the largest child pornography site called 'Playpen' was arrested, the site had more than 150,000 users registered to the 'dark web' hidden service [51]. The operator was well equipped for running such a site on the 'dark web', he had knowledge, time and the energy to do so, which as I've stated earlier is much rarer than many may think. It is true that 150,000 users were registered, but these were users who simply had to download a browser to access the resource, instead of the hard parts, essentially maintaining the site. This one operator, called Chase "chose the name of the website; selected and made payments to the website hosting company; regularly updated the website with new features and security fixes" [52] amongst many other things. His competencies of technology will be worrying to many, there is no doubt that this particular community would have been attacked by hackers and maybe even governments. Keeping the site afloat with such a mass of users is a particular skill that comes from experience in server management, which takes years of understanding of an operating system and general networking.

Playpen was taken down by the FBI, this was due to the administrator known as "Chase" in documents revealing the IP of the server [51]. TOR allows a server and client to be anonymous, neither will know the location of each other in theory, revealing the IP address meant an investigation could successfully take place. While the details of how the IP address was disclosed are hazy, it lead to a successful investigation full of arrests and rescue missions. The server was located in the US which allowed law enforcement to take copies of the website and start investigations into individuals. The sheer number brings to question how active paedophilia is on the internet and the 'dark web', the ability to hide away from any law enforcement is unfortunate and an obvious worry to many. This is what most people would associate with the 'dark web', the lack of ability to remove this content meant that it was able to

flourish and grow as a community. The amount of registrants may be distorted by researchers, law enforcements and attackers attempting to slow the system in some way, but cutting the numbers by a quarter (which is very generous) still shows a huge community which share content online which is unthinkable. These type of private communities are part of the crux of the issue for anonymous networks, while the idea of a completely free private network for all to express their views without a chance of censorship is great, in practice it can bring content that most find abhorrent. This is not untrue of the internet, private communities are available for many who wish to find them where content is also equally horrific. Much like the comparison between anonymous networks tolerance for all content and the ability of 'bulletproof' hosts to provide a safe haven on the internet previously mentioned, there are private communities inside social media (on the open web) which share content which many would find unsettling alike to content from Playpen. According to a BBC report in 2017, Facebook "failed to remove sexualised images of children" [53]. Most troubling is the statistic from the article that only 18 images were removed from 100 images. The hard line for freedom of speech from social media means that many of these groups can remain active and are simply having some of the content removed. This is far more dangerous than the 'dark web' in some respects, accessing the 'dark web' still requires some knowledge, especially knowledge of which hidden service to access for illegal content. Facebook is readily available to anyone which could certainly exceed the user base that the 'Playpen' attracted. Facebook has 1.23 billion use its service every single day [54]. Facebook and other social media services are far larger networks than any anonymous network currently are and have the capability of having small pockets of closed off groups which are hard to govern. Facebook is one of the largest social networks where user generated content is shared behind closed doors, most users of Facebook have set their privacy settings away from global posting, although accepting friend requests is another matter [55]. There are different ways people approach privacy [56], but it is obvious that it is far more complicated to follow, track and measure Facebook users than on far more open platforms such as Twitter and Instagram. Due to the design of Facebook you have closed groups not in the conventional 'groups' feature that Facebook has, but also groups as friendship circles, closed off social networks within Facebook that can defined by many features, one being a group chat which can involve not only friends but others too. These areas, rightly so, are not public and are hidden away from view from anyone else aside from the participants. The only real regulation of what is said in these conversations and these groups is Facebook, media can be shared within seconds and hosted on Facebook servers within a few clicks. The problem with hosting so many users within a network is how information is circulated, the sheer number of activities happening at one time mean algorithms and automated controls must be designed to regulate users in some way. These algorithms are not humans, they will get things wrong and misidentify users [57]. Facebook employed artificial intelligence to be able to correctly identify nude content that may appear in images or live streams, but artificial intelligence has had issues itself due to the design of how artificial intelligence works, it must learn from the 'sets' (a collection of samples) its given. If we have a huge amount of images submitted to Facebook every second, artificial intelligence must first learn how to identify potentially naked material with what many call a 'training set'. This 'training set' allows the computer to learn what to look for, what are the key indicators that a human operator is trying to teach the computer to do. A problem now occurs after this, if you let the computer learn from the content that is generated from the users, it can lead to problematic results, as not all users want to play the game [58]. Flooding content that is right wing led to the A.I "Tay" from Microsoft, to be openly racist on Twitter. This showed how leaving A.I to learn from users is ripe for abuse and defeats any meaningful use of A.I, as it's not governed by who designed the artificial intelligence initially, but who interacts with it the most and is able to manipulate

its learning ability correctly. Tech researchers in early 2017 discussed how easily A.I could be abused, calling it “a fascists dream” [59]. Many technology companies are looking to employ artificial intelligence in a variety of ways, the one important aspect is how it learns. Learning from users who produce user generated content has obvious issues that produce an issue for social media sites, how can you keep freedom of speech for the right people and remove content that is obviously abusive in such high numbers? If you don’t let the A.I learn from user generated content, you don’t have a system that can learn fast enough, it will become a trailing enforcer online that has little or no user to it. Artificial intelligence is still within its infancy and removing content using such a subject is questionable, the problem is that the system will still misidentify images, it will still have to have a human analyst review content to correctly review it. Learning from human analysis is still requiring manual work, which will be slow compared to how many submissions a system probably receives. While this system of following a human analyst will be the best outcome out of possibilities to how the A.I learns, it still means it won’t be perfect.

Social media is borderless, they receive a barrage of requests from various countries with very different ideas on freedom of speech and content overall. What’s worrying is the fact that social media tools that report content are being abused by governments, government affiliated organisations or supporters of oppressive regimes to silence individual ‘dissidents’ [61][62]. These individuals have a right to freedom of speech on social media, by policy, but most social media outlets have an extensive terms of service which many groups can abuse to silence people. In Syria, where tragedies are daily occurrence, social media has become a hub for information to many interested parties, especially humanitarian. The Syrian Electronic Army are a group who support Bashar al-Assad, they understand how to remove people of opposite view on social networks [60]. Unlike on anonymous networks, content can be brought down easily from the internet, whether is perceived by most as correct or not, it can be removed mostly because of an understanding in policy. Anonymous networks do allow for content such as child pornography to flourish, although as discussed, has a small number of individuals who could be capable of doing such a thing. These networks also allow for content whatever it is, to remain, this can be against an oppressive regime to which activists can remain safe, anonymous networks also allow someone’s identity to not be revealed unless they do so (in theory, there are exceptions). These are why anonymous networks are seen by some as a positive step in allowing anyone to express what they feel, without fear of it being removed.

Social media networks are dangerous in their own right, they are where paedophiles can actually groom children to meet and manipulate them. In the ‘dark web’ distribution of content is obvious, but the actual grooming of children is done on the internet. Social networks are becoming an obvious target for grooming, with an alarming rise of 50% in online grooming cases [63]. Grooming on social media does not simply target children, but vulnerable individuals who are targeted for radicalisation. Nicky Morgan in early 2016 discussed how ‘Islamist extremist were using the same grooming tactics as paedophiles’ [64] in which methods are primarily targeting children on social media. When we discuss the ‘dark web’, active exploitation is seen as red rooms or something much darker. Social media networks do have individuals actively seeking to exploit children and vulnerable people, a percentage of users will use this network to be able to abuse individuals and the service itself. There is an obvious comparison here from anonymous networks, that a percentage of users of a service begin to exploit a network because of how many people there are. Many would state the big difference being that banning or removing content is far easier on social networks, but as we see from the BBC’s report on secret groups, it may not be as easy as many may perceive [53]. In 2012, there were 1,145 reports

incidents related to online grooming in UK according to CEOP (Child Exploitation and Online Protection) [65]. These numbers show a high amount of reports in online grooming, there may be many more unreported to the police. The number of reported incidents is from 2012 and has probably risen since social media has become far more popular compared to other services like chatrooms and community boards. The sheer amount of content that is being posted on social networks means there must be abuse, the modern features that many have been implemented in many of these networks such as the “live” feature, means content is much harder to regulate [66]. Although Facebook, YouTube and Twitter have technologies that they hope identify illegal content, as we see from artificial intelligence technology this can be easily manipulated or evaded in some manner. The content that is available on these networks or on the internet may be available in a more temporary manner than on the ‘dark web’, but there are higher numbers of users with abusive content or abusive intent. It is much easier for a criminal to exploit online than on the ‘dark web’, it is much easier for a terrorist to spread propaganda online than on the ‘dark web’ and it is far easier for a paedophile to groom a child online than on the ‘dark web’. These actions are where communities of these groups are made, spreading propaganda gives terrorists links to sympathisers to which they can lead to the dark web or closed off groups. Criminals can exploit members of the public and sell their details on the ‘dark web’ in a safe manner and paedophiles can groom and collect content for later distribution on the ‘dark web’. The ‘dark web’ is indeed not closed off, as many of you probably now realise, the connection between many anonymous networks and the internet are strong.

A video of murder being published is reserved for the ‘dark web’, but there is content like this that is on social networks too [67]. As previously mentioned, this type of content is hard to regulate, the main defence over this type of content is the users within the network, using the report button. The issue with this feature is it being heavily miss-used, as identified the report button is abused by oppressive governments and organisations which wish to silence peoples content. Technology is unable to currently cope with the activity that humans do because the media is so dynamic. Changing a single bit of a picture, or screenshotting a still of a video changes the whole picture completely, making identification of media hard. It is true that social media is aware of this problem and are putting energy into identifying abusive content, but research shows that technologies like artificial intelligence are easily abused themselves, becoming a ‘fascists dream’. Many won’t like to think it, but the ‘dark web’ and social media have a lot in common, content that most in the world find vile to look at. They also have percentages in their network that actively look to exploit young children, in the case of social media, actively groom them to later possibly meet them. While it is correct to be worried about the content that the ‘dark web’ holds and the possibility that it will never be taken down. We should also worry that many do not see the dangers of social media and the tide of issues that these networks face, many that aren’t just technological problems but diplomatic/social problems as well.

Criminals who utilise malware for monetary gains do not necessarily communicate over the ‘dark web’ or have communities or groups in the ‘dark web’. Darkode was a cybercrime forum which had been around since 2007, it had some reputation behind it due to the members reportedly within the community. The community, like many other hacking communities was very private, with an invite only system of registration. This registration differed from others, it did not ask for payment, it was simply inviting what was perceived at one time as the ‘best of the best’. This was to create a private community of elite members, but later ended up rife with security researchers. Darkode was taken down and like much illegal content on the internet, came back up, at least this time it was on the ‘dark web’ to be more ‘secure’ [68]. Although Darkode had immaturity in some administrators and members,

there were many who were pretty big criminals ranging from developers of malware toolkits to exploit kits, these toolkits facilitate grabbing details like keyboard logs and bank details. Evidence of money laundering and carding were also revealed when a security researcher named “Xylitol” leaked the forum contents by taking pictures of virtually every post possible in 2013, when it was accessible through the internet and had not been taken down [69]. What became clear from “Xylitol’s” post was that the forum was in decline, many original members who gave the forum a reputation were either arrested or were not participating in the forum as much. It had begun to advertise for extra members in forums that did not have the best reputation, most likely to try and keep the community active and look busy. Many of the forums that the administrator ‘sp3cial1st’ advertised to had very few skilled members, the ones who were skilled hardly posted content or viewed many parts of these targeted forums. What administrators started to receive were new recruits who would have potential and would want to prove themselves, later it was proven Lizard Squad had affiliations with the Darkode forum [70]. Although the takedown from law enforcement was significant, it was described as “one of the gravest threats to the integrity of data on computers in the United States and around the world” [71]. It would in the past, to be seen as one of the “gravest threats” but after seeing its decline in 2013 when screenshots were revealed by Xylitol, it seemed criminal landscape had moved elsewhere or had become more distributed. The forum like many dark marketplaces and other areas of the internet of interest was monitored heavily by security researchers and more than likely law enforcement. The issue with forums is of course it has a permanent record available on what you said at that time, giving a concrete understanding of the landscape. Communication over far more private channels such as using XMPP (Instant Messaging protocol) allow for far more intimate conversations less susceptible to be picked up by law enforcement. I could add a far more descriptive finite argument on XMPP instant messenger security and the problems it faces, but in general terms, it’s less susceptible than a forum.

What was quite clear was the reputation Darkode seemingly had from the early years of its birth, was still there in later years, many people over Twitter publicly asked a security researcher “Xylitol” for an invite [72]. The system in place on the forum was that every member had a number of invites which they could nominate someone to join, the big part about the invite system is that it connected two people together. Members had to use their invites intelligently, inviting members with high ability in various areas of crime. What seemingly happened was this invite system suffocated growth to which the administrators were trying to fill by mass inviting people and advertising on open forums full of unskilled hacker kids. One feature of the forum that was quite special was the “watermarking” feature for each user. The concept is similar to many oppressive regimes where distribution of media is forbidden (the media being pictures of the forum contents). When researchers released screenshots of forum posts within Darkode, administrators were able to work out the user id (identity) of the suspected researcher account from elements on the page [73]. This is fairly impressive, it reminds me of North Koreas system of tagging metadata of users unique id’s to pictures and other media to understand how media is distributed around the country and try to limit as much as possible to remove dissent from the regime. This showed that the forum had sophistication but as I’ve described it degraded heavily to a point where it was looking for unskilled members, what it originally was designed not for. Darkode reportedly moved onto the ‘dark web’ after its take down from the internet, although because of many arrests after the mysterious take down many thought the site would not reappear. It is questionable whether the reappearance of the site was genuine, it was hacked and the database was leaked to ‘database leak’ sites. It is always seen as quite ironic that a forum devoted to hacking and computer security would be hacked, it is true that we cannot verify the authenticity of the forum and therefore cannot judge. The forum is now dead in 2017 with no references to it or meaningful content about it

around anymore. This community never really embraced the ‘dark web’ but was labelled a “grave” threat to the integrity of innocent victim’s data. One of the most sophisticated hacker forums that was English speaking seen by many, declined in ability in the later years before being taken down by law enforcement. Some of the most apparently sophisticated criminals and biggest threats to our security did not move to the ‘dark web’ and in fact, actively used the internet instead of utilising the ‘dark web’ for community hosting.

One thing many use in criminal ‘private’ communities that privacy activists also develop is Jabber which utilises the XMPP protocol usually coinciding with the OTR plugin that is available (Off-The-Record). This is much like an e-mail service as The Intercept has alluded to [74], but with a big difference, it is far less worried of the identity of a user and takes seconds to setup. Again, it is decentralised, unlike e-mail which is becoming far more centralised with businesses opting to go to cloud solutions. Because of its decentralised nature, its plugins and lack of blocking IP’s from many services, many individuals can register the accounts using TOR or blacklisted VPN’s. There is no limit with the amount of accounts you can register, although many employ CAPTCHA as a defence of mass account registration. This is a common method of communication outside of community forums where individuals can discuss things such as payment, important links to files or accounts and other sensitive information that criminals may distribute. It is again, not only criminals who use XMPP, many, including myself use Jabber to talk to people who are security researchers, journalists and hackers in the broader sense of the word. These servers can be hacked and have been in the past, this is a risk in being decentralised in this manner, where security is down to the operators of a service unless you utilise which many do, OTR. Off-the-record messaging requires both clients to have a supported plugin in their instant messaging client, with this implemented both clients can feel much safer because of encryption, to be more definitive, end-to-end encryption. This end to end encryption means the jabber server is simply the vessel in which a client will use to receive and send messages, it becomes pretty much impossible for a server to read what a user is saying because it is encrypted. This is much like a relay in the middle of a TOR network (not completely though, I must add), where the contents will be unknown to them, they are simply forwarding them. This means it is very hard to read what anyone is actually saying in this particular state, the servers can spring up from anywhere and the use of OTR means reading from hacker or seized servers is a challenge. Although the ‘dark web’ can be used with Jabber as a proxy, you can communicate through the internet, although many may argue that this particular way of messaging would constitute as being in the ‘dark web’. The fuzzy and confusing lines in which people define such terms mean much of new privacy orientated projects utilising cryptography are sometimes merged with projects which are traditionally seen as being the ‘dark web’. Nevertheless this messaging protocol is wide in its applications much like the ‘dark web’, but is treated less harshly than anonymous networks. XMPP, the protocol that is used in Jabber, is also used in social media network messaging, IoT (Internet of Things) projects and gaming.

When I was younger I first came across the XMPP protocol through Facebook. Childishly when I was still in school, I was pursuing the idea of bypassing content filters and being able to communicate with people over Facebook messenger. Although now, Facebook has deprecated this ability (sorry young hackers still in school) at one time they allowed XMPP to communicate to the Facebook Chat API [75]. This allowed many to use a XMPP compatible client to message friends from Facebook, some jabber services were available online and allowed me to communicate to friends online through online jabber chat clients. This, although I admit not the most noble of intentions, showed why XMPP cannot simply be understood as a criminal tool, but a protocol used by many, much like the classic TCP/IP. Many of

the projects that utilise XMPP are for improving how we work on the internet and usually revolve around us becoming more connected, after all it is a messaging protocol. The exploitation of this protocol is evident, it is not only used by criminals as communication between each other but is also seen as a useful communication channel between themselves and malware [76]. Criminals have also used this protocol as to notify themselves in a particularly notorious piece of banking malware called Citadel, which was prominent around 2012 [77]. Anonymous networks are different in nature and usually aren't set protocols on how routing is addressed in an over confusing manner. The similarity of XMPP and anonymous networks, particularly the anonymous network TOR, is the exploitation from criminals. Criminals understand that both have desirable properties for them, which include decentralisation, open source code, privacy considerations, cryptography implementations for better security and more. These were not designed for criminals but were embraced by them, the problem is that many of the ideas that anonymous and protocols like XMPP give us are innovative and pinnacle to keeping our information secure on the internet. It was not too long ago encryption was seen as dangerous.

Lots of what are supposedly private communities leak out there information, such communities such as the very entry level forum for hacking "0day". "0day" has sections for carding (stealing credit cards), malware and other illicit activities. The board is meant to be open with no invite system but allows non-registered users to view titles of posts and the users who post them. This can be seen as a privacy misconfiguration in my eyes, but the board administrators simply see it as how they've set the board up. An interesting aspect of "0day" which is also similar to many other 'private communities' on the 'dark web' is that they not only have an onion address (an address that allows you to navigate to a hidden service) but a generic top level domain. This allows anyone to view the forum from the TOR browser or the internet, essentially allowing anyone from either network to contribute to the forum. This is most likely because most forums hosted on TOR which relate to hacking are dependent on visitors which sometimes do not use or know how to use TOR. This makes the 'dark web' seem less scary, it could be perceived as a network which is heavily connected to the internet, almost like a smaller brother or sister. The amount of connections and traffic that both the internet and the 'dark web' have together makes it seem less like a dark corner and more like a hardened network similar to the internet to me.

There are many websites like "0day" who have a web and onion address, Facebook has an onion address that allows anyone to visit through TOR's hidden services feature, allowing anyone to access the website without censorship. In 2015 Facebook announced that 1 million people use "Facebook over TOR" [78], a huge number when we think of other communities that were or are on the 'dark web', such as Playpen, Hell Reloaded and Silk Road. A comment in a company blog post on Facebooks corporate section depicts why it is so important to have Facebook over TOR, a user comments giving praise to Facebook on their decision to have their service over TOR due to the censorship they receive in Ethiopia. The Ethiopian government blocked social media in the hope it would stop further protests and dissent across the country, they also blocked TOR as well using a technology called deep packet inspection [79]. This technology is quite common in repressive regimes and areas of the world which have an aggressively authoritarian government. The anonymous network project TOR has features which now allow Ethiopians to access TOR itself so they can access hidden services and the external internet without censorship [80]. Ethiopia is seen as one of the least free places in internet freedom [81], this means activism online is watched intensely and many social media sites are blocked. While the erosion of more internet freedoms is becoming increasingly common through many countries,

Ethiopia is certainly seen as one of the worst in world. The TOR project certainly has allowed citizens around the world to feel more confident and secure in displaying views online, if the figures of a million users using Facebook through TOR is correct, Facebook must be the largest community by the numbers connecting to its service. These anonymous networks do not have to only be for activists expressing views online, blocking social media in a country means many citizens become outsiders in a world which is becoming ever more so connected. Everyone in the world is connecting through social media and technologies like anonymous networks mean that even if a government disagrees with the idea, users can message who they wish, however banal a conversation could be. While I believe that activism takes place through TOR and is the main reason why so many get behind the anonymous network project, I think it is over romanticised, many individuals most likely wish to follow updates in their country, talk to people around the world and take part in a less restricted life. I think the argument can be made to piracy on the internet, however heroic some intentions can look from piracy, the majority of users of piracy simply wish to consume content. This does not mean this service is any less important, if anything it is more important, it allows no idea to be censored or shutdown. Facebook is the 3rd most visited site on the internet and on the 'dark web', Facebook is one of the most visited, if not, the most visited hidden service. With this information, many may think differently on the importance and significance of anonymous networks.

If Facebook isn't the largest hidden service, then it must be AlphaBay. This hidden service is the current (After editing this, yes, Alpha Bay has now been seized) successor to the notorious hidden service 'Silk Road'. AlphaBay has a frequently asked questions section, it outlines its origins stating that "AlphaBay is a marketplace founded by reputable members on Russian carding forums, and transferred to new administrators in May 2015 in order to make better plans for the future growth of the market". Because of how secret AlphaBay is, it's hard to gage how many registrants there are and much of the activities within the market. I have already described how much of the market in AlphaBay is essentially rubbish, full of guides which cheapen the look of the market, especially specialised areas like malware. AlphaBay administrators have understandably noticed how shockingly little malware developers have embraced the marketplace and are attempting to remedy this by making a new sub-community within the forum which is primarily focused on malware and coding. The forum post by an Administrator 'DeSnake' outlines it is a community which is currently invite and applications only, so users will have to post and show why they are worthy of being part of a private community. What's quite comedic is that applications are essentially public, registration to the forum requires that you are registered to the market and link the accounts together. After you successfully register an account you can view posts, although there are private sections of the forum, you cannot read any posts without being a member of the forum. The applications are posted on the thread where users reveal information about themselves, many are inexperienced and can only code in high level languages. While it's becoming increasingly easier, it is best to be able to code in low level languages when developing malware. The inability to attract large members of talented programmers who develop malicious code is obviously a worry for the administrators of AlphaBay, who wish to make the marketplace the de-facto marketplace for all blackhat activity. They have had marginal success, with developers of the ransomware called 'Philadelphia' selling their ransomware on AlphaBay. This group which have been active on AlphaBay, have had many reports about them from Anti-Virus companies. But they still are not very sophisticated. They utilise the programming language 'AutoIt' to be able to support all Windows machines (which they proudly advertise). This programming language is very easy to decompile and read a representation of what the programmer was coding, far easier than C++ or C. As well as being trivial to decompile, the file size of most executables from AutoIt compilation is large,

usually over 1MB. This bloated compilation means it is far more difficult to distribute the malware, even if the internet has become far more connected and faster than before. Nevertheless it has been distributed and many companies have picked up on its presence, most files which are coded in AutoIt are automatically treated as malicious and therefore would require further obfuscation from a 'crypter', which would most likely increase the size. The use of 'UPX' is shown in screenshots that the seller shows which is to make the file size smaller, but is also widely seen as malicious from many antivirus solutions. As this seems to be the most notorious malware from what I see in AlphaBay, it is no wonder the administrators of the site are attempting to make a community devoted to improving the skill level and quality of the malware market within AlphaBay. The only prominent piece of malware is ransomware, which is fairly easy to develop without any special features to it. The people who are currently using this ransomware are a very wide range of individuals, many are utilising exploit kits to distribute their malicious executable, which requires contacts and trust by the exploit kit developers. Others decide for a more targeted approach, by utilising email to attempt to infect potential victims [82]. What is clear to me is that even with a hefty price tag of over $300 amateurs with little to no idea how to use this purchase it in the hopes to make money, in the forum post advertising this ransomware on AlphaBay, users ask for support, more features and help with spreading methods.

In April 2017 a teenager was arrested for spreading Philadelphia ransomware to a local company in Linz, Austria [83]. In a post within the forum thread for Philadelphia ransomware another individual boasts his wish to infect his work which is a theme park where they receive large sums of money. Although there is evidence of criminals with knowledge of how ransomware works and how to keep yourself safe from being caught, there are many currently in AlphaBay who purchase products like this and begin their journey into further criminality such as malware. AlphaBay is primarily a drugs market, even if they do have a wide range of categories for different products that is where most of the sales are made. To become the 'dark web' marketplace giant, they must have individuals who are capable of producing the next generation of dangerous malware. They must find individuals who understand the internals of operating systems and networks. Currently, they have a small set of less than sophisticated developers who have a customer base with a wide skill level. They must be able to fill the gap with competent developers to be seen as the marketplace to go in the 'dark web', many have rejected the use of AlphaBay and stuck to classic forums to discuss and develop malware. It may be that the seasoned and more sophisticated members who develop and understand malware do not currently trust the platform, AlphaBay introduced an API which led to private messages being leaked. In total, 218,000 user's messages could be retrieved from the individual who was able to identify the bug [84]. This led to private addresses being up for grabs for a few hours before the AlphaBay administrators were able to patch the security bug. Because how open AlphaBay is, it must implement the harshest of security measures, even with such stringent security, AlphaBay information was still able to leak. The individual was given a reward for their findings, none of the private information was given to law enforcement, well, publicly there is no evidence of this. This has now happened twice for AlphaBay, where private messages have been leaked due to a flaw in the system. Even though hidden services are masqueraded behind TOR, they can still be hacked. AlphaBay is much larger target to law enforcement and competitors than other private communities, many who develop malware and technology to facilitate the spreading of malware naturally aren't that sociable. With the ability to sell toolkits that are more sophisticated in more private areas of the internet, there is no reason to transfer to a place where it is publicly sold to anyone. A lot of developers wish to keep their customer base small but active, but implementing new features and keeping stable. Many who are professionals sell updates to their software for a price. If we look at the malicious software products available on the 'dark

web' markets we see a polar opposite with sentences like "Lifetime updates for free" being a regular occurrence. This lines would usually be reserved for products that are seen in more 'clearnet' entry level hacking forums where developers starting out wish to make the largest amount of money as fast as possible.

The private communities that are within the 'dark web' have some worrying content, from content like child porn to drugs, it is as much of the media portrays it, a lawless area. But these communities are fairly rare, when we look at the amount of communities that come and go, which may be for drugs or hacking, there are far fewer than first thought. The amount .onion addresses that are actively used are around 60,000, within these are hobbyists, privacy advocates and even political parties. Comparing social media networks with private communities within the 'dark web' shows we should not only be worried what's on the 'dark web', but what's being tolerated on our social networks. There are many reports of horrifying content being held on social networks and private groups sharing questionable content in closed groups, these chilling similarities give us real questions on how we regulate content not only on the 'dark web', but in places which hold masses of data on us and control large portions of the internet, social networks. Current technological buzzwords like artificial intelligence do not give us an easy fix, we currently have a situation where huge pieces of information are published on social networks in which manual analysis of content would be impossible. The 'dark webs' most notorious marketplace at the moment (Again, when writing this, AlphaBay was still online, the marketplace is still in flux and has no dominant marketplace yet), AlphaBay, is full of drug suppliers that are competent and able to sufficiently provide good quality drugs. The marketplace is also full of other categories, one which I have highlighted, 'Malware', is lacking in professionals who are sophisticated enough to develop a good piece of malicious software. These private communities, while some worrying, are not as open or sophisticated as some may think. Some of these private communities are actually beneficial, allowing activists and oppressed citizens to view the world and communicate without fear of government surveillance. The surprising fact that Facebook is one of the largest sites (if Facebook numbers are correct) hidden services available on TOR provides a different picture of the landscape anonymous networks have. While they do, largely have illicit material, large portions of these anonymous networks are used for freedom.

CHAPTER 5
ON TERRORISM

Extremist content which cannot be regulated is why many states fear anonymous networks, the apparent lack of ability for states to control extremism not only on the ‘dark web’ but on the internet is a worry for anyone. The media reports on the ‘hunt’ for terrorism on the ‘dark web’, where terrorists breed easily compared to other areas of networks, but this is simply not true when looking at hidden services. I have previously cited a study which crawled through hidden services on TOR [17], what is evident is how many sites are inaccessible or inactive/non-illicit compared to extremism. The study supports the idea that individuals of extremist ideology do not use anonymous networks hidden services feature as much as first thought. The amount of traffic that goes to hidden services is miniscule compared to traffic going to domains on the internet, which also supports the idea that many use TOR as a proxy like service to mask their identity while viewing the ‘clearnet’. There are of course some hidden services that serve extreme content, but is dwarfed by content on the internet again. The simple mathematics of the ‘dark web’ and the internet is that from the reported TOR metrics, there are only around 60,000 active hidden services. There are considerably more sites on the internet which potentially host extremist content simply by the size of the internet, it can be the case arguably, that these few hidden services have a large following, but very little evidence is available for this. There is though, more evidence of terrorism utilising and grouping on encrypted messaging applications and social media which are available on the ‘clearnet’.

A lot of the terrorist attacks taken place in Europe have had coverage referencing the use of messaging apps such as WhatsApp, Telegram and Signal being used just before the attack by the media. These apps allow you to message individuals or groups using end-to-end encryption, making it hard for others except the sender or the recipient to read the messages. The message applications are capable of connecting through an anonymous network but many still seem to use phone networks and rely on end-to-end encryption that is available on these applications for their security. The use of anonymous networks with end-to-end encryption is becoming increasingly popular, as extremists begin to understand the technology and why it is important for them to route information into TOR or similar [85]. This makes traffic analysis much harder but it does not mean that WhatsApp is a completely safe haven for terrorists and extremists, even with the use of anonymous networks, WhatsApp cannot be prescribed for giving the ability for terrorists to go ‘dark’. It is correct, that messages are unreadable to not only law enforcement, but to WhatsApp and Facebook, this is because of end-to-encryption. This is not a refusal from Facebook, as many media outlets have headlined to aid law enforcement [86], they

simply just cannot because of the technology they use. This is to make sure even if WhatsApp was hacked, the ability to read every message, which would be disastrous, is impossible. Many individuals use WhatsApp; UK politicians [87], Syrian activists [88] and foreign correspondents [89]. Most of these examples are public, but there may be many individuals who have sensitive communication that we do not know about, such as senior diplomats, businesses and employees of important governmental organisations. Because of such public examples, it is obvious why it is so important why end-to-end encryption is used. The amount of messages transferred are huge, if they were stored in one location such as WhatsApp servers it would become a global disaster if it were hacked. End-to-end encryption provides no possibility of leaking messages because WhatsApp have no idea what's being said (unless you type a URL, and you're the owner of the URL location) [90]. The internet overall has been moving to safer modes of transport for a few years now, where most popular websites serve the user HTTPS by default instead of unsafe HTTP. Many may be thinking while this is fantastic for the end user, terrorists still use this service and it's incredibly irresponsible to give terrorists a 'safe place'. But this is simply not true, while the metadata is encrypted in transport to WhatsApp, it is given to WhatsApp servers and stored. This would allow law enforcement to request single users metadata, which can provide a good picture on what is happening. There are privacy concerns by many that WhatsApp holds this metadata which can shared to Facebook to drive more targeted advertising [91]. Metadata can contain a lot of information that can sometimes be more important than the messages that are actually sent, it can correlate people together and understand how frequent people talk to each other amongst other important attributes. I am currently researching on the importance of connections rather than user generated content (messages) and can see the importance of metadata, metadata can be seen as the attributes of a network message. What time was that sent? Who was that sent to? When collecting this metadata you can deduce strong relationships between people, patterns of behaviour and also begin to predict abnormalities from collection of metadata. One important point to note here is that WhatsApp must be willing to hand over data to law enforcement, the metadata is encrypted in transport as noted by WhatsApps own whitepaper [92]. Even though the data is encrypted over transport it is eventually received by WhatsApp where it can be read correctly, this metadata is an interesting aspect to the privacy and security debate that we currently have. Even with a connection over TOR through WhatsApp, the identities of WhatsApp users are down to phone numbers, these identities are identified in metadata and can give law enforcement a picture of what connections a suspected terrorist has. Many may think that timestamps of successful messages are fairly useless, I would disagree, but WhatsApp also asks permission for, is features like location which are more than likely going to be in metadata if enabled. TOR and anonymous networks allow the identity of a user and contents of the data to be completely secret when in transport, this does not mean that WhatsApp is like a hidden service. TOR will be acting more like a proxy in this situation, a TOR exit node will be connecting to the WhatsApp service but the actual metadata will be generated locally on the phone. Anonymous networks allow a user to stay safe during the transport of data, but the responsibility of the identity will still remain with the service, in this case WhatsApp. The balance between law enforcement being able to do its job and online apps being able to keep the privacy of its users is tough, but on a case by case basis, which are thought upon by apps on the severity of the case, is the best possible balance we have right now. There also ways of retrieving messages outside of the end-to-end encrypted channel, such as infecting terrorist's phones with malware and retrieving the database locally. Which is something the ex-chief of GCHQ also highlighted in an interview for the 'Today' programme on BBC Radio 4 [148]. The messages are held in an encrypted database where the key is held within the phone, although a high privileged user is required to derive the key, it is certainly not out

of reach for law enforcement to achieve. If the actual phone is able to be retrieved in some way, which has no operating system encryption and a lock screen can be bypassed, non-root (less privileged users) local retrieval is possible as well [93]. Finally, another possible way which has been connected with the Turkish government's methods, is retrieving messages from user's backups [94]. A feature that was brought by WhatsApp that allows you to backup your messages into the cloud. For any individual in security, this sounds like the worst possible feature you could ever imagine, but it has been implemented. It should be noted that this feature is not on by default, although a nag screen is presented to a user every once and a little while, the user must interact to enable this feature correctly. The messages that are saved to cloud solutions such as Google Drive seem to be stored in plaintext, this would make sense as keys for encryption for these messages may change (down to a number of reasons) and the user will unable to ever decrypt their messages again. There would be no reason for backups if a user would be unable to actually read the backup after a while, so it is obvious why the messages have been left without encryption. This does risk leaving WhatsApp users susceptible to abuse, simply because law enforcement could request data from the cloud provider (having a good guess probably) and read messages without worrying about end-to-end encryption. What is clear to me is that the media is not being clear with individuals about the overall security of these applications, it is fairly clear even with the use of anonymous networks like TOR that a user can be not only be identified but potentially their messages could be read. The big problem that law enforcement may have is the relationship they have with the service provider terrorists or extremists are using, most times it won't be a technological problem, but an ideological one, of complete privacy. The actual amount of requests for information on users is not revealed to us by Facebook, although Facebook has a transparency report itself there is no such report available for WhatsApp. It is hard to understand the relationship between WhatsApp and law enforcement on how much metadata is given to authorities, but it would not be too hard to request information on the basis of terrorism and retrieve the contacts the individual had been communicating with if the relationship was amicable. The WhatsApp messaging service is not a hard to reach space on the internet, neither does the parent company Facebook, give terrorists a safe space. The whole point of end-to-end encryption is to put the reliance on the device and not on the servers, making it much better for the user in regards to security. Even with the implementation of anonymous networks into the connection of WhatsApp, it would still be possible to identify a user by its phone number, which is WhatApp's identifier. Because of this identifier you can quickly understand someone's contacts without the physical access to the phone, the metadata sent to WhatsApp servers should allow you to see who speaks to who, building a contact list of an individual. Because the application is installed locally on the phone, the metadata is about the phone, so even when the metadata is transported anonymously, it will eventually reach WhatsApp servers and can be requested by law enforcement. This is not perfect in security terms, but in my eyes is the best we have right now. There is no need to read messages of millions of people to which much can be taken out of context. The data should also be requested on a case by case basis, there should be no backdoor or channel where governments can simply lift data

There is a vast difference between many terrorists technological aptitude. Most use messaging applications, some use WhatsApp, others use services like Telegram, Signal and iMessage. At one point they must identify themselves and send a unique identifier of some sort, be it a phone number for WhatsApp or identification number for other applications, individuals can always be attributed to a unique identification through a channel which can be requested for by law enforcement. Terrorists also differ in their competency in operational security, many use different techniques that are less technologically sophisticated. An example of a different approach that didn't use encrypted messaging

applications or anonymous networks in communication during the attack was the Paris attacks. This must be taken with some understanding that we are not analysing the setup previously to which a network must have been devised to retrieve explosives, weapons, forged documents. These contacts may use encrypted messaging applications and anonymous networks to communicate with each other, one fact we do know is that just before the Paris attacks, all the individuals used burner phones which were communicating in plain text (possible for agencies to read). One text message that was sent that the police later read was “On est parti on commence.” (For those that don’t speak French like me, “Let’s go, we’re starting”) [95]. Court records, according to the New York Times indicate that previous plotters of attacks would use simple phone operations such as calling and SMS to plot attacks, while this group used burner phones to ensure it was harder to follow and track operations during the attack commencing [96]. The use of encryption and anonymous networks is not completely out of the picture as previously stated, even in the New York Times article it describes a strange operating system which was used during the attack which hostages saw, describing it as having “no image and no Internet”, many are presuming that this would be encryption software of some sort as it is also described as having “lines of code” when the laptop was booted. Anonymous networks may have created a smokescreen for the attackers online but the use of burner phones made it hard for law enforcement and intelligence agencies to track the individuals. They were well versed in how to remain safe by using burner phones religiously, some articles have described how the burner phones used while communicating during the attack were activated only hours before. This problem is technological but is not down to encryption or anonymous networks, this is because of how erratic the nature of the groups communication was, not relying on one single phone to communicate with, which presumably made it much harder to be tracked.

It is obvious that terrorists use anonymous networks and encrypted messaging applications, it is confirmed to me by reviewing a document which outlines operations security measures to take which is advised by ISIS recruiters (Note, this manual was available on the ‘clearnet’, I did not access it via an anonymous network). I have only reviewed a handful of manuals that have been distributed but it is clear that these operatives have not researched the security issues a terrorist may face extensively, the reliance of the security on applications developed by westerners is very high and has little to no advice on a diverse range of subjects (I of course only have access to limited material). Short sentences describing why someone should use TOR are dangerous and show weakness in the writers knowledge. There is less than helpful advice which can possibly give problems to ISIS recruits if they follow a particular document completely, but it does offer worryingly good advice on encrypted messaging applications, operating systems and suggests using TOR to evade detection. WhatsApp is seen as not a viable choice because of the phone number being an identifier, while other alternatives are seen as the better option. This is interesting to see, because many indications from the media and many governments around the world after attacks always discuss how attackers have used encrypted messaging applications, the most often attributed applications, WhatsApp and Telegram. The difference in opinion with encrypted messaging applications in regards to the terrorist group “ISIS” shows a lack of solid policy and organisation. Terrorists make mistakes and all have different levels of technological ability, not all levels of terrorist organisations are going to uphold operational security, which would usually require members to browse through anonymous networks such as TOR. Many modern terrorist organisations are very forward in releasing propaganda online, although devout followers can more than likely use the ‘dark web’ to watch or view content from their chosen terrorist organisation, a lot of the internet will be used to not only host but share extreme terrorist propaganda. While anonymous networks and encrypted messaging applications allow for transport for information

securely, there is no real migration to the ‘dark web’ as many media outlets put it, in regards to terrorism, specifically Islamic extremism. Hidden services sometimes do contain extremist content but not to the levels many will see on the ‘clearnet’. The information must go somewhere, many simply use TOR as a proxy and utilise services like WhatsApp, Telegram, Signal and more. The bomber who attacked an Ariana Grande concert in Manchester which killed many used tutorials on the ‘clearnet’ to understand how to make a bomb. The video tutorials were available on the video sharing platform, YouTube, which has now removed the video [97]. Most articles which provide these claims that the bomber used YouTube to download bomb making videos also include that some materials downloaded were from the ‘dark web’, although vague, it is obviously possible. The anarchist cookbook amongst other relevant material is readily available on the ‘dark web’. The initial steps seem to be openly available on the internet, where anyone can learn without downloading special software like TOR to utilise anonymous networks for terrorist activities. The harsh reality is that extremist content can pass filters that many sites may impose such as bomb making and require manual reporting for content to be taken down. We have previously discussed how even with experimental areas of instant identification, such as artificial intelligence, it isn’t as effective as many may dream it is. This seems to be one of the largest problems that we face today as the internet grows exponentially, how we remove content that doesn’t remove liberty and freedom, but stunts the growth of terrorist activities not only online, but in real life as well. Anonymous networks have a diverse range of active users, but terrorists do not fully utilise the ‘dark web’ as much as drug dealers and drug users do. In regards to Islamic terrorism, specifically the so-called group ‘ISIS’, seemingly wish to recruit through social media and internet protocols. The initial contact from potential radicalised individuals would be through contacts in real life or from social media. The number of accounts which are used to spread propaganda from this group is large and puts pressure on freedom of speech on the internet, we must remove terrorist propaganda from so-called ‘ISIS’, but must be able to let individuals express opinions which are different to show the strength of democracy. Anonymous networks may mask the network identity of a user, but the campaign on social media sites like Twitter could not be only done with TOR exit nodes, the use of technologies such as VPNs would have made Twitter accounts less restrictive and easier to create than on anonymous networks like TOR. Vast scrutiny is put on accounts which are created from a TOR exit node due to the barrage of hackers and nefarious behaviour associated with TOR exit nodes. Google’s head of ideas in January 2016 stated that so-called ‘ISIS’ “must be locked out of the open web” [98], this is far easier to say this than actually perform this action. With the internet or open web full of activity related to malware, child pornography and extreme views, it is obvious that it is hard to keep removing what is deemed harmful content from the internet. We might not be able to completely remove so-called ‘ISIS’ from the open web but removal of content should be concentrated on the largest of networks on the internet such as YouTube, Facebook and Twitter. Radicalisation occurs through social media [99] and making it as hard as possible to send propaganda through these popular networks really hurts the organisation at source. Anonymous networks are not closed off but require further steps to access compared to social networks, anonymous networks require knowledge to access which many do not know. Anonymous networks may be used for communication and planning by terrorists, but recruitment and propaganda is the home for social networks, where individuals are picked to carry out attacks on home soil.

Encryption is used in all modern technologies to keep people safe, including anonymous networks. Encrypted messaging applications are usually used with anonymous networks by terrorists and others to provide some privacy and safety from law enforcement. The use of end-to-end encryption worries many states, they wish to know not only know when a message was sent and to who, but also what the

message contained. Metadata is still available to derive some information about an individual, this relies on first identifying that someone should be monitored of course. Metadata is important information about how people communicate, such as who is sending to who, what time a message was sent and what location was this message possibly sent. This should be sufficient for states to be able to understand connections between contacts, the ability to read all messages from applications would be disastrous for privacy and modern day democracy. WhatsApp and other messaging applications are not only used by potential terrorists, but politicians and journalists. Therefore messages should be end-to-end encrypted but law enforcement must be able to retrieve metadata from messaging applications to keep people safe and track potential terrorists well. The activity that terrorists have on the 'dark web' is minimal when we look at hidden services, the TOR network hidden services that are active have small pockets of extremist content, but is dwarfed by crime and drugs by looking at surveys of hidden services. Anonymous networks do provide a mask for terrorists to use which does not reveal their actual internet service provider, but we can gather information and identity on an individual in many other ways. There are technologies that are used by terrorists who carry out attacks that do not rely on encryption and anonymous networks, it must be understood that there are many different ways of attempting evasion from law enforcement and intelligence agencies. Content which helped aid an attack in Manchester started on sites such as Facebook and YouTube and later the 'dark web'. Although details are not clear, it is obvious the 'dark web' is not the first place to go to understand how to produce a bomb for an attack. The 'dark web' was used to help in understanding bombs, but it is not the easiest resource where it is easy to find content on bomb making.

The purchase of weapons is another feature commonly associated with the 'dark web', seen as the natural place to order if you have no real life contacts. When looking at 'lone wolf' terrorist attacks, be it from right wing extremists or Islamic extremists, the 'dark web' is placed as the one source for an individual to successfully purchase primarily, firearms. In the Munich attack of 2016, police believed that the weapon that killed so many was purchased from the 'dark web' [119], while evidence isn't available, there are references that it was bought in a 'darknet chat' [120]. Which hints not at a marketplace which is commonly what media outlets refer to often. Marketplaces commonly sell weapons and for the most part, the sellers in these marketplaces cannot be verified. There are a numerous amount of cases where an individual has an intention to purchase an offensive weapon, but is hit by a law enforcement sting where undercover agents pose as weapon sellers to find addresses of people posing a risk to the public. There are confirmed purchases of a guns on the 'dark web', although it is quite difficult to understand the volume of gun purchases from the 'dark web', as there are no way of tracking items being transported. Much like drugs in the 'dark web', guns and other weapons are usually concealed within other items to disguise the actual item. One case which was seized when being transported from the US to the UK was a gun which was being disguised as an 'antique radio' [121]. This case also supports the assertion from recent research that the US is the primary exporter for 'dark web' firearms. The research was conducted by RAND, this well needed research found that the 'dark web' was an enabler for the illegal firearms trade. What's interesting about the research is that it does not give an absolute conclusion on the marketplace, stating that the "dark web has the potential to become the platform of choice for individuals (e.g. lone-wolves terrorists) or small groups (e.g. gangs) to obtain weapons and ammunition behind the anonymity curtain provided by the dark web. In addition, the dark web could be used by vulnerable and fixated individuals to purchase firearms" [122]. The report also indicates that firearms listings were the most common listing on the dark web, I think that this conclusion of the 'dark web' is incorrect, I think drugs are truly the most common listing on the 'dark web', many are hidden in invite only communities. Firearm listings are

increasingly being created by scammers and law enforcement, there seems to be far more availability of drugs, although, drug products can also be susceptible to scamming. What is clear is that the firearms market is just emerging as more and more individuals decide to use the 'dark web' to find weapons. The increase in media attention has more than likely brought new purchasers who previously would have no knowledge of the 'dark web', this emerging market has aided terrorists, gangs and twisted individuals to carry out their deeds. The real question is, how much of the 'dark web' illegal firearms trade is 'legitimate' (not a scam) and how much of an epidemic it is. In recent year's terror attacks on Europe have had less guns, instead knives and vehicles have begun to crop up as the weapons of choice. There are many reasons for this trend and a full analysis from me would be impossible (I'm no expert, obviously!), what is clear to me is it is far easier to rent a vehicle or to buy a knife without causing too much suspicion compared to a gun. A gun has only one real purpose, smuggling these items are risky and also they cost a fair amount instead of purchasing large knives. A gun can fail, guns may not work if they are remade and also purchasing a gun provides links to associates from terrorist group's contacts which can hinder future operations. Remote 'lone wolf' terror attacks rely on the individual to gather their own weapons in most cases (there are cases where they are helped), finding a gun on your own may be a tricky task, while renting a vehicle or large knife requires very few steps. This is why ultimately I am undecided on how serious the 'dark web' illegal firearms trade is, it is currently undergoing a period to which many people are waking up to the real idea of selling actual guns on there, whether there is enough supply and demand to keep the trade afloat on the 'dark web' is something yet to be seen. Terrorist groups seem to be moving to alternate methods but whether it remains in one area or away from the purchase of firearms is unknown. What is clear, is the 'dark web' is not the one stop shop it may be perceived as, gun listings are riddled with stings and scams, the purchase of knives in the UK has only recently become much harder to order over the internet, previously one could simply ordered knives online without too much verification of age [123]. What is clear is that we cannot simply attribute the purchase of firearms simply to the 'dark web', so much is unknown in this area and far more research is needed for a more conclusive answer.

Many sympathisers and members of the so-called 'ISIS' group are not as open to the idea of embracing advanced technologies in the aid of privacy and security. While I have discussed that guides have been made and many members of so-called 'ISIS' are technologically competent, it does not mean that all individuals in the group are, many may not abide to policies or advice given to them. We must understand that many of these individuals are like much of the world population and do not receive intensive training on operational security or security at all for that matter. It is much easier for sympathisers, especially, to abide by minimal security guidelines such as using an encrypted messaging application and utilising VPN's, most likely free. This became apparent in an eye opening article from ComputerWeekly by Bill Goodwin [100]. It is much easier to install a few applications from the Google Play store and use a phone than to follow what many may see as laborious steps for the sake of security. A good example that would resonate with many is the use of PGP (Pretty Good Privacy) for the safe transport of emails, which in the security community in 90's thought would take off. It did not. Security professionals today now admit that PGP isn't user friendly and overall, it sucks. It doesn't allow an easy way for emails to be encrypted instead of being transported in plaintext. Many in the security industry would advise that PGP is 'best practice' and should be used for confidential information through email, but because of its inability to be easy it has largely not been used, even by people in security. There are many who agree in the security industry that we should "throw in the towel" for PGP [101]. Unlike TLS (or SSL for the old folk), PGP has not been widely adopted as standard, it has become something that some security professionals do and vigilant security conscious

companies do. HTTPS (TLS/SSL) transport is becoming increasingly normal with most large companies now using HTTPS by default when browsing. Terrorists groups, especially large terrorist groups face this issue of having to try and compromise to less security conscious individuals, which seems to have resulted in adoption of popular encrypted messaging applications like Telegram. TOR and Tails have been “shunned” as discussed by Bill Goodwin, this doesn’t mean some do, but the large majority of the group finds they cannot progress further than encrypted messaging applications. Many of the guides that are given to so-called ‘ISIS’ sympathisers and members reference often free VPN’s that can be downloaded from the Google play store. This is not a good idea. The reason for this could be because most of these members are placed all around the world where instructions come remotely, possibly to individuals who only have similar ideology to individuals online. ‘ISIS’ are a group which have a small set of individuals who are competent with technology, the problem is that the group overall lacks understanding in more advanced subjects in terms of technology. When spreading propaganda online the group hijacked Twitter accounts and signed up masses of accounts to social media, these methods are relatively trivial and are regularly used by spammers and fraudsters. The misuse of hashtags is also not a new method in social media, again, many criminals use this to reach innocent users who may visit content from a social media post. What is clear is that much of what the group has done in public in regards to social media is unsophisticated, the issue is the energy that individual ‘ISIS’ sympathisers and members have. Not a vast amount of training is required to flood social media with propaganda, it can indeed be done through a phone quite easily. The worry should be when and if terrorist groups begin to start taking anonymous networks seriously, utilising hidden services to where it becomes ‘impossible’ (I put in quotations for a reason, never say impossible) to track in any meaningful way. I do not see this happening anytime soon, anonymous networks can be slow, hard to work with and doesn’t allow members to spread propaganda and recruit openly. Advertising a service requires the internet, and to advertise effectively you must be able to utilise the ‘clearnet’ where you must have a reputation or a large following. As an initiative takes place to try and combat terrorism on the internet through an alliance of major internet companies [102], it is only time that can tell us if future terrorist groups decide to embrace the ‘dark web’ or are able to exploit the internet still. We also must note, I am modelling this conclusion on how the well-known terrorist group so-called IS utilise technology, other groups such as al-Qaeda have a different approach to recruitment, technology and ideology. The assumption is many terrorist organisations will take note of how the so-called IS had been able to recruit through social media easily.

CHAPTER 6

THE IMPOSSIBLE PRODUCT

With the advent of the ‘dark web’ the media have been relentless in their coverage of it, mostly due to the misconception that terrorists and paedophiles fill these networks, but also due to the criminal element which follows the term ‘dark web’. The fear of being unable to know the identities or origins of criminal activity worry many, including businesses around the world. The understanding of the ‘dark web’ is most likely minimal in many businesses, because many legitimate businesses do not see any reason to conduct business on such a platform. This is especially true as many label anonymous networks as the ‘dark web’ which gives the impression of something evil or wrong. It is true, that credit cards and business data is transferred through anonymous networks, indeed the ‘dark web’ has many sites that offer such data. It is natural that companies and organisations wish to have some form of intelligence into this platform, where they can understand the patterns of criminals in this seemingly opaque network. ‘Dark web’ monitoring is a product that to me is impossible, understanding the marketplaces, forums and credit card shops within this small network will be a mammoth task and would involve exploitation of anonymous networks to fully monitor individuals. Without exploitation of anonymous networks, such as entering new relays to derive some forms of information, ‘dark web’ monitoring will rely on analysing and understand hidden services, which is what I think most ‘dark web’ monitoring services actually do. The traffic on hidden services is minimal compared to individuals using TOR like a proxy, thus, not getting a full picture of the users on anonymous networks, like TOR.

I decided to look at recent marketing videos of various companies advertising ‘dark web’ monitoring and they do not give me too much confidence that they actually work. A large amount of companies seem to advertise the service of identifying threats to find fraud, stolen credit cards and business assets information that surfaces on the ‘dark web’. Most if not all carding shops (credit card stealing shops) from the ‘clearnet’ or ‘dark web’ do not reveal any information without authentication of some kind, be it logging in with a username and password or a mutual assurance of criminal reputation. After this information is passed through correctly, individual credit cards are censored in parts until the actual purchase takes place, the authenticated individual willl know the credit card type and the country it’s from but the other details will only be revealed after they have been purchased. It is very rare that credit card shops reveal any more than this, account numbers may show minimal information, but the overall amount of information is not given until it is purchased. This means it is basically impossible to understand what the criminals are selling without actual purchase of data. I hardly think monitoring platforms are essentially automating purchases for credit card information. So I do question what these companies are actually doing. In many forums and communities public credit card ‘dumps’ are posted, samples to give authenticity and reputation, although they are mostly worthless as they have passed

through many hands since initially being gathered. I think these public data dumps are what many monitors follow. It is not just credit card information that is distributed amongst hackers, hacker communities usually have a sub-forum devoted to public data dumps and private information such as login information and databases that have been acquired by hacking a company. These pieces of hacked information, much like hacked credit cards shops or carding shops as they are commonly referred to, are individually sold because they are worth something. There are, on occasion where websites names are mentioned, but the most important information, such as the account name or subdomain that is worthy of money, is only given after monetary purchase. Monitoring sites may be able to purchase individual hacks or accounts, but the hacker may be lying.

'Dark web' monitors most likely crawl through pages of hidden services retrieving user generated content from forums and posts (many hackers provide free samples in blogs as tasters, although usually aren't good). These public data dumps should be analysed and it is quite correct that companies are monitoring such sites for these details, but this is a very small area in the criminal aspect of the 'dark web'. 'Dark web' monitor advertisements give the perception that their technology facilitates them a light inside the 'dark web', to which they can gather all aspects of criminality and allow them to notify you. There is a large misuse of the word 'dark web', in these marketing videos as well, some describe the 'dark web' which will also include what many call the 'deep web', such as sites pages previously mentioned, Pastebin. Pastebin is a fantastic resource to which hacked information, samples of credit card information and doxing takes place, some of these posts on this site are unindexed. This is obviously a place to have identity monitors and business monitoring, but simply is not a part of the 'dark web'. The original Pastebin, although there are many variants, does not have an onion address (hidden service address). The customer of these 'dark web' monitors might have the impression that the product is searching constantly through the 'dark web' to find evidence of hacked information, but this simply is not true. There are many barriers to much of the 'dark web', a vast amount of the hidden services are complete nonsense. Many in the surveys of crawling through hidden services are either broken or non-responsive within a couple of days, meaning it is hard to fully grab a picture of what is within the 'dark web'. Joseph Cox wrote an article in early 2016 precisely on this subject of 'dark web' monitoring, to which he interviewed many staff members from these 'dark web' monitoring companies to try and understand what they actually did. The authenticity of the information collected in the 'dark web' is something that is touched upon in this article, to which the interviewee discusses how 'confidence levels' are used to try and distinguish how authentic this information is. This seems to be decided by the forum reputation of whoever posts. One striking quote from the article is "In some instances, we may communicate to our customers that we're observing something going on, so it's more of a 'be on the lookout' notification, that we may have a low confidence level in, because there just isn't enough information available" [103]. Automated crawlers most likely view the reputation of the user on forums and marketplaces, although this is an assumption, it can be dangerous in volatile markets such as AlphaBay, to which reputation can be built up by providing products for free which are basically useless.

Taking the assumption that crawlers and manual analysts in these companies use the internal reputation systems on these marketplaces and forums as a confidence level, this could be ripe for abuse. As described, one of the most popular dark marketplaces, AlphaBay can be manipulated by registering and selling free products which are mostly useless. There are active examples of users wishing to build a reputation currently on AlphaBay, one example given was a user 'selling' a defunct and now broken piece of malware called 'Blackshades'. Users registered on the site who have little to

no idea on such things but think it is worthy of their time give a user positive reputation and they can build the trust of many. Building these reputations can take time but can be worthy of money, especially in giving false ideas that a company has been hacked. Recently, researchers have correctly identified that reputation/rating is more important than price on these markets, and this could be a vector that law enforcement could exploit to disrupt 'dark markets' [134]. What is clear, is that reputation or ratings cannot be used as a marker for a registered user's value in a dark market in regards to understanding a marketplace. If you are simply purchasing drugs, this is probably important to you. This is what the research is touching upon, an intense amount of trust is needed in these markets between a buyer and a seller, if this can be undermined or exploited, markets may become stagnant. Users can register many accounts as TORs network makes it hard/impossible to differentiate between different people connecting, thus, allowing a network of fake users building reputations and giving each positive feedback. An example of how these systems can be abused is that a network of users are farmed for reputation on AlphaBay, to which they sell mostly digital products which are for the most part, low hanging fruit or unworthy of real money. For example, this individual who is developing this farmed network is being paid by an individual company to bring down the stock value of a competitor and learns they use monitoring systems for data breaches and credit card leaks. Once they have enough reputation on of the most popular dark marketplaces on the 'dark web' they must sacrifice one of the most reputable users they have to start selling fake information on the target company. The listing can even have purchases from the other farmed users to bring some legitimacy from it. The individual can then start simulating how hacked information is spread, by putting samples or discussions of hacked data into more throwaway public places such as Pastebin, Twitter and IRC channels (a way of instant messaging commonly used by hackers). The monitoring system may utilise both the 'dark web' and 'clearnet', with only a few available copies of information set for the data release either the company buys to see if it is authentic or hopes that the information is fake. This sort of simulation is certainly possible and these 'dark web' monitors can only go so far in understanding the 'dark web', because of these limitations these systems have, they can be abused for monetary gain in many areas. Confidence levels cannot expand any further than what information they currently have around the actual dark market, the reputation can be abused to a sufficient level that would raise confidence levels. Of course, this takes a lot of assumptions that the confidence level is simply taken on the users reputation of sources, but how else would confidence levels be built? Much of aliases used on the 'dark web' change often and make it hard to track, this is intentional, for illicit purposes. If the confidence levels utilise aliases and correlate them between different sources on the 'dark web', this could also be ripe for abuse as well. Because of how the 'dark web' is designed, where hidden services are not supposed to link, activity is supposed to be masqueraded and privacy is of upmost importance, systems such as 'dark web' monitoring give a murky outlook on the criminal underworld overall.

Even if the 'dark web' monitoring companies were exploiting anonymous networks such as the TOR network it would be unwise to do so. There is a lot of research on the use of exit relays (the last node on the connection chain in a TOR circuit) and the abuse that is possible by owning such a relay, TOR takes active measures in identify exit relays which modify responses to perform man-in-the-middle attacks. If a relay is seen trying to attack TOR network users by modifying responses, they will be eventually put out of exit node responsibilities, and largely become a middle relay. It would be problematic to exploit TOR through exit nodes even by passively sniffing responses due to them potentially sucking up information from government agencies, journalists and other users who are not criminals. Government credentials have been harvested before by passively sniffing as the owner of a number of exit nodes [104]. Although this was 2007 where encryption wasn't adopted as much, it is still

relevant today that you will be potentially storing data that you shouldn't be with users using protocols which don't utilise encryption. TOR software is installed on servers to which the maintenance is primarily down to the owner, certain flags are set when TOR checks whether the server is operational and is up to date. This means TOR cannot guarantee that the operator is not logging plaintext network transfers, as the server is not owned by them, simply their software is installed on it. Monitoring the servers for sniffing and other mischievous activities would not be taken well by most operators and contributors to the project, as this would be putting surveillance on operator's servers, which the TOR project is obviously staunchly against. TOR is obviously open source, so can be modified and rebuilt anyway. If an operator was to passively sniff TOR users as an exit node, it would be protocols like HTTP and FTP that they could capture, protocols such as HTTPS and SCP/SFTP would be unable to be sniffed because they use encryption. As I have previously stated, the TOR project is well aware of these activities and actually produces some legal advice for people who are thinking of potentially logging plaintext responses. The legal advice in conclusion says to consult a lawyer on logging on the TOR network, which to me is quite comical. The full statement reads "Tor relay operators in the United States can possibly create civil and even criminal liability for themselves under state or federal wiretap laws if they monitor, log, or disclose Tor users' communications, while non-U.S. operators may be subject to similar laws. Do not examine anyone's communications without first talking to a lawyer." [7]. This to me, is enough evidence that most if not all 'dark web' monitoring companies don't use exit relays to understand the 'dark web', in fear of legal repercussions. A large portion of relays are within Europe and the US which would more than likely have legal repercussions in pursuing such activities and the ones who aren't can be susceptible to interference by a state's censorship policies, such as Chinas, this has happened already in 2006 [105]. While TOR now holds exit relays to account by what is blocked, states may identify TOR traffic in such countries and manipulate it in other ways. In the 2006 example, it was simply because the internet was setup this way, it was not an intentional move from China to disrupt or manipulate the TOR network at that time, this does not mean in other countries TOR nodes are unidentifiable and could not be manipulated.

So without exploiting the TOR network or anonymous networks in some way, 'dark web' monitoring companies are limited to automated crawling and analysis of hidden services and manual analysis of hidden services conducted by analysts. Both have a very small looking glass into the 'dark web' as most of the traffic that is used within the TOR network goes outside the 'dark web' onto the 'clearnet'. Large portions of these onion sites are regularly inaccessible meaning they would have to trawl through indexing sites (which is not all of the hidden services on the dark web), bruteforce onion sites or utilise the TOR networks technical aspects and exploit them to identify all hidden services [106]. This means that much of the 'dark web' is probably undiscovered for a considerable amount of time and that much of the content on the 'dark web' is in places where 'dark web' monitors cannot go without purchase of mass data, essentially paying criminals. Forums on the 'dark web' usually have tiered levels of trust, which these 'dark web' monitors can infiltrate, however high they go, credit card information and account information is not distributed or shared unless purchased. Automated crawling also will make forums and marketplaces more suspicious, 24/7 scanning will lead to security challenges set to the automated system such as CAPTCHA which will further slow analysis, even if the system is able to circumvent or solve CAPTCHA challenges. Overall it is a bleak outlook for much of the 'dark web' monitoring companies, I don't see any viably legal way to have full access to all content and transactions that appear within the 'dark web'. If it were even possible, many states would be far less uneasy to anonymous networks like TOR than they are now. There are individuals who own hidden services who do not wish to have excessive crawling on their hidden services, and why would they

wish for such a thing? It uses so much bandwidth up! Crawling can also be used almost like a DoS (Denial of Service for many who may not know) in some cases if a server is not well resourced. There have been cases of individuals utilising how data is transferred to crawlers to either slow down or completely stop the crawler operation. Dr. Neal Krawetz is one such individual who decided to stop or slow down what seemed to be crawlers [107] by using 'zip bombs', which later eventually exhausted most crawlers memory resources. His work shows that crawlers can be targeted to be removed or actively exploited in the 'dark web', although this is possible on the 'clearnet' as well, crawlers are usually unaware of being identified because of how the 'dark web' is designed. The combination of active attacks such as zip bombs, CAPTCHAs for reauthentication and response manipulation keeps me highly cynical of how high quality the information 'dark web' monitors can possess. Although, it must be noted, not all 'dark web' hidden services operators are as vigilant as Dr. Neal Krawetz, some cannot configure their servers correctly to keep the server location anonymous. Overall, it is much more challenging than some way think, simply crawling the 'dark web' can lead us to results which give us little to nothing in regards to 'intelligence'.

My personal opinions of 'dark web' monitoring is it must be hot air (excuse the idiom). There is no feasible way to correctly analyse all parts of the 'dark web', individual leaks of information, such as an individual's credit card information which are closed off usually using general terms for the hack. They do not give huge amounts of data away because it is most likely worthy of monetary value of some sort. Public dumps of information by hackers are usually motivated by politics, corporate competition or worthlessness of data. It is illogical to post data that you have just gained into even private forums, because dependent on the target, it will probably be worth something to someone. The amount of hidden services is relatively small compared to much of the internet, as previously discussed, although the 'dark web' has previously had breaches surfaced first on it, many have simply posted on 'clearnet' sites. So while gathering *intelligence* from 'dark web' hidden services is good practice, it may be more fruitful in concentrating on assigning considerable resources for identifying information leaks on the 'clearnet' too. With only a small number of hidden services entered on any given day (certainly under 100,000), the TOR network is misidentified as the biggest threat to many companies, especially in finance. The idea that the 'dark web' is mysterious has led many to be able to market services which 'monitor' this network, whether these services actually do so is another thing. There are many technical challenges a company would have over fully monitoring the TOR network, otherwise many of the private communities within it, would not use it. The public facing side of the 'dark web' to which automated programs can vacuum information is available to these companies, be this authenticated forum users or sites which require no authentication for information retrieval. The TOR networks hidden services do still have forums with private messaging features, private sub-forums and services which sell information individually not on a wholesale basis, although some sellers do sell wholesale (not very good quality is perhaps why). And therefore even vacuuming vast information from public facing forums/markets/communities will not provide a detailed picture of the 'dark web' activities. Caution should be given to 'dark web' monitoring services, for what they can provide is something far less than what they are marketing. It is impossible to fully scour all areas of the 'dark web', it is a very different animal to the 'clearnet'.

CHAPTER 7

IS FULL ANONYMITY REAL?

Many security professionals state that there can never be a system which is unhackable, there will always be flaws because we are human (even if we do incorporate AI or other technologies into security). A system can only go so far in being secure, it then relies on the time it takes and how hard it is to break down. One of the fundamental pieces of security in the modern world is Cryptography. Cryptography is a good example of how long it takes for someone to be able to 'hack' you in theory, although it would take a patience of a saint, even for big powerful organisations around the world. Many who read this may understand cryptography and argue how quantum computing could potentially endanger our security, but for now, powerful organisations around the world, be it a company or state do not have computer resources like quantum computing. Cryptography has many different moving parts, but I am going to keep to one test case that I think resonates well with the time it takes to 'hack' someone. Bruteforcing all possible options to recover the information that has been encrypted is the last tool in someone's arsenal when attempting to recover or find ways to recover future encrypted communications. It essentially tries every single possibility there is in 'recovery' in which eventually it will buckle. This sounds dangerous and worrying, but it isn't, it takes considerable computing power to do this and even then takes a substantial amount of time. With the modern algorithms it would take longer than our lifetime in theory to crack keys conventionally (I am referring to the AES algorithm here), if information is harder to recover than other ways, attackers will naturally move to other areas which are more worthy of their time. This property of how long it takes and how worthy of an attackers time it is, is something I note when looking at the subject of anonymity, especially full anonymity. I don't think full anonymity is real, the only real way of having full digital anonymity is not owning a computer and to not have it connected to the internet. Essentially, not having a digital identity.

Anonymity is slightly different to my example where it takes too long for even a powerful organisation to recover encrypted communications. If you wait long enough you will deanonymise the individual in question, even within networks designed for anonymity, like TOR. Ultimately the responsibility has to lie with the individual and the actions that they make and of course after all we are all human, we make mistakes. Recently it was discovered that a large portion of hidden services on the TOR network actually reached out to 'clearnet' services to grab images, libraries and other dynamic content that a site may need. This can deanonymise an individual in theory, but is slightly misleading, the New Scientist article states "More than 20 per cent of the 1.5 million dark web pages they analysed imported resources like pictures, documents and Javascript files from surface websites" [108]. This statement makes the vector that they analysed seem like the majority of the 'dark web' but can be simply just crawling through different pages of large hidden services. It is quite apparent that a lot of hidden

services available on the ‘dark web’ do contact outside services like image/content storage services and trackers that allow operators to see analytics. This can be largely put down to two things; the incompetence of a hidden services operator, where they simply copy templates from other sites and do not remove tracking code from the previous author. It can also be down to the fact that many do wish to know what type of activities different users do on their site, which again, isn’t a smart move either. The authors of these hidden services who have decided to have outside resources like images and tracking code on their site must have little understanding of how anonymous networks actually work or simply do not care too much about visitor’s identities, which is hard to believe. The former seems the most likely, a large portion of hidden services are projects that are hobbies or services which run through the ‘dark web’ and ‘clearnet’. Most people don’t really fully understand the power of Google Analytics or the power someone has in being able to identify you through characteristics and behaviour. I first came across Google Analytics when I was fairly young, first starting to develop websites in a web programming language. I decided to append Google Analytics to a web proxy, I had heavily modified a popular script that would allow people to retrieve internet resources through my server while still in a browser. Not needing to modify and operating system configuration, it’s easy, but not very secure. Seriously, don’t ever use a web proxy. At the age of 17, I didn’t fully understand the issues that could arise from being able to track people who wanted to essentially hide their IP from internet resources. Around this time, it wasn’t common knowledge that these types of IP cloaking services were unsafe and anonymous networks weren’t as prevalent. Google Analytics allows you to track what pages your visitors are going to, the script I developed showed the website resource they were visiting in the URL, thus allowing me to understand what they were looking at (For the technical people reading, I hadn’t learnt fully what a man-in-the-middle attack was but yes, I could of done a lot worse). Google Analytics allowed me to see unique visitors visit different pages, see them change the page in seconds using what was called Live View from what I could remember, of course, a lot of this traffic was people viewing porn from conservative Asian counties. It was a 128MB memory server with around 5TB of bandwidth, a low memory high bandwidth server that soon had to be upgraded again and again, I was overloaded with visitors and my bandwidth was sharply rising. I later closed the project, I was young and unable to invest enough financially to steady the surplus of traffic. The majority of the traffic though was from one country that at the time I was perplexed by, I simply built this website out of curiosity, and advertised it to understand how to maintain a high traffic based web server on low resources. Google Analytics was fascinating to me, I thought I could understand why people flocked to these proxy websites by trends and Analytics, but the majority of traffic were coming from Iran and at that time I had no idea why, in fact, I didn’t even know Iran existed until then. I looked at the analytics to try and understand why there were so many Iranians that were on my proxy website and found a startling trend, while there were a lot of different countries which overwhelming viewed porn. Iran viewers were primarily viewing one site, Facebook. A few years later after remembering the project it finally clicked, Facebook is censored in Iran as many other popular western websites are. Iranians were utilising my service to evade censorship from state filters [137]. The power I had of controlling these viewers was high, these behaviours could be brought into patterns to identify users if I didn’t have their IP addresses, which is something you don’t have on TOR. Google Analytics could possibly decloak users through behaviours, but not to the level of a web proxy could. It seemed to these individuals that utilising my service would help them remain anonymous, but could actually endanger themselves through it, not only could the service be run by Iran state operatives, but the actual script was technically not safe to use in an anonymous context. This case to me really highlights the power of Google Analytics and the gap between common knowledge and expert knowledge, where users were

utilising services that were basically unsafe for their identity, although they felt they were anonymous. This false sense of anonymity is something I take note of, it shows much work is to be done, for people to fully understand the intricacies of anonymity and how important it is.

One site that uses all its own resources to provide images and dynamic content is AlphaBay, AlphaBay has no outside connections and simply connects to its own onion domain. AlphaBay goes one step further by advising all users to enable 'NoScript' by default to be safer. This is one problem that the New Scientist article has with the possibility of deanonymisation by using trackers like Google's analytics service. Criminals who take anonymity seriously will have 'NoScript' enabled, all new installations of the TOR browser have 'NoScript' installed and enabled by default. 'NoScript' essentially removes any possibility of dynamic content, static HTML and CSS can pass through, but Javascript is not allowed, hence the name 'NoScript'. Even if a user of the 'dark web' was to visit a page with a tracker on, it does not mean they can be tracked, as stated the majority of the pages uses Google's analytics tracker, which, is coded in Javascript. The real question is how many TOR users have 'NoScript' disabled, this answer will allow us to understand how serious most TOR users are on operational security. A large majority of users browsing the 'dark web' also view content on the 'clearnet' through TOR, this is evident through TORs internal metrics, so it is possible that a vast majority of users using TORs browser have 'NoScript' disabled, otherwise websites become broken/unviewable. There is an indicator from hidden service operators errors of judgement by using outside 'clearnet' resources that there is room for complacency by anonymous network users, but anonymous networks do not simply aid criminals, as many must know now. A subset of anonymous networks userbase are criminals, whether the large majority of them have 'NoScript' enabled is another matter.

We cannot assume that criminal professionals do not disable 'NoScript', in 2013, one element of the PlayPen case, which has been previously mentioned is that malware was used to find other individuals who view the site. As investigators were able to get hold of the server, they could append additional code that exploited individual's browsers to identify the user. The 'Tor Browser Bundle' is the user friendly way of entering onto the anonymous network TOR, utilising Mozilla's Firefox browser to offer anonymous network web browsing. The TOR Browser Bundle can be seen as almost a hardened version of Firefox, with 'NoScript' and 'HTTPS Everywhere' extensions installed by default. TOR also provides minor alterations to help the user with privacy, for example, if the TOR browser is maximised, a toolbar is shown stating to the user that this is dangerous, as leaving a window maximised allows you be tracked by understanding screen size. The majority of the TOR network users who browse the web, do not route traffic through their normal browser (this would be a bad idea), they usually spawn a TOR browser bundle process (although it is possible to route traffic from your browser to TOR). Javascript code was used in 2013, to be able to identify individuals who used Playpen, by exploiting a flaw in the Firefox browsers code. This allowed someone with this exploit to remotely execute computer commands from someone simply visiting a website, in this case the PlayPen hidden service. If 'NoScript' was used by PlayPen users they may have escaped justice, I have not been able to analyse the forum and so assume that the forum used Javascript in some manner, all popular forum products utilise Javascript in some way or another and is how exploits are devised. Essentially, PlayPen users in 2013 visited the onion hidden service, which was then being controlled by the FBI who took control of responses made to these users. Javascript code appended by the FBI would allow code to operate not only from the web browsers control, but outside of that context to the computer. When outside of the browser context, a user may be identified, dependent on the networking configuration, the code or

more precisely put, malware sent a standard HTTP request and another request (ARP protocol for the nerdy) to identify another usually unique portion of a user's identity, called a MAC Address [109]. Although many of these things can be spoofed, masked or manipulated in some manner, many do not practice these techniques often and usually rely on the TOR browser for the safety of their identity. This led to many arrests of individuals using the horrendous hidden service 'PlayPen', it also led to controversy that the FBI had such power and was remotely installing malware on individual computers through TOR. In total, 870 were arrested in this case in which it seems the malware was able to identify individuals correctly and there was enough evidence. Many do question its ability with only 870 users arrested, from a reported 150,000 userbase. Many must take into consideration that many individuals may have set the 'NoScript' extension on, or rather left it on. We must also understand that many individuals who have knowledge in technology could also be under other layers of security, such as a VPN. This makes it of course much harder for them to be tracked, as the TOR network is not the only protection an individual could use to keep themselves safe. There are many other questions that I will never have answered such as was there only one operating system targeted? From the small amounts of evidence online, it seems so. There may not be that many active users on the website too, I discuss this briefly previously on how researchers, law enforcement and hackers may have bumped these figures up in attacks against the community. It is by no means a poor effort from law enforcement, it is reported that not only did 870 individuals get arrested but 'at least 259 sexually abused children have been identified or rescued from abusers outside the US' which many will see as worth it [110]. In 2017, Hansa Market, a dark market selling drugs was seized by law enforcement. Similar to PlayPen, law enforcement was running the hidden service for a short time to identify individuals, in this case, drug vendors. Law enforcement did not have an exploit that the PlayPen case did, instead, individuals were tracked in far less technical way. Downloading files and executing them leaves the potential of being identified, Playpen users had an exploit that forced this, but users can voluntarily do this as well. In the Hansa market, vendors of the market had a feature of downloading a summary of transactions according to Joseph Cox, a well-respected journalist who covers hackers [135]. A change happened just before the seizure notice of Hansa, this feature changed to downloading an xls file, or as many know it an Excel spreadsheet. The Microsoft Office suite file formats are fairly easy to understand, they are encapsulated in a popular archive format which is identifiable (ZIP), which allows analysis of documents to be trivial. This file format was standardised and is used by most office processing formats. A user decided to analyse this new feature that was available in Hansa, most likely out of suspicion that the file could contain malicious macros. The identification of a user was far less obvious than this, the file instead had a link to an image which would be presented in the office document. This required an internet connection to respond to a server within the context of the office program. The image URL was an IP with a unique identifier to a non-standard web port [136]. It would allow law enforcement to identify users if they did not route all traffic through TOR or a VPN. This of course required considerable work on the users part, to trust Hansa, download the file and execute it in the correct manner. It is unclear how successful this technique was, but showed some form of creativity by law enforcement. One user on Reddit repeatedly posted on multiple subforums warning users of this image that they labelled a 'beacon image' but seemed to never fully grab enough attention from many users on these forums.

The 'dark web' is seen as impenetrable, a network which masks its users to where it is impossible to uncloak them. This is simply not the case, while it is correct that it is difficult, it is by no means impossible to identify individuals as shown by the PlayPen and Hansa case. Flaws in code wrote by humans can be identified and exploited to give access to machines, to which law enforcement in this

case wished to identify individuals. You can probably see why many privacy activists, journalists and citizens around the world may be unsettled by this ability that law enforcement have. TOR is seen as one of the best solutions for anonymous networking that we currently have, although note I said one of, because it can be put in combination with other solutions to better ones position. This highly rated anonymous networking software is exceptional but like much of technology, it will never be perfect. The ability to target individuals that are on TOR can be exceptionally targeted, the TOR browser can be identified not only by exit node IP addresses, but also the TOR general version. Identifying TOR browser version can help in exploits that may be already around for earlier software, although TOR is quite militant on its update system, it is still possible for users to have old versions of TOR in more restricted areas of the world. By Firefox design, in which the TOR Browser Bundle is built on, there are ways of retrieving resources that allow adversaries to fingerprint and understand what version TOR is [111]. This is not reliant on a user agent, to which can be manipulated and modified quite easily, this is part of the internals of the browser. The current issue is deemed as Firefox's issue and has been left unpatched, as of writing it is still able to identify the TOR browser to a reasonable amount of accuracy. My definition of reasonable accuracy is major version number, which is currently 7. Moving further there is even research on basic Javascript functions that could potentially identify a TOR user [112], while quite minimal in actual results, advertisers use similar techniques to understand the system of a user to fingerprint individual users correctly. TOR cannot defend a user who wishes to enable Javascript, the organisation disables this ability by default and it is down to the users choice. Nevertheless, behavioural analysis of users on TOR, if access to a popular hidden service like PlayPen could be dangerous which is why TOR advises users to keep the browser window minimised, to ensure fingerprints are less accurate. I think fingerprinting users through behavioural analysis is much like biometric authentication, it comes down to the tolerance rate of the system and will never fully identify a pattern the same as before, while much in-depth research needs to be done in this subject, these are my early assumptions of behavioural analysis simply through browser fingerprinting. It does provide an example of how seemingly fragile a user can sometimes be in the TOR network, anonymous networks can only go so far in the protection of its users before it becomes the users responsibility to protect themselves. Let's take a case where even if all protections were in place in the TOR Browser bundle, the individual was still able to be caught due to time analysis and understanding how users connect to the TOR network. It seemed in the Harvard University bomb threat case, the user had a reasonable understanding of operational security, by using the Guerrilla disposable email service. In 2013, a bomb threat was made where an email was sent to Harvard administrators through a service called 'Guerrilla Mail'. These types of services aim to get rid of spam by giving a disposable email address that a user will never use to registration forms that users don't fully trust. Guerrilla is slightly unique in the fact it also allows users to send emails to anyone through its service. The user who sent the bomb threat was evidently aware of basic networking and decided to utilise the TOR network while accessing 'Guerrilla Mail'. The service appends the originating IP in the email as well, to avoid abuse such as this. The originating IP in this case would be a TOR exit node, as the user was accessing the site through TOR and the last node in the chain would be communicating with the 'clearnet' service. When analysing the email, the FBI and Harvard administrators would be able to understand whoever decided to send this email were going through the TOR network. This would seem like a dead end, but in fact, it wasn't. The individual responsible for the threat was logged into the university network and was the only one connected to TOR on the network [113], if packets are captured and stored, it is quite clear when someone is connecting to the TOR network if certain configurations aren't set. As this is a university network environment it is certainly likely that packets were stored for later analysis if any abuse like this

was made. Because there were no other users who were using the TOR network during this time, one single individual would be singled out on a university network. Many operational security mistakes were made here, most notably, logging into the universities network to carry out this bomb threat. It's a famous case amongst many people who follow anonymous networks, it shows how outside of TOR is as important as using anonymous networks, how you initially connect to the service and how you conduct yourself while interacting through anonymous networks like TOR.

Traffic analysis is another problem that the TOR network faces, as the internet becomes more popular around the world, more eyes are watching for what they may deem as suspicious activity. If a powerful state is able to see the majority of communications of a user, be it encrypted or not, the TOR network is useless. Onion routing is the process of how TOR routes traffic, this first must go through conventional communication before entering the TOR network. After entering the TOR network it will either exit the network or communicate to a hidden service by means of rendezvous point, not directly communicating to a hidden service within the network. Inside the TOR network there are 'relays' which are operated by volunteers, these relays might seem like they are run by individuals but maybe they're not. Traffic analysis assumes a lot of things, one being that many ISP's simply accept state requests for real-time information on someone and another being that countries cooperate together to identify what they may deem as dangerous individuals. While there are hints of this, I don't think there is vast amounts of cooperation to where there is a, how TOR describe, a 'global passive adversary' [114]. This is a matter of opinion and readers can decide for themselves whether this threat to anonymous networks is viable at their current time. Traffic analysis is quite politicised after various leaks and articles appearing online in recent years, the increasingly worried public on the information of mass surveillance has led to vast coverage of the subject, yet we still have no real answer to a decent system of intelligence and perfect liberty. Traffic analysis to a scale of being a global passive adversary would have huge ramifications for not only citizens of these global passive adversary states but around the world as well. Although a lot of countries in developed worlds have discussed the issues in length, nothing really has come out of it. This is a concern I have, that politicians are unable to understand issues in any great depth, due to poor advisory. Leaving issues to manifest until politicians react with misfiring, ill-judged policies which do not resolve the complex problems we face in the future, leaving the issue to further become more complex. Surveillance is a subject that is long, complex and beyond the overall scope of this book, I think for this book it would be best to leave the overall subject of surveillance.

In 2004, one of the core developers for TOR gave a talk at a conference called 'HOPE' [115]. In this talk Nick Mathewson describes the possible ways to break anonymous networks and how it may be possible to defend against some of them. From this talk there were many points on traffic analysis, which is still a seemingly viable attack method today. He talks about long term statistical methods in certain anonymous networks which can deanonymise someone. While some of the attacks are defunct, many are not, this talk from over 10 years ago makes it clear to me that anonymous networks face similar problems today. Some problems do not die, but remain, stagnant for years. Anonymous networks are not easy to design and there is always going to be traffic analysis as that one flaw, simply because of how networks are designed. Traffic analysis, software flaws and the user being identified by their own actions are three main issues that are highlighted for me. Many of this seems unfixable, how can we change the behaviour of the user to ensure everyone looks completely the same? In the talk, Nick Mathewson describes how examining individuals writing style can give indications of an identity. The behaviours that an individual has is what identifies them, we cannot supress behaviours from a user of an anonymous network, although this is most likely the least accurate way of deanonymising an

individual, it is still theoretically possible. TOR has done its best in removing some fingerprints of a user, such as the reminder of minimizing your window out of full screen context, but writing is something that TOR should not interfere with. Traffic analysis has been proven to work against TOR, not to identify individuals but to actually block access to the network itself. Traffic analysis is a very generalised term, it literally means analysing network traffic for a certain goal. When TOR developers talk about a global passive adversary, it is someone who is silently analysing traffic from nearly all points of network communication, thus, allowing someone to be identified easily. Traffic analysis can also refer to identifying certain characteristics of traffic to block, which China have previously done. In 2011 China added capabilities to the 'Great Firewall of China' to be able to identify TOR bridges, which are unpublished to ensure they can be used by individuals which wish to circumvent censorship [116]. When a specific request (SSL/TLS Client Hello for the nerds) was sent to a TOR bridge, China could somehow identify it as 'TOR like', Chinese IP addresses began to probe the specific IP with TOR requests to try and identify it as a bridge to fully verify it's intentions, to which later if correctly verified it would be blocked [117]. These Chinese IP's would act like clients trying to connect to the anonymous network, to which the bridges would reply to tell them they were bridges (they could only oblige to what they thought were genuine clients). The interesting aspect from China blocking these bridges is it was seemingly done dynamically through a system identifying traffic inside China, little to no human intervention was needed. The Chinese government had employed deep-packet-inspection (DPI) boxes which were able to identify the initiation of TOR clients connections, this is what many would fear for an anonymous service. As it is completely possible from being able to verify these TOR bridges, they were able to identify IP addresses within China who wished to connect to the service. TOR developers later created some new ways of accessing TOR through countries like China, if you're interested they are named obfs4 and Meek.

Looking at technologies such as PGP, it is clear that usability is ultimately what motivates the mass population of the internet to implement security technology in their daily lives, if something is not easy to use, even with the best security, users will not use the technology. Anonymous networks, like many other security products, must compromise security with usability to make sure users are at least somewhat protected. An ideal anonymous network is possible, but it would most likely be too fiddly and would not provide varied content on demand, it would delay communications to further mix connections and pad communication packets. This type of ideal communication is possible, but as noted by Nick Mathewson in 2004, it is not economical as well as not being good for the user. The expectation of anonymous networks, especially TOR, is to receive the information requested as soon as possible. There are many individuals who find TOR slow now, to where the project has certainly compromised security to some level for usability. This does not mean the TOR network is easily 'broken' as so many on the internet postulate, the network is simply ensuring added security is available to all around the world. The ideal for anonymous networks that I envisage, is much like the property of cryptographic algorithms, how long does it take to break and see the plain text? In an anonymous network context, how long does it take for a powerful/global adversary to identify a user through statistical traffic analysis? The ideal anonymous network design would be that it takes longer than attacking a user's behaviour on the services requested by them. TOR works better when there are large amounts of relays which are diverse and maintained by various owners (this can never be fully verified). When there is relay diversity, where no organisation can be the majority in relay population is where this may be possible. There is no real vetting on relays as this would be against the idea of the TOR network, instead the directory authorities, a small number of independent servers are in charge of keeping the many millions safe on the network by trusting certain relays compared to others.

With so many different aspects to anonymous networks, it is nearly impossible to believe there is a perfect anonymous network system. I am very cynical to the idea that we can gain full anonymity, where no organisation will be able to identify us simply by how we behave online. We do not currently adhere to an exact standard when communicating and we certainly do not wait hours for messages to come back to us, could you imagine Netflix? It's quite clear why anonymous networks were designed to prevent eavesdroppers to understand our everyday activities, even with encrypted communications technologies like SSL/TLS, anonymous networks have a place in the world. Recently researchers were able to identify encrypted video streams from Netflix, Netflix nobly moved all video streams from non-encrypted to encrypted so eavesdroppers could not identify what users were watching. Traffic analysis aided researchers in being able to still identify what users would be watching, even with encryption, which shows the power of traffic analysis outside of TOR [118]. The problem is that even through TOR traffic analysis is still possible, just harder, traffic analysis as previously stated should be forced to gather masses of data, to where it takes far more time than it would to identify a user through their online behaviours viewable from a service (hidden or Clearnet). Traffic analysis, relies on statistics to identify a user in some way, it is arguable that this would not bring an individual's identity beyond reasonable doubt. Even through the Netflix traffic analysis, there was a 0.5% that was misidentified, although a fairly high success rate, traffic analysis may only be seen as supporting evidence to identify someone. What is clear once again is that politics is important in the future of the internet, to prevent a dystopian future for the internet overall, politicians must rethink how to approach the security of a nation and the security of the internet. Identities can be seen to be masked on the internet and certainly on anonymous networks, but the simple fact of it is they are not. Identities are valuable products on the digital world, everyone has a face; shopping habits, online behaviours and personalities. While some of these attributes can change in our identity, overall we only have one identity, we are who are. These identities have now been on the internet for many years and issues are arising from this, as more and more websites get hacked where databases are leaked we must face the monumental task of attempting to regain some forms of privacy for individuals. Anonymous networks provide innovations and ideas to keep identities safe, to which they should be noted, but I do not believe it is the final solution, especially TOR. Many anonymous networks are relentlessly searching for a system to which an individual has complete freedom, they feel so comfortable in complete anonymity that they can express themselves fully. Currently anonymous networks and law enforcement are under an equilibrium (sort of, anyway), individuals are caught who are utilising the network for abhorrent acts but far more resources are required for them to be caught by law enforcement. If one of the two outweighs one it will become dangerous, either anonymous networks lose the ability for individuals to become anonymous or terrorists and paedophiles are able to roam freely. It is fairly common knowledge that in the world, there is no perfect system, at least, made by humans.

CHAPTER 8

THE DARK MARKET LOOP

The rise and fall of ‘dark’ marketplaces on anonymous networks are a regular thing, in earlier chapters I discussed the volatility of not only marketplaces but hidden services overall within anonymous networks. ‘Dark’ markets are very much a prominent part of the ‘dark web’, especially markets which sell drugs. The drug market on the ‘dark web’ is huge, which is why they can be so competitive, you can earn large amounts of money by owning such a marketplace. The popularity of these markets are evident on the ‘clearnet’, with various places advertising how to access the ‘dark web’ and how to actually buy drugs on ‘darknet markets’. In fact, one YouTube video alone which was published in March 2017 on how to access and purchase darknet markets has 180,000+ views, that’s around 3 months of views. The popularity of these markets have led to law enforcement and scammer interest, but the markets keep springing up which leads me to compare ‘darknet markets’ loosely to the way piracy is treated online.

The Pirate Bay, FirstRowSports and 1Channel are all instances of piracy sites which large corporations and bodies have attempted to block. The censorship techniques have been made through courts where internet service providers (in regards to the UK) have been ordered to block particular sites [124]. This rudimentary technique is fairly easy to bypass, we see proxies and alternatives crop up all the time on the internet because the demand is there. On 31st of May 2006, Swedish police raided the datacentre that the infamous ‘The Pirate Bay’ was hosted at, temporarily shutting down the operation of the site much like shutting down a site due to malware or a hidden service like AlphaBay or Hansa. This made the site go offline in a total of just 3 days. What’s evident in this case is that technology can withstand raids from police and move to other locations around the world with ease. Technology is far more dynamic than laws or law enforcement themselves, with a savvy group of technologists, bypassing censorship can be trivial. As Torrent Freak note 11 years on from the raid, the raid actually provided The Pirate Bay with more visitors and more press attention than it could ever hope for, it allowed ‘The Pirate Bay’ to become a big name in piracy [125]. Much like potential ‘dark markets’ which receive press attention now, many may not of heard of names like ‘Silk Road’, ‘AlphaBay’ and ‘Hansa’ but variations of these names on the ‘dark web’ may become popular due to the extensive media coverage that entails after raids, seizures and other events. ‘The Pirate Bay’ has been able to keep servers online while the dark markets have been shut down for good, but, much like ‘The Pirate Bay’, the dark markets community are very resilient and soon offshoots and different variants appear from the shutdown sites. If there is money available, someone will surely create an alternative. In 2013, the original Silk Road dark market was shut down, leaving a huge vacuum of customers and vendors. It only took a month for a viable alternative to appear, Silk Road 2.0. This constant cycle of dark markets

rising and falling leaves a permanent community that are hard to police, many would see the shutting down of dark markets as a good thing, but from experience it can lead to worse outcomes. There has been now Silk Road 3.0, Silk Road Reloaded and Silk Street since Silk Road 2.0 among other obvious familiar named variants. Reviewing the dark market community, harsh security measures are becoming the norm in most vendors activities. Most markets will require public keys for PGP communication, overall web application security is strengthened from past mistakes and purchasers learn further how to remain safe while purchasing dark market items. Of course, there are many markets which fall out of this trend, these are commonly fly-by-night operations or exit scams. There were no less than 7 other markets that were active after the original Silk Road was shut down before Silk Road 2.0 appeared, all of these markets ceased operations before Silk Road 2.0 was raided. When the markets are in flux it seems as if no other alternatives will appear, but as we can learn from the dark markets timeline an alternative will finally appear. There is far too much money to be made in these markets for a viable alternative not to appear. The owner of the now raided 'AlphaBay' listed his assets and came to the conclusion he was worth $23 million US dollars [126], this sort of money can bring all types of groups to try and produce a safe and secure dark marketplace. The symmetry between how much money can be made between piracy and dark net markets are quite startling, although, the revenue for most pirate sites are indeed ad revenue not direct sales. The revenue shows that if money is to be made, it will be resistant to law enforcement in some manner. Either someone starts a fresh different alternative or the owners are able to carry on operations in some way. The Digital Citizens Alliance produced a report 'Good Money Gone Bad' in 2014 showing the top 30 pirate sites on average receive $4.4 million in ad revenue, the report goes further to add that 'even smaller sites can make more than $100,000 a year' [127]. The incentive to start a new dark market is obvious, money that can be raised from the operations of markets can be vast, especially if another market has fallen, been raided or is inaccessible at the time. Analysing where the market was when the original Silk Road was around from now, it is clear that the market has increased significantly. Many would attribute this to media coverage on 'dark markets' and the increase of 'dark web' content on the 'clearnet'. When the original Silk Road market was raided in 2013, another market was online at this time called 'Black Market Reloaded'. This site later had its database leaked which provided important insight into the inner operations of a dark market, especially after another marketplace had fallen. 'Zaufana Trzecia Strona' analysed the database to find anomalies in user registration, the anomalies being significant increases in registration, either in line with Silk Road being inaccessible or later, the raid of the Silk Road which brought huge numbers as it was clear, it was not returning [128].

Law enforcement may have taken notice to the very fact that people flocked to other markets when the primary choice became unavailable when the original Silk Road was brought down. In 2017, AlphaBay became unavailable to access, one of the largest dark markets to ever surface the 'dark web', far larger it can be noted, than Silk Road. During my time writing this book I was regularly accessing AlphaBay to view listings and critique the largest dark market on what people call the 'dark web'. Rumours began to spread across 'clearnet' dark market communities that AlphaBay had become an exit scam, essentially running away with all the users' bitcoins. People began to choose the secondary choice of dark market, suggestions were made and most people chose the increasingly popular Hansa. Hansa had a different way of business, it used multiple signature escrow, essentially making payments much safer than many other markets available at the time. New features made Hansa stand out in the marketplace, it allowed it to become a second option almost by default by many after AlphaBay had been brought down. What many did not know after AlphaBays long time off, is that Hansa was also in the hand of authorities, the authorities had taken over Hansa and was gathering intelligence from new

registrations. Alexander Cazes, the owner of AlphaBay was in the news in July, he had been arrested in Thailand and later been found dead. He had reportedly hung himself in his cell. At this time I had been researching and writing about anonymous networks and dark markets for well over 2 months, I had committed myself to this project and was taken aback by the sudden state of flux that the market was in. I woke up one morning, about to start writing and decided to do what I do most days when writing this book, I look at potential updates in the market. Everywhere I looked there was just one story that I saw that morning, the capture and apparent suicide of Alexander Cazes, the owner of the notorious dark web drug marketplace, Alpha Bay. I was not researching or writing this book when Ross Ulrbicht, the owner of Silk Road was captured, I was aware of it though, as I have always had interest in anonymous networks. The death of Alexander Cazes was something very different, it felt like it was out of a blockbuster film. Many members of the 'dark web' community decided to pay tribute to Alexander Cazes by posting comments on the news on popular 'clearnet' forums, mostly commenting things like "RIP Alex". Many owners of 'dark markets' who are captured by authorities are treated as martyrs, seeing 'dark markets' as the cause to fight against the war on drugs. There are vast differences between many owners of 'dark markets'. For example, Ross Ulbricht had very strong views in the economic side of 'dark markets', many forum posts on his site had philosophical elements to them and he lived a fairly humble life. He shared a 3 bedroom house in San Francisco with basically strangers, using the site craiglist to find a place to live. In comparison, the Alpha Bay owner, Alexander, seemed to relish the lavish lifestyle that 'dark markets' could provide him. There are pictures with him standing next to a Lamborghini and he owned reportedly 4 properties in different countries. Different personalities can certainly withstand the strain that can come to someone owning a secret market which handles millions of dollars per year, but seemingly, there is no perfect type. Alexander Cazes had a far shadier past than Ross Ulbricht, well known to many who partake in carding activities, which I loosely define as 'fraudulent activities for gain'. His handle is known in various carding communities which allowed him to gather contacts for structures and experience in keeping a low profile, although similar mistakes to Ross Ulbricht were made. In fact, Alexander who in the criminal complaint has the handle "alpha02" attributed to him, if true, created an extensive guide to the art of carding. Distributed in some marketplaces and around the 'clearnet' a carding guide developed by 'alpha02' which is 16 pages long is available. In the introduction the author states "I'm an experienced carder, carding tens of thousands of dollars worth of merchandise and rarely failing", it is clear that if alpha02 was Alexander Cazes, he was perfectly positioned to run a 'dark market'. Ross did not seem to have any other criminal activities previously from running the 'dark web' market, Silk Road and so was more active in advertising and building up contacts. Building up trust is one of the most important things not only in the criminal underworld, but in the 'dark web' overall. These 'martyrs' are very different, have very different goals, but are always remembered for one core issue that has been around for some time, the war on drugs.

Once the confirmation was made that AlphaBay was no more, Hansa was later also struck offline and then later presented a seized notice from various crime fighting organisations around the world. This seemed like a big hit from the authorities, they had not only taken the largest dark market that had ever been on the 'dark web'. But had also gathered decent intelligence from another market 'Hansa'. The problem as I've said, is the fact that AlphaBay outgrew Silk Road into a huge marketplace. AlphaBay reportedly had 20 times more product listings than Silk Road did and was online for around the same time, the demand for online dark market products is increasing fast. When AlphaBay went offline, new registrants made other markets, not only Hansa, have issues. Dream Marketplace, which is now the oldest out of the well-known dark markets, went offline due to the demand (it came back up).

Researchers at Swansea University noted that Silk Road 2.0 had growth that was unparalleled in any others parts of the market, probably due to the use of the brand 'Silk Road'. Familiarity to a brand may have played a part in such growth, but the requirement after Silk Roads departure, leaving such vacuum, in my analysis is something that threw Silk Road 2.0 as the main dark market at that time. This point of markets falling giving others fame is something that the Swansea researchers noted too, confirming after the original Silk Road was seized, 2.0 had considerable growth [133].

The policies that governments have for the 'dark web' are minimal, seen as it is hard for many politicians to understand cryptography fundamentals or the internet overall, it is clear why the 'dark web' has been mislabelled or confusingly associated with other problems in the world. It is true, the 'dark web' or rather, anonymous networks harbour some horrific material, but is evident that the internet overall is the far worse abuser. It is also simply a network, attempts to identify criminals in other more creative ways are successful, both Ross Ulbricht and Alexander Cazes were primarily identified through what many call 'operational security' failures. Ross Ulbricht initially advertised Silk Road like many on the 'clearnet' in which he participated on forums to try and drum up business through the TOR network, forums like Bitcoin Talk. By reviewing the official criminal complaint made against him, he also used the same account to advertise work in the BitcoinTalk forum, which used his what seemed to be his personal email address (It included his name in it). The criminal complaint goes further to discuss links between his identities on stackoverflow where he asked for help in requesting information on a hidden service utilising the PHP programming language [129]. Some of these mistakes could be avoided by Ross Ulbricht, but no one is ever perfect, humans make mistakes and was caught not only from operational security failures, but also he was unable to distance his identity from Silk Road sufficiently, which provides solid evidence against him. The Grugq, who is regarded as an expert in operational security by many (I hate to use the word expert, but seriously, this guy is almost a machine when it comes down to the intricacies of operational security) analysed Ross Ulbricht's case, identifying the glaring issues that faced him in this high profile case. One big highlight that is quite obvious is the issue of compartmentalisation, as previously mentioned, he was unable to sustain sufficient distance between his identities and ensuring they didn't connect with one another [130]. Ross Ulbricht attempted decent operation security, he paid his rent in cash and went by another name to many, but as one of the largest operators of a 'dark market' at the time, reviewing online personas would seem a priority to many in a similar position. Blake Benthall also had awful operational security, the operator allegedly behind Silk Road 2.0 used his own personal email (much like Ross Ulbricht, who used his personal email in instances which connected him to Silk Road) to register the servers used for Silk Road 2.0. This is obviously some of the strongest pieces of evidence you can have on an individual to connect them to the case and shows possibly naivety after the arrest of Ross Ulbricht. It was clear from the evidence that he had made an operational security mistake, but Blake made no adjustments to how he acquired the servers for Silk Road 2.0 [131]. Alexander Cazes, the alleged operator of Alpha Bay, used his personal email (Seeing a pattern?) for a welcome email when users registered to the site, which law enforcement took note of in 2014. There was also a password recovery feature which also utilised the same personal email. This was beyond poor operational security, the features were later deprecated but it was too late for Alexander Cazes, law enforcement had an email which so happened to be a personal email address linking to him [132]. All 3 of these used personal emails and all three also had 'Linkedin' profiles, which allowed law enforcement to not only gather information about them as a person but have verifiable pictures of the alleged operators. In fact, Ross Ulbricht had a half an hour video of himself discussing various personal areas in his life, allowing investigators to analyse him as a person. Due to the advancement of privacy from anonymous

networks, law enforcement must look further into far more abstract and usually more creative ways in identifying the sites operators. Eventually, an operator will make an operation security mistake either in the 'clearnet' or in the 'dark web', it depends how long that mistake is available for people to see that will decide whether you are caught. Technological issues have existed, where dark market operators have little knowledge in security, but operational security is currently the number one failure in big dark markets. Swathes of members in 'clearnet' communities are active and participate in continuing dark markets, they may not be perfect, but they have a large number of individuals with vested interests in its continuance. In the criminal complaint against Alexander Cazes, it is notable that on the staff list is a member by the name of 'Trappy', described as being in charge of 'outreach to the dark market community by posting on public forums such as Reddit' [132]. Modern markets have departments like any other business and promoting your own dark market is very important, as there is so much competition involved. Outreaching onto the internet is something I have discussed previously, its requirement as the markets cannot hold themselves within anonymous networks, they must utilise public forums and communities like Reddit and YouTube. These public spaces are also how dark markets produce growth in sales and listings, it is not only the media coverage of seizures by law enforcement. The AlphaBay dark market even had a department to combat against phishing attempts wishing to scam customers by stealing bitcoins. Dark markets cannot rely on what many businesses do on the internet which is review previous history of IP connections and behaviour, the original identity of the user is hidden from view due to anonymous network specification (This is of course, with the exception of traffic analysis, behaviour analysis and exploits to denanonymise someone). This means other security measures must be in place like security pins, public key cryptography and 'anti-phishing' departments. These departments give a structure to the dark market and AlphaBay is not the exception, due to the amount of money that is processed through dark markets and as the main currency of these dark markets sky rockets, at time of writing I will add. Dark markets are having to create structure and hierarchy in the markets, making real business decisions like any other business would. An increase in sophistication is clear in regards to correct structuring and segmentation of work, although Silk Road had others help Ross Ulbricht, it is clear that AlphaBay, the most recent case, had considerably more thought put into how it was structured.

Reviewing dark markets from afar, it is clear that seizures simply won't change dark markets or the community. It will continue to evolve, wiser and more secretive members will conjure up new marketplaces. So far, very few creators of dark markets have been able to handle their operational security, but that doesn't mean someone won't. Ross Ulbricht chose a new name for himself while operating the Silk Road dark market, instead of being called 'Admin', 'Silk Road' or 'SR' he renamed himself and asked to be called 'Dread Pirate Roberts'. Many parts of the criminal complaint against Ross Ulbricht reference 'DPR' which is 'Dread Pirate Roberts'. Dread Pirate Roberts is from a fictional novel named 'The Princess Bride'. The novel reveals Dread Pirate Roberts is not one man, instead, it is multiple individuals who pass down the name to 'successor' they chose once they are wealthy enough to retire. It's a striking choice of name that was very deliberate, with so many operational mistakes from previous dark markets, individuals may look at the idea of becoming temporary administrators of a dark market, to which they transfer after retiring with enough financial gain. This was the intention of Ross Ulbricht it seems, although he acquired a decent amount of wealth before his arrest. The Dread Pirate Roberts name can also be seen in the dark market as a whole, individuals have carried on the crusade of dark markets, and the only difference is that Ross Ulbricht did not choose them. Dark markets by my prediction will continue to rise until we provide social change in countries, eliminating the supply of drugs has not decreased demand and in fact many gangs have

been able to circumvent law enforcement. While drug policy in various countries is starting to gather momentum, especially marijuana, the policies are not coming fast enough. The largest demand from anonymous networks like TOR is simply drugs, there is of course weapons, terrorism and other horrifying content, but predominantly drugs are the main agenda. The 'dark web' has become a million pound industry in dark markets and many other areas such as fraud simply by the fear many have of it, it is misunderstood by many. If countries drug laws were to be amended or significant social change occurred in economic powerhouses, the dark market for drugs would collapse completely. The money that is potentially going to gangs from dark markets directly or indirectly would also collapse, there is no easy way of verifying someone's identity on a 'dark market' after all.

There are also cases of dark markets misleading law enforcement and others to go down a rabbit hole and probably try and spread law enforcements resources. Dream Market is the most prominent in misleading visitors who wish to pry the identity of the site, as one the oldest markets, there are many questions within the community of its authenticity but it is still used as of writing by many. One case of them trying to mislead users was by leaving a benign IP which they referenced as a 'Debug URL' in code which updated 'buddies' on the site. A user caught wind of the IP in the source code and decided to share this information on the popular 'clearnet' website Reddit. This was in conjunction with the seizure of AlphaBay and Hansa, which is strange, surely Dream Market does not wish to scare users away by revealing apparent frailty in security? A couple of weeks later, Dream Market once again tries to deceive users who try to gather the actual location of the servers which contain Dream Market property, in this case the forum. The Dream Market admins decided to append a HTTP header into the header file of the forum code, which is trivially done. Adding the optional response header 'Content-Location' [138] which resolved to a Zimbabwe server, whether this was trying to hurt rivals, honeypot attempts at intrusion or simply trying to mislead many people we may never know. It's interesting to see an administration be so active in trying to deceive many. The current marketplaces available show a distinct lack of understanding in regards to security, I discovered this when I first started looking into dark marketplaces, there are markets which had relatively good security. I can recall that AlphaBay when online had a system that could capture trivial attack attempts like SQL injection and other abnormal activity that an attacker may do and halt it somewhat. There are many markets currently online which show lack of experience in web application security experience and heavy reliance on open source code for security, while admirable, many admins do not change or customise this code. Some Administrators do not even understand the bare basics of administering a hidden service, especially a dark market, rule 1, don't reveal your server to inbound traffic outside of TOR such as the 'DHL Market' (Dark Heroes League) which is now dead. By searching through a popular internet scanner service available from the internet and searching a specific string, you can see that the service found the DHL Market server due to the server responding with the markets name in the server's response to a request. Not good. This event also happened after the AlphaBay seizure where everything seemed to be in flux, DHL Market were actively advertising invites on 'clearnet' forums and seemed the natural choice to many. There are less known flaws that aren't horrific, but show that most markets currently online are not well versed in web application security or have some tolerance to the flaws that are in many of these applications. I analysed forum software which Dream Market uses, Traderoute also uses this software. The way passwords are stored in the forums database is worrying, in today's security standards, subpar. I'm unsure if it were a coincidence but after writing my article on the problems of the forum software the popular marketplace Traderoute administrators announced they would be 'starting from scratch' with the forum. Dream Market has remained satisfied with the software it seems.

For people who wish to have some technical definition, the database passwords were stored in the SHA1 hashing algorithm without a salt. I could verify this by looking at the CSRF token responses that were given to me from the forums. I found that CSRF tokens were not random enough on the internet, and certainly not through anonymous networks like TOR. A hidden service will have no knowledge of the clients location, it will return 127.0.0.1 as the request is served. The CSRF token was divided among a publicly accessible user ID, hashed password and hashed 'Client Location' which, in regards to TOR, will always be 127.0.0.1. These features in a cookie allowed me to register and confirm that no administrator had changed the security of the forum software, and in fact, passwords were stored in simply SHA1 with no hash. Salts allow hashes to be 'cracked' (They are not decrypted, as many like to refer to, it is a one way function) far slower. Although quite optimistic, it is indeed possible, and I say possible very loosely, to takeover someone's account in these forums through the CSRF vulnerability I discovered in these TOR hidden service forums. This would require a victim to visit another malicious hidden service among other variables [139]. What's clear is that admins either don't care or don't know the issues that could arise using a hashing algorithm like SHA1, which was found not to be collision resistant by Google in 2017 [140]. Dark markets are probably one of the biggest targets to hack on the 'dark web' due to the amount of sensitive and interesting information it holds. It holds information on drug dealers around the world, potential firearms (Depending on the market) salesman who wish to remain anonymous as well as a wonderful stash of bitcoins. Phishing attacks are rife but attempts at disrupting a marketplace by hacking it for monetary gain have also been prevalent. On the 23rd of August 2017 the Traderoute Administrator confirmed there was a vulnerability that allowed hackers to get away with $100k, some would say a large amount, but in dark market terms, this is fairly small. Traderoute is still an active market as of writing, the post that the administrator gave in explanation to the hack showed how routine this seemed to them stating 'We already released a patch and moved on'. In 2013 an emerging market called 'Sheep Marketplace' was hacked, the attackers stole around $6 million bitcoins (worth at the time) [141]. This though, was not all of the bitcoins available in the 'Sheep Marketplace' and is sometimes the issue with anonymous users providing a service, users of such a marketplace are also susceptible to 'exit scams'. Users are threatened in the dark market by law enforcement, phishing attacks, hackers on the platform and the owners themselves. Trust is something that is worth a lot in the 'dark web'. Alexander Cazes gained his through being notorious at carding, Ross Ulbricht gained his organically by being the pioneer behind the now popular platform for purchasing illicit items. The hacking of 'Sheep Marketplace' led to two individuals being arrested in Florida, these were the hackers who stole a fairly small amount in the market compared to the overall amount available in Sheep Marketplace. This seemed to have spooked the author of Sheep Marketplace and thy decided to shutdown the market, they suspended withdrawals and decided to run with the bitcoins into the distance. After all, all marketplace administrators are there to make money, even the Silk Road founder who seemed to have ideological reasons for creating the market became possessive of power and money in the end. In total, the Sheep Marketplace founder stole 40,000 bitcoins which was around $40 million dollars at the time [142]. The bitcoin marketplace value was very high at the time which probably nudged the founder to go for an 'exit scam'. Thomas Jiřikovský, the alleged owner of the marketplace was arrested by authorities due to using a fairly direct way of exchanging bitcoins for currency to buy a house, it was a large sum of money which law enforcement were attempting to track. Users were also aiding in tracking the money trail as seen from many threads on the popular 'clearnet' forum Reddit. The sheep marketplace 'exit scam' is widely cited as the largest exit scam to ever take place, Sheep Marketplace grew in user base due to Silk Road shutting down due to the arrest of the owner. Modern markets are trying to gain trust by making a more decentralised

model in how currency is exchanged, making users less reliant on owners being trust worthy. The evidence given in 'clearnet' forums about the Sheep Marketplace owner moving bitcoins out of the market shows the use of 'tumbling' the bitcoins, a common method to try and conceal where the money is heading to, it is often also referred to as 'mixing'. Exchanging the money is another issue that not only owners have in the 'dark web' but also vendors have when trying to remain anonymous. Eventually currencies that are used for the marketplace, exclusively cryptocurrency, almost always bitcoin, have to exit into other currencies to pay for regular things. Although, it is becoming increasingly popular in digital products, it still has a way to go when you want to buy things like let's say a house or a car. The Sheep Market owner has very little known about him, but he was unlike the alleged AlphaBay owner from what I can see. Alexander Cazes was very good at exchanging money and understanding how to lose track of money through carding, the inability to realise that exchanging money through services which are known to be law enforcement friendly from the Sheep Marketplace owner shows. Bitcoins are being used by many law abiding companies so we should not write them off as a criminal currency, unlike previous dodgy digital currencies like Liberty Reserve. When owning at that time 1% of bitcoins, you should probably look at keeping a slow and steady approach to exchanging the bitcoins for other currency. What is clear is that there are many threats that face all parts of the dark market landscape; buyers, vendors and owners, all have to provide a decent amount of trust in one part of the system for this to work. Dark market technologists are trying to move the markets further into a complete decentralised structure, but whether you can get purchasers to move further into more technologically intricate environments is something I have not witnessed from any community, even parts of the security community.

I have pointed out multiple times that anonymous networks provide us with security innovations that we can use on the 'clearnet' as well, but dark markets can also allow us to see interesting ideas in the security realm. This is mostly due to the threats like law enforcement and the big pay offs that phishing attackers can provide to any dark market, security must be tightened further from even normal standards from the 'clearnet'. While I have discussed problems in dark marketplaces there are marketplaces who also are creative with their approach to developing a marketplace. Trends begin to set from initial innovators and emerging markets begin to implement these to keep the trust they have with its user base and also to keep itself safe (Forced PGP Communication/ MultiSig transactions). Forced PGP vendor communication is becoming more and more of a requirement for a dark market due to seizures and hacks that have occurred in recent years, it allows customers to remain confidential and safe to a certain degree. Forced PGP communication is not required in normal 'clearnet' markets (When I talk about 'clearnet' markets, I am referring to markets like eBay and Amazon, not 'clearnet' drug marketplaces that may occur), it probably won't occur in the future either as PGP seems a dieing technology. A lot of what dark markets do can be seen as an experimentation, many wish to remain as secure as possible and must learn increasingly more about harsh security measures. Forced PGP communication on the 'clearnet' is usually required by internal bank emails and governments.

TradeRoute is a market that has gained popularity since the fall of AlphaBay and Hansa has an interesting anti-phishing mechanism that I haven't seen in any other dark market as of yet, be aware, I don't actively research every market, so I'm not stating they are the initial implementers. Image based authentication is essentially where an image is used to authenticate the user that the page they are visiting is the real deal, this is what Traderoute are doing. An image is associated with your account, if you enter your username and find it does not have this step, or isn't the image you associate with your

account, then this surely would be a phishing page. A simple way of authenticating authenticity. It has however been implemented by banks a few years ago to which some have phased it out, others still use it, this is mostly due to banks wishing to defend even if a user is infected, where this sort of anti-phishing technique would not pay off. There are other security ideas like multi-factor authentication that are far more helpful to banks than image authentication. What's clear is that dark markets cannot implement modern day bank security features like two factor authentication where a mobile device is associated with an account, this would have obvious problems for people wishing to remain anonymous. There are distinct differences between some of the banks image based authentication and Traderoutes, you do not have a choice of what your image is on Traderoute, you are simply assigned one, therefor unless you keep spamming registration with requests (which will take a while, they have a CAPTCHA in place) you will not have any knowledge in regards to how large the image array is. It could contain hundreds of thousands of unique images that could not be replicated by a phishing campaign very well. Banks on the other hand, from my experience, allow you to choose say, a wild animal for you to remember from a matrix of images containing wild animals. Giving one account different possibilities of other images to choose from allows them to gather knowledge on other possibilities for an attack. Whether users actually take note of the image is something to be argued about and Traderoute still have issues with this method, to receive the image we don't want to reveal a password, therefore only a username and a CAPTCHA is required to reveal the image. This gives us potential issues that can help phishing attacks, if CAPTCHAs can be resolved easily by a machine this method is useless, an attacker can send a request, solve the CAPTCHA and grab the image in a matter of seconds. This seems like an easy task as I've simply stated an attack within a matter of sentences, but solving a CAPTCHA is not as easy as many may think. You can pay for services which I've never used which can supposedly resolve CAPTCHA's but I'm sure it can be inconsistent at times. Alternatively you can look at the CAPTCHA source code (if available to you) and try and find how you can solve the CAPTCHA. Luckily, many Dark Markets have CAPTCHAs which are relatively easy to find on the internet, using open source code makes understanding a system relatively easy. What should be noted and what I'm trying to point out is that all these security experiments should be followed by many, anonymous networks are a highly volatile place, where many users wish to harm dark markets. Dark markets are certainly attacked on a daily basis through application level attacks. Some are trivial, but some aren't. Watching how administrators remain vigilant or make mistakes can give an interesting insight into how to maintain a companies 'IT Estate' as many put it. There has been dark markets that have paid bug bounties to hackers who have disclosed *responsibly* a vulnerability which could have harmed the marketplace, it is not simply large companies on the 'clearnet' who are friendly towards hackers finding vulnerabilities. In fact, Dark Market administrators must be some of the most paranoid people on anonymous networks.

The volatility of anonymous networks, dark markets in a constant cycle of rising and falling, allows creativity and abstract ideas to flourish to try and alleviate what seems to be a never ending battle for calm. Decentralised markets are currently the communities' favourite flavour of the month, but how this is done and if it would catch on is another thing. As I've discussed, there are always a hardcore sub-group of technologists in an organisation or group that will be able to religiously follow intricate security procedures to remain safe, it is whether the majority of other users have the ability to be converted easily and whether these ideas remain safer than current ones. This is the type of thinking that produced anonymous networking and dark markets as well. There is never ending updates, drama and surprises when looking into Dark Markets, the environment it's in, on an anonymous network – but not

limited to – is something that leads to more questions about not only dark markets, but models in a future economy too.

CHAPTER 9

THE GREAT MIGRATION

Now available on the ‘dark web’. Something I see often in headlines from news articles and website owners, a large portion of extreme and illegitimate material is migrating to the ‘dark web’. Does this mean that content removal on the internet is finally winning or is the control of information being lost? 2017 has been an explosive year for the world, tensions among many nations are rising and countries internally have vast domestic issues. On August, Charlottesville in America had a white nationalist rally which provoked many to protest against, the two sides present proceeded to clash which led to a state of emergency to be called. During all of this uncertainty and craziness an event took place that changed the relationship between the ‘clearnet’ and the ‘dark web’. Someone died during the protests. A far right white nationalist drove a car into protestors which led to the death of a woman, who was a civil rights activist named ‘Heather Heyer’. One notorious Nazi website was attributed to organising the Charlottesville demonstration which later insulted Heather Heyer, this led to many organisations which control how the ‘clearnet’ is connected turning against them. Leaving them with no choice but to migrate to the ‘dark web’. Many of these organisations that hosted in one way or another the Nazi site Daily Stormer were regularly citing the line that they were breaching the terms of service, but most believe with such a high profile site with the current news at the time, business would not go well. The Daily Stormer used classic tactics that many criminals use after their initial infrastructure has been taken down. They seemed to purchase a Russian domain amongst others to try and keep the site online on the ‘clearnet’. To keep the service safe from DDoS attacks and users pressuring a hosting provider into withdrawing their support, they enlisted the help of Cloudflares services, a service which can mask (*mask in very italic characters*) a servers location by using Cloudflares to forward traffic through, it’s primary purpose is so Cloudflare can ‘scrub’ bad requests such as hacking attack requests or DDoS attempts. I must stress that many legitimate businesses use Cloudflare, it is simply exploited by criminals and others due to its firm stance on freedom of speech. Sound familiar? A service which makes it hard to find a servers location? Cloudflare had initially hosted the Nazi site Daily Stormer on their service, in which many other non-desirable sites have been kept safe, but for the first time the site was terminated from their services. A rather lengthy reason why was promptly posted on Cloudflares blog detailing why they had decided to remove Daily Stormer from their services [143]. A similar fate of migration occurred to the Nazi forum named StormFront, which has a rather sadly long history of being online on the internet. The forum StormFront is a horrifying forum, not only is it linked with over 100 murders, but also seems to provide answers to alienated white men online looking for a cause [144]. One member from Stormfront many will remember, in 2011, produced a horrifying attack which killed 69 people. In Norway, Anders Behring Breivik was responsible for a large attack that Norway had not

seen before, according to SPL center, Anders had been a member of the forum for around 3 years. Stormfront was registered in 1995, it's webmaster a former Klu Klux Klan member who learnt basic programming while in prison. Stormfront has grown as the large base for holocaust denial and white supremacy. A extremist website which has members who have killed citizens of western nations would be mostly understood to be exclusively Islamic extremism, if it were, it probably would have been shut down swiftly for terrorist material. How interesting it is to note that a website which can be attributed to so much killing was able to withstand being online for so long. And only another death led to the forums demise. Forums are becoming an old way of communication, but there are many which are thriving and growing, including 'dark market' forums. On the 'dark web', forums are usually seen as the communication method of choice due to the requirement of not using JavaScript, there are forums with messaging features and other markets who wish to utilise Javascript, but generally it's seen as a bad idea. Static websites are usually not seen as a characteristic of what many call 'Web 2.0' and so old ideas from the 'clearnet' are usually recycled on the 'dark web'. After the far younger site Daily Stormer was kicked offline and out of the internet, Stormfront was also kicked offline at the same period, looking through the records it is clear that Stormfront also utilised Cloudflares technology to remain 'safe'. These two sites were forcibly removed from the internet, they only had one choice while trying to keep their server location private, the only possible choice the administrators had for these abominable sites were to move them to the 'dark web'.

An onion address is generated by using properties from cryptography that are required to operate a hidden service, specifically, utilising public key cryptography. Many websites like to create 'vanity' addresses that allow the onion address to seem less random and easier to remember, for this to work, the user must generate keys until the correct combination of characters is met (Simplified, yes, hashing is involved). This is no easy task. Hashing is a less computationally expensive task unlike public key cryptography, where the generation of a 'public key' and a 'private key' are considerably more. This means that users with vanity addresses have used a decent amount of computing power to generate these addresses, probably utilising hardware specifically for the task, much like hardware that is specifically designed for mining bitcoins. Most generating these vanity addresses will be using or following the concepts that the 'scallion' project has available to the public, the project is specifically designed to craft vanity onion addresses [145]. The onion address is limited to base-32 which gives some limitations to what you can have within an onion address, and in fact complete vanity addresses like Facebooks will be a thing of the past due to new Tor specification, changing the way hidden services are dealt with in the TOR network overall. One part of the specification outlines the new much longer addresses that will appear in the network. At the time of writing onion addresses rely on SHA1 hashes, this can be problematic as Google have recently proved that this hashing algorithm is not collision resistant. This is not good for a hashing algorithm, TOR have opted to upgrade the onion address by keeping to the same format, utilising base32, but using a checksum, constant version and public key bytes for the onion address. Relatively the same. One thing that will ruin a lot of full vanity addresses, is the fact that the version field for the onion addresses is set without the possibility of it being set by the user, defaulting currently to the letter 'd' [146]. Although a full vanity address I've only seen from Facebook, others opt for the start of an onion domain to have some vanity and then randomised characters afterwards, making it slightly memorable. What we know from onion addresses, is there is no third party involvement, no need for registrars who can remove your domain from the network it's on, which has happened to some far right extremist sites which have previously existed on the internet. Hidden services are censorship resistant by design, registering a hidden service to the TOR network is administered within the network, but there is no such feature which allows revocation

of a onion domain, thus allowing virtually anything to be hosted. This major feature of TOR is what leaves many scared, it allows anyone to be able to say what they want without fear of being shut down (unless your host doesn't want your content that is of course). One problem that may calm many people's concerns which I have highlighted many times is that anonymous networks are not exactly like the internet, in fact, anonymous networks at the moment, especially the TOR network, need the internet for users to be aware of it. Anonymous networks are a subset of the internet, you must first use protocols familiar to many to access TOR. There is simply further features that are added on to be able to access the network. The internet is required to promote services, throughout this book we've seen dedicated departments in organisations to market their onion hidden service, this is the crux of the matter in regards to how worrying the 'dark web' can be. The 'dark web' is unable to keep itself afloat, there are no good search engines because it is exactly designed in this way. The internet essentially is the gatekeeper to the dark web, we are in control of what gets promoted, there are search engines and wikis on the 'dark web', but are miniscule to the traffic that is made on the 'clearnet'. This can be made clearer by seeing how phishers exploit this fact and promote their onion urls online to scam users of the 'dark web'. Primarily they are focused on 'dark marketplaces' but I wouldn't be too surprised if they branched out to other valuable accounts available exclusively from the dark web. There is also the issue that the internet faces which is the base-32 addresses are much like IP addresses, forgettable. Sure, you cold note all the onion hidden services you wish to view, but, we are human and most do not do this. We built DNS to ensure we didn't have to remember complicated IP addresses for a reason, so it was memorable and people couldn't exploit swathes of innocent users. Individuals will go on a search engine on the internet to find the onion address they wish to visit, search engines on the 'dark web' are rarely updated well. This means that the way people connect to services on TOR hidden services means you do not simply peruse or surf the 'dark web', you locate the point you wish to go to and that's it. Almost, by design, anonymous networks are designed to be supported by the 'clearnet, especially in the context of TOR (Don't bite my head off – I know lots of people are doing different stuff with anonymous networks, but in general this seems to be true). This means users not so dedicated to causes or are less enthused by the idea of having a separate browser to visit one site, they will drop off from a lot of hidden services radar, including Nazi sites. Hopefully I've calmed you slightly with this fact, that it does take considerable effort to reach the hidden services often. Alexa estimates that Stormfront got around half a million unique visitors in a month, these are numbers that you won't see in anonymous networks, it relies on user donations and will find it hard to gather resources appropriately to where it can keep administration of the site. The lack of spotlight that these sites are getting is showing when Daily Stormer followers were trying to distribute PDF material, a 'flashy' magazine which covered far right topics to spread through social media, a tactic often attributed to terrorists who are unable to gather enough infrastructure to distribute effectively and consistently. Mostly this is due to take downs by providers who have no appetite in serving the material. One user on social media states 'The Daily Stormer is now using a polished PDF format. Readers are obligated to share it'. What the administrators of The Daily Stormer and many other hidden services on the 'dark web' have noticed, is the traffic they generate comes predominately through the internet and to spread ideas they must be able to still distribute information through the 'clearnet'. In their publication it is clear they are desperate to remain in the surface web/'clearnet'/internet/whateveryouwant by having multiple references to censorship and stating 'we would rather be publishing on the open Internet if only they wouldn't keep seizing our domains' (genuine quote, no, really). They reference multiple times their 'dark web' onion address but do understand that many simply won't visit this strange place to many, which is why they have decided to distribute a magazine through the 'clearnet'. The issue they have is

distributing through social media, a similar tactic that is used by terrorists groups such as so called IS who have mass posted on social media like Twitter to gather attention from the west. This method is not as powerful as running a 'clearnet' website, unlike Pirate Bay or other websites which have kept an active audience since media outlets started publishing stories on them. The distribution of PDF's on the 'clearnet' and hidden services on the 'dark web' cannot maintain the same audience, the technology is different and is not what people would call conventional viewing in regards to web content. This is why many far right individuals are franticly trying to find a domain extension which will accept them, so they can serve content which can be spread easily.

The only hope of remaining uncensored in some way without domain registrars taking action on them is spreading the use of middle services which work on the web that can interact with TOR's anonymous network. This obviously has the huge issue of trusting this service to not manipulate the response it gives or track you any way, services like onion.to and onion.link have had dark web hidden services linked and gathered into Google's search engine, but not high enough to get any real credible traffic. They are also highly unreliable, since writing this, one service is down and the other is incredibly slow. In fact, on the onion.to main home page it states that is has no anonymity and the best possible choice is to download the TOR browser, promoting these services may in fact endanger many groups who possibly do not wish to be known. It states 'Onion.to as a gateway cannot offer any anonymity for the visitor. For example, both onion.to and the hidden service itself can see the visitor's IP address'. One of these web gateways to TOR highlights the issues with having such a gateway, the need for revenue. A large portion of sites have started to look away from conventional revenue streams such as advertising and started to look at more creative ways of making money, such as cryptocurrency mining. Cryptocurrency has come a long way since its inception, and some have become more profitable. One of the TOR gateways decided to use technology to mine a cryptocurrency from visitors browsers, found by Yonathan Klijnsma. Essentially, utilising the computing power that every user has, slowing down the computer essentially. It is quite obvious, that you cannot rely on these services. Overall, it's a bad idea using these services for anything meaningful, while extreme sites like Daily Stormer and Stormfront may try and remain on the 'clearnet', they remain chaotic, moving domain to domain or isolated on the 'dark web' with very little engagement with users on the internet. To those who think the 'dark web' hosts terrible things and can only do harm, from evidence, it seems it leaves extreme groups isolated and lonely, requiring them to take extensive steps to stay relevant. Such as mass posting social media, setting up mirror sites throughout the internet to remain prominent or distribute media such as magazines or videos to keep followers to the 'cause' they may have.

Facebook realised this in 2017 when details of Instagram users had been taken from servers, information such as phone numbers, this information had been taken by exploiting a flaw that Instagram had in their API. Instagram began to ensure damage limitation by registering over 280 domains that Doxagram would try to market, the main search term for the Instagram hack would be 'doxagram', as this was the teams apparent name. By purchasing these domains and suspending the ones 'doxagram' had already registered they suspended the possibility of purchase on the 'clearnet'. The group swiftly took action and began to setup a 'dark web' version of the site shop, which allows you to purchase information on Instagram accounts, utilising the stolen data. This was something that Instagram could not affect, the registration of onion domains has no regulator. Information about doxagram was outdated at the time media groups took note of the hack and the group, individuals hearing about this mysterious shop would be unable to find any such market at the time of publication from most media outlets. Instagram also seemed to have flexed its muscles with social media, with

some posts being taken down, some which held little significance to actually accessing the shop. What was interesting was that momentarily, Instagram/Facebook had stopped the internet from finding or purchasing from this group, it now has a 'dark web' alternative and a 'clearnet' domain in which people can purchase account information. Luckily some would say for Instagram/Facebook, a huge data breach occurred around the same time, taking the story of Instagrams data leakage out of favour. The Equifax hack that eclipsed Instagrams API flaw has led many to believe this will affect people for years due to the severity of the data leak. What's different from the Instagram hack and Equifax hack is that Equifax hackers are much quieter than the Instagram hackers were. There have been many scam sites available on the 'dark web', supposedly offering the Equifax data for sale, none really showing anything viable except from what seems to be doctored 'sample' data. There were clear indicators that when migrating to the 'dark web' as many groups must for various reason, they still have to be supported by the 'clearnet' in some manner, this is evident with the Instagram data leak, in which the 'Doxagram Team' as they call themselves, persistently advertised the data online. This included places such as Pastebin and BitcoinTalk, common areas of the internet where similar services are sold. The advertisements are quite similar to those of carders, or old advertising techniques. Having bold sentences all in capital letters trying to attract the attention of the customer, ensuring they must not delay their purchase. Carders usually wish to offload the information they receive as fast as possible, as financial institutions usually notice abnormal behaviour pretty quickly. One sentence depicts my point well 'BUY QUICK, FAST SELL, FRESH STUFF! CONTACT PEOPLE THAT YOU WANT WHILE YOU CAN, WHILE DATA LASTS!!!!!'. This advertisement is made to attract attention from users by including the 'dark web' address, current 'clearnet' address and XMPP contact. The advertisements will then be crawled by search engines resulting in users around the world hopefully (in the view of the sellers) ready to become customers to the 'doxagram team'. All of these 'dark web' hidden services almost exclusively flourish through 'clearnet' means, without the internet, the 'dark web' would be unable to support itself. The assertion that many individuals give on the 'dark web' that it is indeed a dangerous place to go, where vast amounts of illicit material flourishes is indeed to some extent true, but can only flourish by being supported through information on the 'clearnet'. We must be able to understand that if a seemingly toxic site, brand, organisation or idea has now only one home, the 'dark web', this is surely a positive thing. A place which requires special software to access safely, which can only be supported through communicating with the 'dark web', which is isolated and outside of mainstream connectivity. If something must migrate to the 'dark web', it has been diverted out to the edges of our interconnected digital world.

CHAPTER 10

ACK

I first wanted to write this book, to really push a message across to people from all sections of society, the ‘dark web’ is not a mystical place where bad things exclusively happen, it is a place where security and privacy are concentrated on due to the fears of large government organisations (and I’m not only thinking of the US). I myself, have some issues with what many anonymous network projects do, the need for absolute privacy is one, although many debate if it is actually possible. As I’ve explained the best possible solutions require the understanding in my eyes that people who exploit anonymous networks for illicit means need to be caught in some way, but due to the grey definition of ‘who is bad’ in a network, we are left with an impossible task. Laws on who are criminal are dynamic, laws overall change constantly, for example, in the UK it’s nearly 100 years since we began to allow women to vote and only since 2014 that we legalised gay marriage. Anonymous networks provide a safe haven for people with ideas that are currently illegal, this may seem wrong but as I say laws are dynamic. Anonymous networks wish to support everyone around the world in being able to access information freely without discrimination and let exotic ideas in some cultures to develop. The borderless nature of anonymous networks with the addition of little regulation worries many governments, especially in highly conservative countries as I’ve outlined. The lack of any regulation on what content is held on the network is something that naturally unnerves me, for as the network matures more and more, vast amounts of content will migrate to this anonymous network. More and more people will learn of such areas of anonymous networks, as I’ve stated for now, it is a lonely isolated place, but whether it retains this attribute is another thing. I regularly ponder whether I am for or against TOR or most anonymous network projects, it is with great deliberation I conclude I am for. You may notice in paragraphs I seem extremely positive with the work from anonymous networks and am upset by the exploitation that is put upon them by criminals and others who wish to cause harm. Other paragraphs I am conflicted, as I describe the rising interest from groups such as paedophiles and terrorists. These anonymous networks are no longer early incarnations of themselves, especially TOR, instead they are mature iterations which are slowly becoming more popular in every corner of the globe, but whether this is correct is another thing. It is not simply about freedom of speech and censorship, it is also about privacy. I do not think all users who contribute to these projects are libertarian, but the overwhelming majority seem to hold some loose view of libertarianism. This ideology is something that while I can understand, I believe is fundamentally flawed. The finite details of my views on TOR, anonymous networks overall and libertarianism is not what I wanted to express in this book comprehensively, I hope I have achieved some level of being unbiased. I wish to project the message that the ‘dark web’ is not ‘dark’ or a ‘web’, it is an anonymous network. It is something that is beautiful and ugly at the same time and is different for every individual on the planet. The ‘dark web’ is a term which misidentifies the

point of anonymous networks and the overall contents of them, although that final point remains subjective (I don't think drugs are *dark* is my point here). These anonymous networks have been an experiment for some time now and are developing at a considerable pace. The advancement and ideas produced by surprisingly very few people has led to anonymous networks being where they are today.

I do not wish to write a conclusion like many technical or complex books which have a wide range of issues where I simply state 'there is a wide range of issues that we must address' with an incomplete, rather beige result. I think anonymous networks should be further developed but the subject of no regulation must be addressed, there are ways of forcing anonymous networks offline but many would probably prefer a solution through 'democratic means'. If anonymous networks are further developed in which it becomes an impossibility to exploit the software it is problematic. The cost for de-anonymising users on the TOR network by looking at history is expensive and used rarely, the cost of such exploits means I hold the belief there is an equilibrium between law enforcement and anonymous networks like the TOR network. There are many variables that can tip one of these forces off, the strength of law enforcement to impact globally is a never ending worry for many and as we all know, TOR cannot help individuals from a 'global passive adversary'. On the other hand, the rise in automated fuzzing (testing software for vulnerabilities) leaves the possibility that law enforcement may be unable to develop exploits in the future to the pace that would allow them to weaponise them in the wild. The question also remains to some whether we can ever remain completely anonymous, after exploring the subject I have come under the conclusion myself that we cannot. While we remain similar to many in our use of grammar, spelling and language overall, we all have uniqueness to us that can lead an organisation to us. This is also supported by the countless variables that we have when operating a computer or electronic device to communicate with people; such as the screen size, version of the software, time in microseconds, support for various capabilities and endless other variants. I decided to not discuss in this book Snowden or Wikileaks extensively, although many are probably unhappy that I did not feature a chapter on various events. I wanted to keep the focus on the actual item itself, the 'dark web' and how it can be misconceived so often. Today anonymous networks thrive, finding new ways to bypass oppressive regimes internet censorship measures which are constantly improving. Anonymous networks, especially TOR, have been fighting against some of the biggest oppressors of free speech in the modern world, such as China who has repeatedly tried to completely remove any inkling of TOR from its complex network. For this, I believe everyone who works on anonymity projects, not only exclusively anonymous networks, deserve commendation, it is no easy task, especially when millions rely on you. There is the simple fact that sadly anonymous networks are not only the home for journalists, free speech activists and citizens of oppressed countries. There are swathes of users who utilise TOR and anonymous networks to cause harm to others, paedophiles regularly communicate in discussion forums and extreme political views such as fascism have now entered onto anonymous networks too. It may be time to find a system that allows us to democratically regulate networks, not through large structures or organisations such as the UN, EU or NATO, but through some form of technological process which allows regulation to content that is deemed 'inhumane' (Videos of real murder, child pornography etc.). The idea of simply allowing any content is fine now, the isolated and anarchic characteristics that anonymous networks currently hold may not be in the future. This will not be down to progress from TOR, which are increasingly looking at compartmentalising hidden services, essentially making it harder to discover a hidden service. Shared throughout the 'clearnet' on forums, social media and archives or mirrors, hidden services are becoming a normality to certain communities on the internet, namely, paedophiles. We have our hands tied, we do not wish the internet to become a

militarised authoritarian mess (at least, the majority of us don't). Content removal is a touchy subject in recent years, which now has long processes, rightly so, to ensure that users are not being censored. But these long arduous processes are what allow hidden services sometimes to thrive, those days/hours where it takes time to be processed, and allows users to share the initial information. There are other possibilities on how information about hidden services is transferred from anonymous networks, obviously one is word of mouth or through private discussions, but initially forums, paste sites, social media and other user generated content sites allow a much wider reach. I'm not advocating looser regulation on content removal requests, some which would be impossible as some sites are advertised on less cooperative internet resources. The idea of censorship, privacy and freedom of speech first entered my mind when the infamous site 'The Pirate Bay' was raided. These ideas which have had lengthy debate over them are imperative in moving not only anonymous networks but the internet forward, we still haven't reached a happy medium or thorough understanding in how to advance ourselves past 'censorship is bad and content removal is hard'. The issues are coming from all angles, copyright, terrorism, anonymous networks, we must be able to bring an adult debate with radical ideas to overcome these current issues. In many countries, we rely on our politicians to resolve these through policy and regulation, but these mostly technological issues have yet been well debated through politics where anything meaningful has happened positively (SOPA was a defence). I don't believe in disruption, as many do in Silicon Valley, I believe politicians should be debating the core philosophical issues with the technologically minded. At the moment, in the UK this is not happening, we have one politician demanding messaging applications to turn back the clock and remove encryption from their services. This is the wrong approach, although I haven't seen the debates or discussions made in private, it's evident it was a demand.

People within technology circles are just as easy to blame, usually quite contradictory to people with little technical ability, we have all been guilty of feeling taxed due to someone's inability to grasp technology correctly. Many simply see the issue as 'we know better' and I don't think this is good enough, positive debate over these matters are more important and are needed. Of course, I feel I may be wrong at points, I am fairly young still and have endless things to learn in my field, let alone, technology. I simply feel that the issue of censorship and privacy have not been debated enough, we have staunch authoritarian conservatives who wish to control the internet and be aware of everyone within it. There is also the anarchists and libertarians who wish to have little to no control over any aspect, to let the content remain without any intervention, even if it may be content which is repugnant. Due to the internet and anonymous networks borderless nature, this will of course take a rather long time, in fact if an ideal is found, it may only be present in pockets of countries, which leads us to our next issue with anonymous networks and why they are key. Until every country with internet access has the freedom to browse content without mass surveillance upon them for no reason, we still need anonymous networks designed the way they are and progressing. With so many conflicts, anonymous networks are sure to be here for a long time and will be needed.

After writing so much, I feel I have set a decent amount of points that many can scrutinise, debate and look over. I want people to be more aware why anonymous networks are important but why they are also an issue. The internals of these networks are far more technical than traditional ones, I haven't covered the technicalities of anonymous networks like TOR as extensively as maybe some would have liked, but as I have stated many times, that is not the purpose of this book. I was writing this book when AlphaBay and Hansa market were taken down and in fact was writing the chapter on markets while this was happening, it felt that nothing I was writing would be good enough after a few weeks due to how

much had happened. The market users were certainly in shock and it was interesting to see how the market moved on from it. The double hit from two markets changed the way many looked at ‘dark markets’ and also pushed many to look for alternative ways of purchasing drugs and other items, maybe something law enforcement were not anticipating. New ideas are starting to rely on the ‘blockchain’ a truly decentralised market, whether this gains any momentum is something I really cannot predict. A few years ago, I really did not think that users with little to no technical ability would be purchasing drugs through TOR, but Silk Road somehow captured people to do so. While researching endlessly on various topics in relation to TOR I have enjoyed the process of writing, it has taught me something that you maybe don’t get while learning technical subjects. Hopefully I have been able to at the very least keep you interested and at the very best given you some inspiration to learn about anonymous networks further.

“We know the past but cannot control it. We control the future but cannot know it.” – Claude Shannon.

[1] Alex Hurn – Us Government Increases Funding for TOR, Giving $1.8m in 2013 - https://www.theguardian.com/technology/2014/jul/29/us-government-funding-tor-18m-onion-router

[2] I2P – jrandom Departure - https://geti2p.net/en/misc/jrandom-awol

[3] Graph Theoretic Properties of the Darkweb - https://arxiv.org/pdf/1704.07525.pdf

[4] Lorenzo Franceschi-Bicchierai - New Dark Web Hitman Site Scams You Even Before Signing Up - https://motherboard.vice.com/en_us/article/new-dark-web-hitman-site-ghosting-place-scams-you-even-before-signing-up

[5] Eva Galperin – Access Now and EFF Condemn the Arrest of Tor Node Operator Dmitry Bogatov in Russia - https://www.eff.org/deeplinks/2017/04/access-now-and-eff-condemn-arrest-tor-node-operator-dmitry-bogatov-russia

[6] Loek Essers – Tor Exit Node Operator Convicted of Abetting Spread of Child Porn - http://www.pcworld.com/article/2452320/tor-exit-node-operator-convicted-of-abetting-spread-of-child-porn.html

[7] Tor Project – Legal FAQ for Relay Operators - https://www.torproject.org/eff/tor-legal-faq.html.en

[8] Chloe – BADONIONS - https://chloe.re/2015/06/20/a-month-with-badonions/

[9] – Uncharted Software – TORFlow - https://torflow.uncharted.software/

[10] – TOR – Support the TOR Network: Donate to Exit Node Providers - https://blog.torproject.org/blog/support-tor-network-donate-exit-node-providers

[11] – Nicole Morley – Father accused of raping daughter, 2, in livestream on the dark web - http://metro.co.uk/2017/04/22/father-accused-of-raping-daughter-2-in-livestream-on-the-dark-web-6590222/

[12] – Allan Hall - Depraved dad 'filmed himself raping his two-year-old daughter with another man and posted sick video online' - https://www.thesun.co.uk/news/3375440/depraved-dad-filmed-himself-raping-his-two-year-old-daughter-with-another-man-and-posted-sick-video-online/

[13] – Kari Paul – The Google Search that Took Down Ross Ulbricht - https://motherboard.vice.com/en_us/article/the-google-search-that-took-down-ross-ulbricht

[14] – TOR – Some Statistics on Onions - https://blog.torproject.org/blog/some-statistics-about-onions

[15] – TOR – TOR Metrics | Traffic on Onion Services - https://metrics.torproject.org/hidserv-rend-relayed-cells.html

[16] – Dr Gareth Owen – TOR Hidden Services and Deanonymisation - https://www.youtube.com/watch?v=-oTEoLB-ses&feature=youtu.be&t=1998

[17] – David Moore & Thomas Rid – Cryptopolitik and the Darknet - http://www.tandfonline.com/doi/abs/10.1080/00396338.2016.1142085

[18] – Myriam Dunn Cavelty – The Militarisation of Cyberspace: Why Less May Be Better - https://ccdcoe.org/publications/2012proceedings/2_6_Dunn%20Cavelty_TheMilitarisationOfCyberspace.pdf

[19] – The Economist – Buying Drugs Online, Shedding Light on The Dark Web - http://www.economist.com/news/international/21702176-drug-trade-moving-street-online-cryptomarkets-forced-compete

[20] – Alec Fullerton – Class of 2017: The Students Turning to the Dark Web for Their Drug Fix - http://www.independent.co.uk/student/student-life/students-dark-web-buy-illegal-drugs-university-2017-digital-dealers-a7578041.html

[21] – Possible upcoming attempts to disable the TOR network - https://blog.torproject.org/blog/possible-upcoming-attempts-disable-tor-network

[22] – Anju Viswam and Gopu Daran – A Survey on Identifying Identical Users among Multiple Social Media Sites - https://www.irjet.net/archives/V3/i10/IRJET-V3I10173.pdf

[23] – Rob Waugh – 12 Scary Things Which Happen When You Go On The 'Dark Web' - http://metro.co.uk/2015/07/08/12-scary-things-which-happen-when-you-go-on-the-dark-web-5285640/

[24] – Daily Mail – The Disturbing World of the Deep Web - http://www.dailymail.co.uk/news/article-2454735/The-disturbing-world-Deep-Web-contract-killers-drug-dealers-ply-trade-internet.html

[25] – The Telegraph – New Powers to Target Dark Net Paedophiles - http://www.telegraph.co.uk/news/uknews/law-and-order/11286849/New-powers-to-target-Dark-Net-paedophiles-explained.html

[26] – TOR – Amount of Onion Sites - https://metrics.torproject.org/hidserv-dir-onions-seen.html

[27] – Michael Berkens – Domain Registration at a Record Pace 460,000 Yesterday - https://www.thedomains.com/2015/11/08/domain-registration-at-a-record-pace-460000-yesterday/

[28] – Bruce Schneier – Paris Terrorists Used Double ROT-13 Encryption - https://www.schneier.com/blog/archives/2015/11/paris_terrorist.html

[29] – Sean Gallagher – Alleged TOR Hidden Service Operator Busted For Child Porn Distribution - https://arstechnica.com/tech-policy/2013/08/alleged-tor-hidden-service-operator-busted-for-child-porn-distribution/

[30] – Internet Watch Foundation – IWF Annual Report 2016 - https://www.iwf.org.uk/sites/default/files/reports/2017-04/iwf_report_2016.pdf

[31] – Bloomberg News (via Investment Weekly) – Morgan Stanley Data Offered On Internet for Virtual Currency - http://www.investmentnews.com/article/20150106/FREE/150109966/morgan-stanley-data-offered-on-internet-for-virtual-currency

[32] – Al Jazeera – Macrons Campaign Hit by Hacking Attack - http://www.aljazeera.com/news/2017/05/emmanuel-macron-campaign-massive-email-hack-170505232002764.html

[33] – Patrick Sawer – Bank details of 100,000 Britons for Sale on The Internet - http://www.telegraph.co.uk/news/uknews/crime/12155403/Bank-details-of-100000-Britons-for-sale-on-internet.html

[34] – Mcafee – Hidden Data Economy - https://www.mcafee.com/us/resources/reports/rp-hidden-data-economy.pdf

[35] – Associated Press (via The Guardian) – Hack in the USSR: Cybercriminals Find Haven in .SU Domain Space - https://www.theguardian.com/technology/2013/may/31/ussr-cybercriminals-su-domain-space

[36] – Fabio Assolini – New gtLDs, Same Attacks - https://securelist.com/new-gtlds-same-attacks/64555/

[37] – The Guardian – Russian Business Network - https://www.theguardian.com/technology/2007/nov/15/news.crime

[38] – FTC Gov – FTC Shuts Down Notorious Rogue Internet Service Provider, 3FN. - https://www.ftc.gov/news-events/press-releases/2009/06/ftc-shuts-down-notorious-rogue-internet-service-provider-3fn

[39] – David Bizeul – The Russian Business Network Study - http://fatalsystemerrorbook.net/pdf/Bizuel_onRBN.pdf

[40] – Ed Pilkington – Playstation and Xbox Facing Issues After Christmas Day Attack - https://www.theguardian.com/technology/2014/dec/25/playstation-xbox-down-lizard-squad-hack-christmas

[41] – Brian Krebs – Lizard Stresser Runs on Hacked Home Routers - https://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/

[42] – Mark Duell – Spokesman for 'Lizard Squad' Hacking Group Allegedly Behind Attacks on Microsoft and Sony Is Arrested Over PayPal Thefts - http://www.dailymail.co.uk/news/article-2893549/Spokesman-Lizard-Squad-hacking-group-allegedly-attacks-Microsoft-Sony-arrested-PayPal-thefts.html

[43] – Hackermanshank – Poodle Corp Video - https://www.youtube.com/watch?v=OYPHQsKZA44

[44] – Oz Elisyan – Lizard Squad Leaked Database - https://devcentral.f5.com/articles/lizard-squad-leaked-database

[45] – Sky News – Lizard Squad Member: Why I Took down Xbox and PlayStation - https://www.youtube.com/watch?v=fPX8yCBdIZ8

[46] – Pastebin - Evidence of Lizard Squad Google Cloud Usage - https://pastebin.com/655ba54R

[47] – Chris Williams – Lizard Squad Gang Moves from PlayStation, Xbox Live Attacks To TOR - https://www.theregister.co.uk/2014/12/27/tor_lizard_squad_sybil_attack/

[48] – Atagar – Possible Sybil Attack - https://lists.torproject.org/pipermail/tor-consensus-health/2014-December/005381.html

[49] – John R Douceur – The Sybil Attack - https://www.microsoft.com/en-us/research/wp-content/uploads/2002/01/IPTPS2002.pdf

[50] – Arma – The Lifecycle of a New Relay - https://blog.torproject.org/blog/lifecycle-of-a-new-relay

[51] – FBI – 'Playpen' Creator Sentenced to 30 Years - https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years

[52] – Justive.GOV – Florida Man Sentenced to Prison for Engaging in a Child Exploitation Enterprise - https://www.justice.gov/opa/pr/florida-man-sentenced-prison-engaging-child-exploitation-enterprise

[53] – Angus Crawford – Facebook Failed to Remove Sexualised Images of Children - http://www.bbc.co.uk/news/technology-39187929

[54] – Ben Popper and Nikki Erlick – Facebook is Closing in on 2 Billion Monthly Users - https://www.theverge.com/2017/2/1/14474534/facebook-earnings-q4-fourth-quarter-2016

[55] – Mashael Aljohani, Alastair Nisbet and Kelly Blincoe – A Survey of Social Media Users Privacy Settings and Information Disclosure - http://kblincoe.github.io/publications/2016_SECAU_Social_Media.pdf

[56] – Pamela Waisniewski, Bart Knijnenburg and Heather Lipford – Profiling Facebook Users' Privacy Behaviours - https://cups.cs.cmu.edu/soups/2014/workshops/privacy/s2p1.pdf

[57] – Daisy Dumas – Facebook Censorship: Which Images Passed (And Failed) The Nudity Test? - https://www.lifehacker.com.au/2016/05/facebook-censorship-which-images-passed-and-failed-the-nudity-test/

[58] – Sarah Perez – Microsoft Silences Its New A.I Bot Tay After Twitter Users Teach It Racism - https://techcrunch.com/2016/03/24/microsoft-silences-its-new-a-i-bot-tay-after-twitter-users-teach-it-racism/

[59] – Olivia Solon – Artifical Intelligence A.I Is Ripe For Abuse Tech Researchers Warn: 'A Fascists Dream' - https://www.theguardian.com/technology/2017/mar/13/artificial-intelligence-ai-abuses-fascism-donald-trump

[60] – Michael Pizzi – The Syrian Opposition Is Disappearing From Facebook - https://www.theatlantic.com/international/archive/2014/02/the-syrian-opposition-is-disappearing-from-facebook/283562/

[61] – Russel Brandom – Facebook's Report Abuse Button Has Become A Tool of Global Oppression - https://www.theverge.com/2014/9/2/6083647/facebook-s-report-abuse-button-has-become-a-tool-of-global-oppression

[62] – Al Jazeera – Facebook Blocks Scores of Pages in Thailand - http://www.aljazeera.com/news/2017/05/facebook-blocks-scores-pages-thailand-170511203548145.html

[63] – NSPCC – Online Grooming Cases Increase By Almost 50% - https://www.nspcc.org.uk/what-we-do/news-opinion/online-grooming-cases-increase-50/

[64] – Richard Adams – Nicky Morgan: Islamist Extremists Using Same Grooming Tactics As Paedophiles - https://www.theguardian.com/education/2016/jan/19/nicky-morgan-islamist-extremists-grooming-tactics-paedophiles

[65] – CEOP – Alarming New Trend In Online Sexual Abuse - https://www.ceop.police.uk/Media-Centre/Press-releases/2013/ALARMING-NEW-TREND-IN-ONLINE-SEXUAL-ABUSE/

[66] – Torrent Freak (ERNESTO) – Facebook and Foxtel Team Up To Crack Down on Live Streaming Piracy - https://torrentfreak.com/facebook-and-foxtel-team-up-to-crack-down-on-live-streaming-piracy-170213/

[67] – Michael Farrel – After 'Facebook Killing', Social Media Confronts It's Dark Side - http://www.csmonitor.com/USA/Society/2017/0420/After-Facebook-killing-social-media-confronts-its-dark-side

[68] – Liat Clark – Hacker Forum Darkode Is Back and More Secure than Ever - http://www.wired.co.uk/article/darkode-back-and-more-secure

[69] – Xylitol – Darkode Leak - http://www.xylibox.com/2013/04/darkode-leak.html

[70] – MalwareTech – Darkode – Ode To Lizard Squad (The Rise and Fall of a Private Community) - https://www.malwaretech.com/2014/12/darkode-ode-to-lizardsquad-rise-and.html

[71] – Justice.gov – Major Computer Hacking Forum Dismantled - https://www.justice.gov/opa/pr/major-computer-hacking-forum-dismantled

[72] – Twitter Xylitol – Invitations - https://twitter.com/Xylit0l/status/310296631645962241

[73] – Darkode (MAFI) – Watermarking - https://krebsonsecurity.com/wp-content/uploads/2013/04/mafionwatermarkingmath.png

[74] – Micah Lee – Chatting In Secret While We're All Being Watched - https://theintercept.com/2015/07/14/communicating-secret-watched/

[75] – Facebook Developers – Facebook Chat API - https://developers.facebook.com/docs/chat

[76] – Ofer Caspi – Global XMPP Android Ransomware Campaigns Hits Tens of Thousands of Devices - http://blog.checkpoint.com/2015/08/31/global-xmpp-android-ransomware-campaign-hits-tens-of-thousands-of-devices/

[77] – Malware Don't Need Coffee (Kaffiene) – Inside Citadel 1.3.4.5 - http://malware.dontneedcoffee.com/2012/07/inside-citadel-1.3.4.5-cncNbuilder.html

[78] – Alec Muffet – 1 Million People Use Facebook Over TOR - https://www.facebook.com/notes/facebook-over-tor/1-million-people-use-facebook-over-tor/865624066877648/

[79] – Runa – Ethiopia Introduces Deep Packet Inspection - https://blog.torproject.org/blog/ethiopia-introduces-deep-packet-inspection

[80] – Runa – An Update On The Censorship In Ethiopia - https://blog.torproject.org/blog/update-censorship-ethiopia

[81] – Freedom House – Internet Freedom Report 2016 - https://freedomhouse.org/report/freedom-net/freedom-net-2016

[82] – Roland Dela Paz – Off-The-Shelf Ransomware Used To Target Healthcare Sector - https://blogs.forcepoint.com/security-labs/shelf-ransomware-used-target-healthcare-sector

[83] – Catalin Cimpanu – Teenager Arrested In Austria For Spreading Philadelphia Ransomware - https://www.bleepingcomputer.com/news/security/teenager-arrested-in-austria-for-spreading-philadelphia-ransomware/

[84] – Dissent (Data Breaches) – 218,000 AlphaBay Marketplace Users Private Messages Acquired By Bug Hunter - https://www.databreaches.net/218000-alphabay-marketplace-users-private-messages-acquired-by-bug-hunter/

[85] – Elizabeth Weise – Terrorists use the Dark Web to Hide - https://www.usatoday.com/story/tech/news/2017/03/27/terrorists-use-dark-web-hide-london-whatsapp-encryption/99698672/

[86] – Gordon Rayner – WhatsApp Accused of Giving Terrorists 'a secret place to hide' As It Refuses To Hand over London Attacker's Messages - http://www.telegraph.co.uk/news/2017/03/26/home-secretary-amber-rudd-whatsapp-gives-terrorists-place-hide/

[87] – Jessica Elgot – WhatsApp: The Go-To Messaging Tool For Parliamentary Plotting - https://www.theguardian.com/politics/2017/jun/12/whatsapp-the-go-to-tool-for-parliamentary-plotting

[88] – Lauren Said-Moorhouse - How Syrian Activists Use WhatsApp to Tell the World Their Stories - http://edition.cnn.com/2016/09/28/middleeast/whatsapp-syria-aleppo-activists/index.html

[89] – towcenter – New Frontiers in Newsgathering - https://www.gitbook.com/book/towcenter/new-frontiers-in-newsgathering/details

[90] – Shaun Nichols – Secure Messaging Springs Leak When Looking up URLs - https://www.theregister.co.uk/2017/06/19/whatsapp_app_flap_in_snap_mishap/

[91] – Nidhi Rostogi and James Hendler – WhatsApp Security and Role of Metadata in Preserving Privacy - https://arxiv.org/ftp/arxiv/papers/1701/1701.06817.pdf

[92] – WhatsApp – WhatsApp Encryption Overview, Technical Whitepaper - https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

[93] – Gudipaty LP and Jhala KY – WhatsApp Forensics: Decryption of Encrypted WhatsApp Databases on Non Rooted Android Devices - https://www.omicsgroup.org/journals/whatsapp-forensics-decryption-of-encrypted-whatsapp-databases-onnon-rooted-android-devices-2165-7866-1000147.pdf

[94] – Jeremy Seth Davis (SC Magazine) – WhatsApp In The Spotlight After Turkey Publishes Messages of Coup Officers - https://www.scmagazine.com/whatsapp-in-the-spotlight-after-turkey-publishes-messages-of-coup-officers/article/529892/

[95] – Liberation – La piste du SMS envoyé par un des terroristes du Bataclan - http://www.liberation.fr/france/2015/11/18/la-piste-du-sms-envoye-par-un-des-terroristes-du-bataclan_1414317

[96] – Rukimini Callimachi, Alissa Rubin and Laure Fourquet – A View of ISIS's Evolution in New Details of Paris Attacks - https://www.nytimes.com/2016/03/20/world/europe/a-view-of-isiss-evolution-in-new-details-of-paris-attacks.html

[97] – Chloe Farand – Manchester Bomber Salman Abedi Learned How To Make Explosive Device from YouTube Videos - http://www.independent.co.uk/news/uk/home-news/manchester-bomber-salman-abedi-learned-explosive-device-youtube-videos-a7805961.html

[98] – Samuel Gibbs – Google Says ISIS Must Be Locked Out Of The Open Web - https://www.theguardian.com/technology/2016/jan/20/google-says-isis-must-be-locked-out-of-the-open-web

[99] – David Smith – 'American ISIS Twitter Scene' Reveals Social Media's Power To Radicalise - https://www.theguardian.com/world/2015/dec/01/isis-america-twitter-social-media-radicalisation

[100] – Bill Goodwin – Islamic State Supporters Shun Tails and TOR Encryption For Telegram - http://www.computerweekly.com/news/450419581/Islamic-State-supporters-shun-Tails-and-Tor-encryption-for-Telegram

[101] – Filippo Valsorda – Op-Ed: I'm Throwing in the Towel on PGP and I Work In Security - https://arstechnica.com/security/2016/12/op-ed-im-giving-up-on-pgp/

[102] – Twitter (@Policy) – Global Internet Forum to Counter Terrorism - https://blog.twitter.com/official/en_us/topics/company/2017/Global-Internet-Forum-to-Counter-Terrorism.html

[103] – Joseph Cox – The Booming, and Opaque, Business of Dark Web Monitoring - https://motherboard.vice.com/en_us/article/vv7b4m/the-booming-and-opaque-business-of-dark-web-monitoring

[104] – Ryan Paul – Security Expert Used TOR to Collect Government e-mail Passwords - https://arstechnica.com/security/2007/09/security-expert-used-tor-to-collect-government-e-mail-passwords/

[105] – Seul – Holy Shit I Caught 1 - http://archives.seul.org/or/talk/Aug-2006/msg00262.html

[106] – Alex Biryukov, Ivan Pustogarov and Ralf-Philipp Weinmann – Trawling for TOR Hidden Services: Detection, Measurement, Deanonymisation - https://www.cryptolux.org/images/f/TrawlingHS.pdf

[107] – Dr. Neal Krawetz – Attacked over Tor - https://www.hackerfactor.com/blog/index.php?/archives/762-Attacked-Over-Tor.html

[108] – Ed Gent – Trackers Could Unmask Dark Web Users Who Think They're Anonymous - https://www.newscientist.com/article/2126472-trackers-could-unmask-dark-web-users-who-think-theyre-anonymous/

[109] – Vlad Tsyrklevich – Tor Browser Bundle Exploit - https://tsyrklevich.net/tbb_payload.txt

[110] – Narjas Zatat – Police Arrested 870 Suspected Paedophiles and Rescue Hundreds of Children After Smashing International Internet Ring - http://www.independent.co.uk/news/world/europe/europol-fbi-joint-investigation-operation-pacifier-uncovers-global-paedophilia-ring-870-arrests-a7722821.html

[111] – "Jonaslejon" (GitHub) – TOR Fingerprint - https://github.com/jonaslejon/tor-fingerprint/

[112] – Jose Carlos Norte - Advanced Tor Browser Fingerprinting - http://jcarlosnorte.com/security/2016/03/06/advanced-tor-browser-fingerprinting.html

[113] – Nicholas P. Fandos – Harvard Sophomore Charged In Bomb Threat - http://www.thecrimson.com/article/2013/12/17/student-charged-bomb-threat/

[114] – Roger Dingledine, Nick Mathewson and Paul Syverson – Tor: The Second-Generation Onion Router - https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf

[115] – Nick Mathewson - The Fifth HOPE (2004): How to Break Anonymity Networks - https://www.youtube.com/watch?v=oVcAI1Z0Em0

[116] – Philipp Winter – How the Great Firewall of China is Blocking TOR - https://www.cs.kau.se/philwint/gfw/

[117] – Tim Wilde – Tor Bug 4185 Testing and Report - https://gist.github.com/twilde/da3c7a9af01d74cd7de7

[118] – Andrew Reed and Michael Kranch – Identifying HTTPS-Protected Netflix Videos in Real-Time - https://www.mjkranch.com/docs/CODASPY17_Kranch_Reed_IdentifyingHTTPSNetflix.pdf

[119] – C. Aliens – Munich Gunman Got Weapon from Darknet - http://www.bbc.co.uk/news/world-europe-36878436

[120] – BBC – Munich Shooting: David Sonboly 'Planned Attack for Year' - http://www.bbc.co.uk/news/world-europe-36878436

[121] – Nick McCarthy – Man Who Bought Glock Pistol Parts on 'dark web' is Jailed - http://www.birminghammail.co.uk/news/midlands-news/man-who-bought-glock-pistol-11538095

[122] – Giacomo Persi Paoli, Judith Aldridge, Nathan Ryan, Richard Warnes – The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web - https://www.rand.org/pubs/research_reports/RR2091.html

[123] – Alan Travis – Home Deliveries of Knives Bought Online to Be Banned in UK - https://www.theguardian.com/uk-news/2017/jul/18/plans-to-make-delivery-of-knives-sold-online-to-private-addresses-illegal-knife-crime

[124] – Mark Jackson – Big UK Broadband ISPs Blocking 3,814 Internet Piracy Related URLs - http://www.ispreview.co.uk/index.php/2017/03/big-uk-broadband-isps-blocking-3814-internet-piracy-related-urls.html

[125] – "Ernesto" – The Pirate Bay Remains Resilient, 11 Years on After The Raid - https://torrentfreak.com/the-pirate-bay-remains-on-top-11-years-after-the-raid-170531/

[126] – Thomas Fox-Brewster – How The Cops Took Down an Alleged $23 Million Dark Web Drug Kingpin - https://www.forbes.com/sites/thomasbrewster/2017/07/20/dark-web-drugs-to-suicide-accused-alexandre-cazes/#5db3f1a91250

[127] – The Digital Citizens Alliance – Good Money Gone Bad - https://www.scribd.com/document/207916626/Good-Money-Gone-Bad

[128] – Zaufana Trzecia Strona – Analysing of Black Market Reloaded user database leak - https://zaufanatrzeciastrona.pl/analysis-of-black-market-reloaded-user-database-leak/

[129] – US – Criminal Complaint against Ross Ulbricht - http://krebsonsecurity.com/wp-content/uploads/2013/10/UlbrichtCriminalComplaint.pdf

[130] – The Grugq – It Was DPR, in the TOR HS, With the BTC - http://grugq.github.io/blog/2013/10/09/it-was-dpr/

[131] – Brian Krebs – Feds Arrest Alleged 'Silk Road 2' Admin, Seize Servers - https://krebsonsecurity.com/2014/11/feds-arrest-alleged-silk-road-2-admin-seize-servers/#more-28608

[132] – US – Criminal Complaint Against Alexander Cazes - https://www.justice.gov/opa/press-release/file/982821/download

[133] – Alois Afilipoaie and Partick Shortis – Silk Road: After being closed twice, can the brand ever 'rise again' - https://www.swansea.ac.uk/media/GDPO%20SA%20silk%20rd%20rise%20again.pdf

[134] – Scott W. Duxbury and Dana L. Haynie – The Network Structure of Opioid Distribution on a Darknet Cryptomarket - https://link.springer.com/article/10.1007/s10940-017-9359-4

[135] – Joseph Cox – This Is How Cops Trick Dark-Web Criminals Into Unmasking Themselves - http://www.thedailybeast.com/this-is-how-cops-trick-dark-web-drug-dealers-into-unmasking-themselves

[136] – pxx51092 – Don't Open the XLSX LockTime File Beacon Image - https://www.reddit.com/r/DankNation/comments/6pi0et/dont_open_the_xlsx_locktime_file_beacon_image/

[137] – Robert Tait – Censorship Fears Rise as Iran Blocks Access to Top Websites - https://www.theguardian.com/technology/2006/dec/04/news.iran

[138] – linkcabin – Content-Location Header Dream Marketplace - https://twitter.com/LinkCabin/status/902840529456693249

[139] – linkcabin – Static CSRF Tokens, Dark Marketplace Forums and Salt - https://itsjack.cc/blog/2017/09/static-csrf-tokens-dark-marketplace-forums-and-salt/

[140] – Google – Announcing the Frist SHA1 Collision - https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html

[141] – Alex Hern – Online Drugs Marketplace Shutdown Bitcoin Hack - https://www.theguardian.com/technology/2013/dec/03/online-drugs-marketplace-shut-down-bitcoin-hack-sheep

[142] – DEEPDOTWEB – Sheep Marketplace Owner Arrested - https://www.deepdotweb.com/2015/03/27/breaking-sheep-marketplace-owner-arrested/

[143] – Matthew Prince – Why We Terminated Daily Stormer - https://blog.cloudflare.com/why-we-terminated-daily-stormer/

[144] – Southern Poverty Law Center – Stormfront, the leading white supremacist Web forum, has another distinction – murder capital of the internet - https://www.splcenter.org/20140401/white-homicide-worldwide

[145] – Lachesis – Scallion (GitHub) - https://github.com/lachesis/scallion

[146] – Nick Mathewson – Next Generation Hidden Services in TOR - https://gitweb.torproject.org/torspec.git/tree/proposals/224-rend-spec-ng.txt

[147] – Yonathan Klijnsma – Tor2Web Cryptocurrency Mining - https://twitter.com/ydklijnsma/status/912646059045851136

[148] – John Leyden – Former GCHQ Boss Backs end-to-end Encryption - https://www.theregister.co.uk/2017/07/10/former_gchq_wades_into_encryption_debate/