**ABSTRACT**

The Dark Web is at the centre of the debate over whether online anonymity should be maintained in spite of the illegal activity that it enables. Policy-makers must gain an understanding of the Dark Web in order to engage intelligently in the debate and enact effective Dark Web policy. This paper aims to provide context and policy recommendations pertaining to the Dark Web based on open-source research. The Dark Web’s complete history, from its creation to the latest incidents of government intervention, remains relevant to today’s debate. By examining cases where a government agency has enforced laws on the Dark Web, one can glean an understanding of which policies will be most successful going forward. This paper explores specific policy topic is exploring the most effective and reasonable methods. As the United States develops and refines policy regarding the Dark Web, the international community will also be manoeuvring to put in place regulations, and it is essential that these regulations be compatible while staying true to the values of the internet users that those governments serve.

# 

|  |  |  |
| --- | --- | --- |
| **S NO** | **INDEX**  **CONTENTS** | **PAGE NO** |
| 1 | Introduction | 1 |
| 2 | History | 3 |
| 3 | What is Dark Web | 4 |
| 4 | How to Access Dark Web | 5 |
| 5 | Applications | 8 |
| 6  7 | Advantages  Disadvantages | 12  13 |
| 8  9 | Conclusion  References | 14  15 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 1. INTRODUCTION

If you’re into computer security at all you may have heard of terms like “Deep Web” and “Dark Web”.

The terms can be confusing so here are the basics:

* **The Internet:** This is the easy one. It’s the common Internet everyone uses to read news, visit Facebook, and shop. Just consider this the “regular” Internet.
* **The Deep Web:** The deep web is a subset of the Internet that is not indexed by the major search engines. This means that you have to visit those places directly instead of being able to search for them. So, there aren’t directions to get there, but they’re waiting if you have an address. The Deep Web is largely there simply because the Internet is too large for search engines to cover completely. So, the Deep Web is the long tail of what’s left out.
* **The Dark Web:** The dark web is the World Wide Web content that exists on darknets, overlay networks which use the public Internet but require specific software, configurations or authorization to access. The dark web forms a small part of the deep web, the part of the Web not indexed by search engines, although sometimes the term "deep web" is mistakenly used to refer specifically to the dark web.

Page 1

* **Surface Web**
* 4% of WWW content
* Also, known as the ‘Visible Web’, it is content that can be found using search engines such as Google or Yahoo. It is under constant surveillance by the government.
* **Dark Web**
* 96% of WWW content
* Also, known as the ‘Invisible Web’, it is the content that cannot be indexed by search engines. And it is hard to keep track of.

According to the calculations in the year of 2003, The Dark Web is estimated to be at least 500x the size of the Surface Web.

# What-is-Dark-Web.png

Page 2

# 2. HISTORY

The web we all know and love is also known as the **‘surface web’**. This is because lurking below the surface is a much deeper place which includes the darkweb.

The **‘darkweb’** is so called because it has been built to hide portions of the Internet from everyday users. Sometimes, the darkweb gets confused with the **‘deep web’,** so we will discuss both here to differentiate them from one another. But first, a little history.

The idea of ‘dark’ parts of a connected network began life not long after the nascent internet. **Timeline of DarkWeb :**

* 2002 – Tor Network developed by US Naval Researchν Laboratory
* 2003 – The I2P peer-to-peer network developedν
* 2006 – Tor becomes a non-profit organizationν
* 2009 – “Satoshi Nakamoto” started Bitcoin digital currencyν
* 2011 – Silk Road Market launchesν
* 2012 – Experts estimate earnings of $22M for SRν
* 2013 – Silk Road shut down (earningsν > $1B)
* 2014 – Other dark web markets proliferate (Agora, Evolution)ν
* 2015 – Ross Ulbricht sentenced to life; Evolution exit scamν.

Page 3

# 3. WHAT IS DARKWEB

The Dark Web (also called Darknet) is a subset of the Deep Web that is not only not indexed, but that also requires something special to be able to access it, e.g., specific proxying software or authentication to gain access. The Dark Web often sits on top of additional sub-networks, such as Tor, I2P, and Freenet, and is often associated with criminal activity of various degrees, including buying and selling drugs, pornography, gambling, etc.

While the Dark Web is definitely used for nefarious purposes more than the standard Internet or the Deep Web, there are many legitimate uses for the Dark Web as well. Legitimate uses include things like using Tor to anonymize reports of domestic abuse, government oppression, and other crimes that have serious consequences for those calling out the issues.

Common Dark Web resource types are media distribution, with emphasis on specialized and particular interests, and exchanges where you can purchase illegal goods or services. These types of sites frequently require that one contribute before using, which both keeps the resource alive with new content.

# 1574675064_Image4.jpg

Page 4

# 4. HOW TO ACCESS DARKWEB

What you want to access are sites using the Tor Hidden Service Protocol. It works over regular Tor (anonymity network), but instead of having your traffic routed from your computer and through an onion-like layer of servers, it stays within the Tor network. You won't know exactly what system you're accessing unless they tell you, and they won't know who you are unless they do - or unless one of you is careless.

**Step 1:**

* Go and get yourself a good VPN (Virtual Private Network), use it ALL of the time, no matter if you are on TOR or not. This site here reviews the best VPN’s for use with TOR.
* You should be taking your anonymity and security very seriously if you are visiting the Dark Web, especially if you are viewing any Darknet Markets.
* What’s even better is that the VPN will give you a fake IP address, in another country if you like, so even if Tor is compromised then the trace just leads back to somewhere else that can’t be linked to you.
* The other benefit of using a VPN is to prevent hackers stealing your identity and or personal files and photos from your computer.
* You need to use a good VPN that keeps NO LOGS, fast performance, preferably accepts bitcoin as payment, has a kill switch for DNS leaks, and is compatible with TOR.
* Then install your VPN, if you buy the better VPN’s then it is usually just a one click install and one or two clicks to turn it on.

Page 5

**Step 2:**

* You can’t access the deep web just using a common browser like Internet Explorer or Google Chrome. To get dark web access you will need to download the dark web browser called TOR browser bundle. Only get it from the official TOR website from your favorite browser, never download it from anywhere else!
* Now close all of your browsing windows and all apps connecting to the internet like Google Drive, Skype, OneDrive, iCloud etc.
* Then open your VPN app and connect to another location other than where you are at, make sure to use the OpenVPN protocol as it is the most secure.

**Step 3:**

* Install the TOR browser bundle on your PC or Mac. When the download is complete, double-click the downloaded file, choose the destination folder (the folder where you want to extract tor browser), and choose extract.

**Step 4:**

* Start TOR Browser. Open the folder where you extracted TOR browser and double-click “Start Tor Browser”. The TOR start page will open in a browser. From here, you now have a good level of anonymity and security and you are able to gain access to .onion websites through your dark web browser.

**Step 5:**

* DO NOT change the TOR browser window size unless you like living dangerously. The FEDS have programs that can match identities on random things such and matching time online and other things with the browser window size, I shit you not. If you don’t change the size, then it is the same as most other people.

Page 6

**Step 6:**

* Please remember that TOR isn’t necessarily 100% anonymous, you should turn off JavaScript within the dark web browser settings to help.

**Step 7:**

* Disconnect your webcam or block the camera with some black tape. Hackers and governments have ways of getting into your computer and turning on the video and cameras.

**Step 8:**

* Disconnect your microphone or cover it with tape to muffle it good. The same goes for the microphone as the camera, the last thing you want is to be recorded saying incriminating things at home. It doesn’t even have to be while on the dark web.

**Step 9:**

* NEVER use your real name, photos, email, or even password that you have used before on the dark web. This is the fastest way to be tracked. Use an anonymous email account and aliases that have nothing to do with you that you have never used before.

**Step 10:**

* If you are using TOR on the dark web for anything other than looking at cute pictures of kittens, you should think seriously about your privacy and security. Jolly Roger has put together a comprehensive guide on how to stay safe on the deep web.

Page 7

**5. APPLICATIONS**

The following breakdown of content by an alternative category set, highlighting the illicit use of .onion services.

### Botnets :

[Botnets](https://en.wikipedia.org/wiki/Botnet) are often structured with their [command-and-control](https://en.wikipedia.org/wiki/Command_and_control_(malware)) servers based on a censorship-resistant hidden service, creating a large amount of bot-related traffic.

### Bitcoin Services:

[Bitcoin](https://en.wikipedia.org/wiki/Bitcoin) services such as [tumblers](https://en.wikipedia.org/wiki/Cryptocurrency_tumbler) are often available on [Tor](https://en.wikipedia.org/wiki/Tor_(anonymity_network)), and some such as [Grams](https://en.wikipedia.org/wiki/Grams_(search)) offer darknet market integration. A research study undertaken by Jean-Loup Richet, a research fellow at [ESSEC](https://en.wikipedia.org/wiki/ESSEC), and carried out with the [United Nations Office on Drugs and Crime](https://en.wikipedia.org/wiki/United_Nations_Office_on_Drugs_and_Crime), highlighted new trends in the use of Bitcoin tumblers for [money laundering](https://en.wikipedia.org/wiki/Money_laundering) purposes. With Bitcoin, people can hide their intentions as well as their identity. A common approach was to use a [digital currency exchanger](https://en.wikipedia.org/wiki/Digital_currency_exchanger) service which converted Bitcoin into an online game currency that will later be converted back into money.

### Darknet Markets :

Commercial [darknet markets](https://en.wikipedia.org/wiki/Darknet_market), which mediate transactions for [illegal drugs](https://en.wikipedia.org/wiki/Illegal_drugs) and other goods, attracted significant media coverage, starting with the popularity of [Silk Road](https://en.wikipedia.org/wiki/Silk_Road_(marketplace)) Market.Other markets sell [software exploits](https://en.wikipedia.org/wiki/Exploit_(computer_security)) and weapons. Examination of price differences in Dark web markets versus prices in World Wide Web was performed on Evolution, one of the most popular [crypto-markets](https://en.wikipedia.org/wiki/Cryptomarkets) active from January 2013 to March 2015.

Page 8

### Hacking Groups and Services:

# Many [hackers](https://en.wikipedia.org/wiki/Hacker_(computer_security)) sell their services either individually or as a part of groups. Such groups are [xDedic](https://en.wikipedia.org/wiki/XDedic), hackforum, Trojanforge, [Mazafaka](https://en.wikipedia.org/wiki/Mazafaka_(hacker_group)), [dark0de](https://en.wikipedia.org/wiki/Dark0de) and the [TheRealDeal](https://en.wikipedia.org/wiki/TheRealDeal) darknet market. Cyber crimes and hacking services for financial institutions and banks have also been offered over the Dark web. Use of Internet-scale DNS Distributed Reflection Denial of Service (DRDoS) attacks have also been made through leveraging the Dark Web. There are many scam .onion sites also present which end up giving tools for download that infected with trojan horses or backdoors.

### Financing :

Scott Dueweke the president and founder of Zebryx Consulting states that Russian electronic currency such as WebMoney and Perfect Money are behind the majority of the illegal actions. In April 2015, Flashpoint received 5 million in funding to invest to help their clients gather intelligence from the Deep and Dark web.

### Fraud Services :

There are numerous [carding](https://en.wikipedia.org/wiki/Carding_(fraud)) [forums](https://en.wikipedia.org/wiki/Crime_forum), [PayPal](https://en.wikipedia.org/wiki/PayPal) and [Bitcoin](https://en.wikipedia.org/wiki/Bitcoin) trading websites as well as fraud and counterfeiting services. Many such sites are scams themselves.

### Hoaxes and unverified content :

There are reports of [crowdfunded assassinations](https://en.wikipedia.org/wiki/Assassination_market) and [hitmen](https://en.wikipedia.org/wiki/Hitmen) for hire, however, these are believed to be exclusively scams. The creator of [Silk Road](https://en.wikipedia.org/wiki/Silk_Road_(marketplace)), [Ross Ulbricht](https://en.wikipedia.org/wiki/Ross_Ulbricht), was arrested by Homeland Security investigations (HSI) for his site and allegedly hiring a hitman to kill six people, although the charges were later dropped.

Page 9

### Phishing and Scams :

[Phishing](https://en.wikipedia.org/wiki/Phishing) viacloned websites and other [scam](https://en.wikipedia.org/wiki/Confidence_trick) sites are numerous, with [darknet markets](https://en.wikipedia.org/wiki/Darknet_market) often advertised with fraudulent URLs.

### Puzzles :

Puzzles such as [Cicada 3301](https://en.wikipedia.org/wiki/Cicada_3301) and successors will sometimes use hidden services in order to more anonymously provide clues, often increasing speculation as to the identity of their creators.

### Illegal Pornography :

There is regular [law enforcement](https://en.wikipedia.org/wiki/Law_enforcement) action against sites distributing [child pornography](https://en.wikipedia.org/wiki/Child_pornography) often via compromising the site by distributing [malware](https://en.wikipedia.org/wiki/Malware) to the users. Sites use complex systems of guides, forums and community regulation. Other content includes [sexualised torture and killing of animals](https://en.wikipedia.org/wiki/Crush_fetish)and [revenge porn](https://en.wikipedia.org/wiki/Revenge_porn).

### Terrorism :

There are at least some real and fraudulent websites claiming to be used by [ISIL](https://en.wikipedia.org/wiki/Islamic_State_of_Iraq_and_the_Levant) (ISIS), including a fake one seized in [Operation Onymous](https://en.wikipedia.org/wiki/Operation_Onymous). In the wake of the [November 2015 Paris attacks](https://en.wikipedia.org/wiki/November_2015_Paris_attacks), an actual such site was hacked by an [Anonymous](https://en.wikipedia.org/wiki/Anonymous_(group))-affiliated hacker group, [GhostSec](https://en.wikipedia.org/wiki/Ghost_Security), and replaced with an advert for [Prozac](https://en.wikipedia.org/wiki/Prozac). The [Rawti Shax](https://en.wikipedia.org/wiki/Rawti_Shax) Islamist group was found to be operating on the dark web.

### Social Media :

Within the dark web, there exist emerging social media platforms similar to those on the WWW.  [Facebook](https://en.wikipedia.org/wiki/Facebook) and other traditional social media platforms have begun to make dark-web versions of their websites and to continue their service in all areas of the WWW.

Page 10

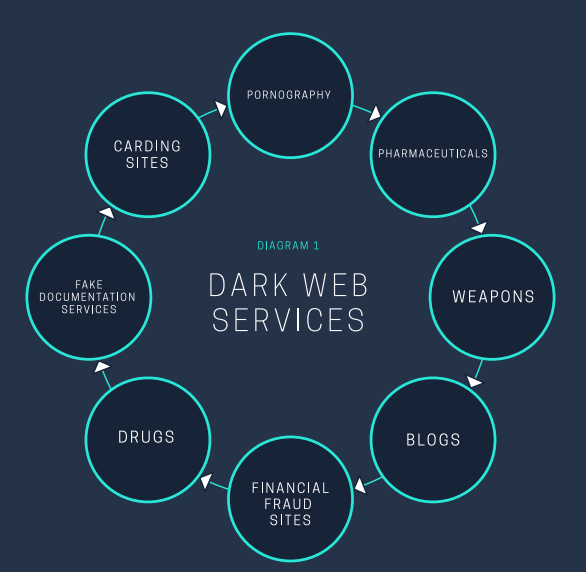
**Things You Can Buy :**

1. Drugs
2. Counterfeit Currency
3. Forged Papers
4. Firearms, Ammunition, and Explosives
5. Hitmen
6. Human Organs

**Things That Make Internet Crime Work :**

1. Cryptocurrency
2. Bulletproof Web-hosting Services
3. Cloud Computing
4. Crimeware
5. Hackers for Hire
6. Multilingual Crime Call Centers

Page 11



**6. ADVANTAGES**

The dark web helps people to maintain privacy and freely express their views. Privacy is essential for many innocent people terrorized by stalkers and other criminals. The increasing tendency of potential employers to track posts on social media can also make it difficult to engage in honest discussions publicly. Finally, the popularity of the dark web with criminals makes it a perfect way for undercover police officers to communicate.

Many are for hackers, writers, and people concerned about censorship. So, the major draw of the dark web is a sense of community and freedom that some don't feel on the surface web.

Some other advantages are:

1. Anonymity
2. Freedom of Speech
3. Political Activism
4. More Knowledge gain
5. Amazing individuals
6. You can publish & do anything
7. You can’t fear
8. Open banned websites also

Page 12

**7. DISADVANTAGES**

The dark web empowers ordinary people, but some people will inevitably abuse that power. The dark web can make it easier to commit some of the worst crimes. For example, the combination of the dark web and cryptocurrencies theoretically makes it much easier to hire someone to commit a murder. While the dark web promises privacy to its users, it can also be used to violate the privacy of others. Private photos, medical records, and financial information have all been stolen and shared on the dark web.

The deep web may sound like a dangerous place to venture and, to be brutally honest; the everyday person can live in complete ignorance of it and still be perfectly content. However, it does have some (legal) practical uses.

Some other disadvantages includes:

1. Hoaxes and unverified content
2. Phishing and scams
3. Illegal and ethically disputed pornography
4. Terrorism
5. Deep Web doesn’t work smoothly
6. Slow campare to our normal browsers
7. Hacking is fastly grown

Page 13

**8. CONCLUSION**

The Dark Web networks such as TOR have provided many possibilities for malicious actors to exchange legal and illegal “goods” anonymously. Dark Web is a growing asset, especially in terms of the illicit services and activities. Security mechanisms should be vigilant to these problems and take measures to eliminate them. The evolving technology with encryption (security) and anonymity (like the Dark Web and its special software) has put law enforcement and policymakers in challenge to effectively struggle harmful actors who are operating in the cyberspace.

The deep web will continue to perplex and fascinate everyone who uses the internet. It contains an enthralling amount of knowledge that could help us evolve technologically and as a species when connected to other bits of information. And of course, it’s darker side will always be lurking too, just as it always does in human nature.

The deep web speaks to the fathomless, scattered potential of not only the internet, but the human race, too. Regardless of if the Dark Web exists or not, the aforementioned activities still occur. The Dark Web just provides an easy way to connect with people of similar interests, and to facilitate further interaction.

Page 14

**9. REFERENCES**

Page 15

1. NPR Staff (25 May 2014). ["Going Dark: The Internet Behind The Internet"](https://www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet). [Archived](https://web.archive.org/web/20150527071850/http:/www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet) from the original on 27 May 2015. Retrieved 29 May 2015.
2. Greenberg, Andy (19 November 2014). ["Hacker Lexicon: What Is the dark web?"](https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/). Wired. [Archived](https://web.archive.org/web/20150607062159/http:/www.wired.com/2014/11/hacker-lexicon-whats-dark-web/) from the original on 7 June 2015. Retrieved 6 June 2015.
3. ["Clearing Up Confusion – Deep Web vs. dark web"](http://www.brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/). BrightPlanet. 2014-03-27. [Archived](https://web.archive.org/web/20150516160539/http:/www.brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/) from the original on 2015-05-16.
4. Greenberg, Andy (19 November 2014). ["Hacker Lexicon: What Is the dark web?"](https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/). Wired. [Archived](https://web.archive.org/web/20150830233549/http:/www.wired.com/2014/11/hacker-lexicon-whats-dark-web) from the original on 30 August 2015. Retrieved 27 August 2015.
5. Egan, Matt (12 January 2015). ["What is the dark web? How to access the dark website – How to turn out the lights and access the dark web (and why you might want to)"](http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-3593569/). [Archived](https://web.archive.org/web/20150619001447/http:/www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-3593569/) from the original on 19 June 2015. Retrieved 18 June 2015.
6. ["Clearnet vs hidden services – why you should be careful"](https://web.archive.org/web/20150628204337/https:/www.deepdotweb.com/jolly-rogers-security-guide-for-beginners/clearnet-vs-hidden-services-why-you-should-be-careful/). [DeepDotWeb](https://en.wikipedia.org/wiki/DeepDotWeb). Archived from [the original](http://www.deepdotweb.com/jolly-rogers-security-guide-for-beginners/clearnet-vs-hidden-services-why-you-should-be-careful/) on 28 June 2015. Retrieved 4 June 2015.
7. Chacos, Brad (12 August 2013). ["Meet Darknet, the hidden, anonymous underbelly of the searchable Web"](http://www.pcworld.com/article/2046227/meet-darknet-the-hidden-anonymous-underbelly-of-the-searchable-web.html). PC World. [Archived](https://web.archive.org/web/20150812065847/http:/www.pcworld.com/article/2046227/meet-darknet-the-hidden-anonymous-underbelly-of-the-searchable-web.html) from the original on 12 August 2015. Retrieved 16 August 2015.
8. Beckett, Andy (26 November 2009). ["The dark side of the internet"](https://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet). [Archived](https://web.archive.org/web/20130908073158/http:/www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet) from the original on 8 September 2013. Retrieved 9 August 2015.