TEAM LEADER
DANIEL SAMEH

Hu111: Technical Report writing
Submit to: Dr.Ihab El-Khodary
Leader: Daniel Sameh Kamal

Faculty of Computers and Artificial Intelligence – Cairo University

Phase 5

Group ID: 4

Project Title

The Layers of the Internet: Deep Down to the Dark web

Student Name	ID
Daniel Sameh Kamal	20221050
Abdelaziz Ali Ahmed Ali El-Araby	20220198
Abdallah Muhammed Abdallah	20220204
Abdelmonaem Mahmoud Abdelmonaem	20220206
Habiba Mohammed Ahmed Shawkey	20220106
Jonathan Mokhles William	20220100
Youssef Ihab William	20220388
Mennatallah Ali Amin	20221225

Table of contents:

Introduction 1

1. Basic knowledge about the internet 2

1.1. Layers of the internet 2

1.1.1. Surface web 2

1.1.2. Deep web 4

1.1.3. Dark web 5

1.2. Difference between deep web and dark web 7

2. The origin and history of the dark web 8

2.1. Creation of the dark web: 9

2.1.1. U.S department of defense and ARPANET attempts. 9

2.2. Initial purpose of the dark web 11

2.2.1. Providing anonymity 11

2.2.2. Browsers of anonymity 11

2.2.2.1. Tor browser 11

2.3. Deprivation of the initial purpose 14

2.3.1. The appearance of the first dark net market: Silk Road 14

2.3.2. Arise of crimes 14

2.3.3. Silk Road's shutdown 15

3. Dark web is properly named 16

3.1. Criminal activities on the dark web 16

3.1.1. How are they widely spread on the dark net's platforms? 16

3.1.2. Why is it so hard to stop these activities? 18

4. Contributions towards stopping these illegal activities 20

4.1. FBI's contributions 20

4.2. Operation DisrupTor 21

4.3. Government's contributions 23

5. Dark web and cybersecurity 24

5.1. What is Cyber Security? 24

5.1.1. What is Ethical Hacking? 24

5.2. What does the dark web mean for cybersecurity? 25

5.3. The Relation between Dark web and cyber security 26

5.3.1. Why are cybersecurity experts interested in the dark web? 26

5.3.2. Some ways that cybersecurity professionals use to enhance the security of systems 26

5.3.3. Some the tools that network admins use to monitor the dark web 27

5.3.4. Dark Web Scanners 27
5.4. Personal information and dark web 29
6. Bright side of the dark web 30
6.1. Anonymity 30
6.2. knowledge 31
6.3. Cybersecurity (hiding information) 31
7. Dark web trap 32
7.1. Instances of famous people being hacked 32
7.2. Vulnerabilities exploited by hackers 33
7.3. Examples of security used by Google 33
7.4. Protection against hacking 34
7.5. Methods of defending oneself from hacking 34
Conclusion 36
Recommendations 37
References 38

Table of illustrations:

Figure 1: Iceberg of the internet 2
Figure 2: OSINT 3
Figure 3: TLD 4
Figure 4: Events timeline of the internet and the dark web 8
Figure 5: Tor browser 11
Figure 6: Onion routing 12
Figure 7: Tor nodes 12
Figure 8: What silk road looks like 16
Figure 9: ross Ulbricht 17
Figure 10: Silk Road payment system 17
Figure 11: Steven W. Chase 18

Summary:

As the addiction to the internet has been implemented into us and a day without it cannot be imaginable, it is pretty amusing how our brains do not get us to think about the thing that we waste our life and time on. People may think that the internet is limited to the pages used in their day-to-day activities, but it is much deeper than what any mind could imagine. As a regular user, the internet is the tool that helps get work done, but have you ever looked at what is behind it, the mechanism of working, the different layers, the methodologies, and history. Throughout this report, we will go through these points to help in learning, be aware of what is being used, and keep yourself as safe as possible. Moreover, it will focus especially on the dark web, and everything related to it.

This report discusses the three different layers of the internet, which are: Surface web, Deep web, and Dark web. We focused mainly on the dark web as it is an anonymous thing, and it is known that humans, by nature, tend to something that is unknown. Besides, it is pretty dangerous to enter the dark web, so we gave you the safest option to fulfill your curiosity. We will know what they are, what you are going to find inside each one, their methodologies and framework, how to access them, how we could benefit from them, etc. After that history and origins of the dark web will be discussed. We will walk through the creation process and know why it was initially created. Also, we will discuss how it can provide anonymity and what the things that could provide this feature are. At the end of this part, we will know why the dark web was deprived of its initial purpose, how, and the crimes raised from it. Other things that will be mentioned are criminal activities that take place on the dark web, why it is widely spread, and why it is so hard to stop them. The next part will mention the different contributions to stopping illegal activities and how they succeeded.

For sure, we cannot mention the dark web without mentioning its relationship with cybersecurity. We will understand the relationship between both and what they mean to each other. Even though it might appear that we are mentioning the dark points of the dark web, next will be the benefits of the dark web and why its existence is essential. Lastly, we will walk you through the steps of how to keep yourself safe from falling into the trap of the dark web and ways of protection.

To sum up, this report can be your guide to understanding the internet world, help you understand the undiscovered and unpopular part of the internet, which is the dark web, and finally, be able to save yourself and your information from any hacking attempt.

Introduction:

According to the NAOS organization, it has been reported that in 2022 Egyptians spent about 8h02 per day using the internet, which is above the average of 6h58. This is 1/3 of your day, not including the time of internet usage inside the workplace or for educational purposes. Even though there will be 4.9 billion active internet users in 2022, only a small percentage could really understand the internet, its framework, methodology, and how to use it safely. According to the Pew research center, only 24% could understand what private browsing is. This percentage is pretty weird, as the internet is taking control of most of the activities that we are doing in our lives, but at the same time, we need to be fully aware of what is behind the pages that we are scrolling through. Also, this unawares could put the user in dangerous situations like hacking or identity thieving. In 2019 alone, 1.76 billion records have been stolen. There are many other activities which we use daily, and without any awareness, it may cause the leaking of our information and data into non-confidential websites.

Most of us think that the internet is limited to the pages that we access while searching for information, but it is only a point in the deep ocean of the internet. This is why we wrote this report, to be your guide in the discovery journey of the different layers of the internet. This report aims to provide all the needed details about the different layers of the internet and to dive more specifically into the dark web. It will give a closure look to help learn about the dark web, its framework, primary purpose, history, ways of accessing, etc.

Throughout this report, we tried to give you a complete look at everything you might need to know or learn about on the internet. First, the difference between each layer of the internet will be presented, and you will know the ways of accessing, the browsers you need, their purpose, working methodologies and their applications. After that, we will dive deeper to explore the anonymous and most dangerous layer of the internet, which is the dark web. We tried to break it into different pieces, as you will learn from each different chapter thing. We started from the initial purpose of initiation to what the dark web looks like from the inside and what you would expect to find. We have been able to collect all of this information through different reports, documentaries, and journals from people who have been observing the working mechanism of the dark web for years and by accessing the dark web to give you the closure look that you have been trying to get but in a much safer way.

1. Basic knowledge about the internet:

1.1. Layers of the internet:

As human beings and to what has been obligated to us, it has been a must to use the internet daily. This obligation made everything obey the force of change; whether in studying, working, or even having fun. This change provided a corner for each one on the internet to find what attracts them; despite their interests, needs, or beliefs. But have you ever questioned yourself about the working methodology of the internet or what it looks like behind the content that you could access easily? In fact, layers of the internet go way far ahead of the simple and surface content that appears to you while searching. There is a much bigger layer of material that isn't accessible through traditional online searching methods. It is pretty similar to what experts have noted: these days, searching on the internet could be compared to dragging a net across the ocean. It doesn't matter the great deal that you might catch on the net, there is still a wealth of information that is much deeper, and as a result, wasted. Moving along this report, the unknown part will be discovered. The hidden layers will be revealed, their functions, their history, working methodologies, etc.

We will walk through the layers of the internet; it is more like the iceberg. The top part is the surface web which is the most commonly used in our daily research. The second part of the iceberg is the deep web, it isn't as cool as the name might infer but we can say that it contains all of our information on the internet. The last part is the dark web. From its name, it is easy to call that it is very dangerous.

Figure 1: Iceberg of the internet

From this small description, a small picture might be drawn into your mind but still not all the details have been presented to draw the big one. Each point will be presented solely so that all the information can be

1.1.1. Surface web:

Surface web (also known as the visible web) – the tip of the iceberg, that is visible to all internet users. This layer is completely searchable and indexable, and hence visible to anyone using a suitable search engine. It is the layer, which is mostly used in day-to-day activities, like social networking, working, and studying. The surface web includes everyday websites and online services, such as e-commerce sites, blogs, governmental portals, educational sites, and much more. So, anything you can search about and get answers for it through links is the surface web. You can access it easily through standard search engines like Google, Firefox, yahoo, Bingo, etc.

Even though the surface web might include everything that we use on the internet but in real fact, it contains 130 trillion pages of search services which represent only 4% of the entire web.

Believe it or not, the surface web is home to some of the deep web. This is because when any web page requires credentials for access technically is part of the deep web as search engines cannot access this content.

Even though the surface web seems pretty harmless but as known that everything on the internet has a dark side. Through the surface web, there are a handful of downsides, which include but are not limited to human exploitation, violence, distraction, identity theft, stalking, and hacking.

Another thing that is tremendously important to learn about is surface web intelligence. Before starting on illustrating surface web intelligence and its applications, a smaller topic must be studied first to walk us to the main point, which is OSINT.

OSINT (Open-Source Intelligence) is the process, tools, and techniques used to collect data from the surface web. OSINT techniques provide insights into exposed endpoints, the latest threat research, and more resources which are often shared publicly.

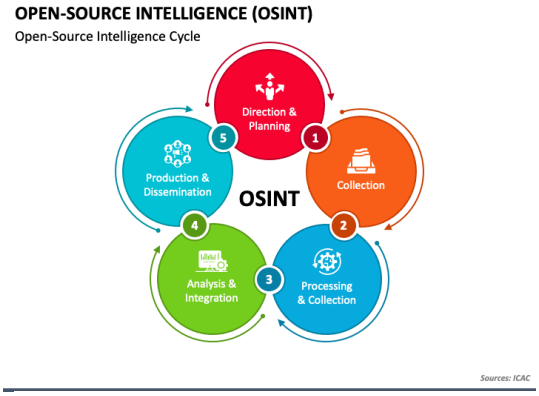

Figure 2: OSINT

The applications of Surface web intelligence include the following:

- Gathering information on the actions of cybercriminals
- Observing public security forums
- Monitoring platforms for threat intelligence exchange
- Keeping an eye out for attack announcements and notifications on social media
- Combating new or existing cyber threats
- Using asset naming conventions to monitor phishing pages
- Monitoring a specific piece of malware, rogue software, or a botnet that is targeting the organization
- Gathering information on threat attack pathways that are geographically, commercially, and infrastructure-specific
- Monitoring social media for reporting on security issues
- Monitoring third-party exposure risk and insider threat
- Activities to control business risk
- Checking for commercial and physical risks
- Keeping an eye out for mentions of the company name, high-ranking employees, email addresses, trademarks, copyrights, and sensitive assets
- Tracking the spread of false information about the organization
- Keeping an eye out for the customer and employee fraud
- Observing shady workers

From all of this, we can conclude that the surface web provides us with the daily internet activities and services that we might need. It can be accessed from any suitable search engine. It has its own black side but also, helps in gathering a lot of information and details from different sides and tracking important information.

1.1.2. Deep web:

Moving to the next part of the iceberg; the deep web. It represents 90% of all websites. As cool as it might sound but it is not that dangerous. Yes, it is from the invisible part of the iceberg and may connect someway with the dark web, but still didn't go that deep enough to be considered vicious. Contradicting from the surface web, the deep web isn't accessible with normal search engines. In other words, it cannot be accessed by normal internet users, as the data provided in it isn't crawled and indexed by search engines. The content of the deep web is hidden behind HTTP forms, which assist in its function.

The type of data stored in the deep web varies from personal information (military, cloud, and organization data) to financial records, academic databases, legal dossiers, medical records, social media profile information, and scientific government records. Another form of data presented on the deep web is online pages that might end with .com, .edu, and .gov because they don't use common top levels domains (TLDs).

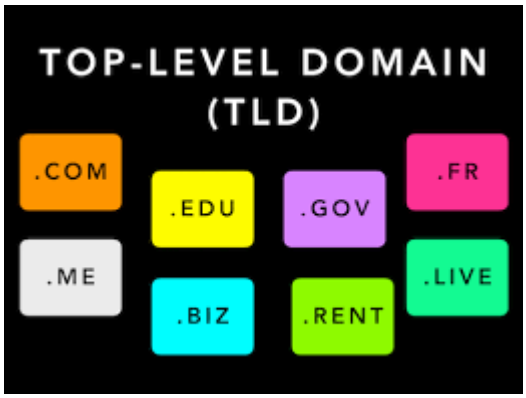

Figure 3: TLD

Users must log in with specific credentials, and have a specific URL, or IP address to access a particular service.

Here are some examples to make the picture clearer:

- When you use your credit card to buy something online, it directs you to other page after entering a specific code.
- When you try to login into your Facebook account, it acquires you to enter specific credentials in order to log in.

After familiarizing with the definition and working methodology of the deep web, discussing the accessibility to the deep web will be opened.

As mentioned, in order to access a personal bank account will need a PIN or OTP, this is pretty similar to accessing the deep web. A special authorization or access credentials will be needed and that's it.

Here are different ways to access the deep web:

- People search engines: MyLife and Pipl extract data from databases that traditional search engines cannot index.
- Scholarly articles: search engines such as Google Scholar, Library of Congress, and JSTOR enable searching through otherwise-isolated records of articles and books, providing access to the deep web's academic section.
- Look for the database: A ‘searchable' database may contain 'hidden' information. In such cases, try describing the "type" of information on a standard search engine like Google. You may be able to access information not otherwise available on the Deep Web if you find that database

If you are considering that the deep web is anonymous, in fact, sometimes it is not. This is because there are certain sites that are observed by law enforcement agencies. And sometimes, you might

be at risk of being targeted by hackers. There is 100 billion dollars' worth of illegal activity conducted worldwide using the deep web. So, for future reference, try to keep your information as safe as possible, try to update your password and make it strong, clear all the cookies from your browser, and don't access untrusting websites.

To sum up everything, the deep web is not that dangerous yet, the data in it is not visual or accessible to anyone. It also acquires special search engines in order to be accessed. It stores personal information, financial information, passwords, medical records, etc. There are different ways to access the deep web, you just need to choose the way that will provide you with the data that you are looking for. And finally, even if it might seem pretty harmless, you may fall into the trap of the deep web so, try to be safe.

1.1.3. Dark web:

Whenever the word dark web pops up in your mind, the word dangerous is directly linked with it. And this imagination is right. Its reputation has been associated with criminal intent and illegal content. It is a place where criminals, predators, spies, drug dealers, and even human traffickers may exist and hide in. Even though it is not illegal to access the dark web, but it is pretty dangerous and acquire lots of procedures in order to access it safely.

The Dark web represents a smaller percentage than the surface web and can be visually represented as the bottom tip of the submerged iceberg. It cannot be accessed with normal search engines as it is not indexed, it requires special software and an anonymizing browser with a suitable decryption key in order to be accessible.

The idea behind the dark web is to provide complete anonymity for you and have a completely encrypted network, and this is why it has been made: to protect the sensitive communications of US spies and give journalists the anonymity to read and write articles that aren't commonly discussed but still important to be shared. But this initial purpose has changed, and the perk of anonymity became a weapon with two edges. People have been using the anonymity feature as a cover to hide under it either to sell prohibited things like drugs, weapons, fake identities, child pornography, and even human organs or just to cover their hacking activities.

To dig in deeper, how to access the dark web will be discussed. As said that in the deep web you just need to have the login credentials or the right IP address, here it is totally different. First, accessing the right search is the first step. Onion, Tor, or I2P could be used. In this visualization. Onion browser will be used:

- Enter onion.ws in the search bar
- Find the raptor hyperlink and copy its link and don't press on any of the other links.
- Delete the ws and https from the hyperlink to the website.
- Choose any link which doesn't have a C beside it, as the C refers to Clearnet and will direct you out of the dark web pages.

For reference, it is totally not safe to access the dark web, the device being used for a process like this might get hacked, your IP address might get tracked, and other scenarios that any of them won't end up well. This report aims to help in learning and safely fulfilling your curiosity.

Other things that need to be known are the levels of the dark web's iceberg. Level one may not be considered as dangerous as the others but still, a lot of crimes could fall under it. Level one contains pages of hidden answers, radios, forums, and chat services. The second level is the

exchange of identities, residencies, cyber chaos, and data with its different forms. Level three is Bitcoin exchange – simply like money laundering but with bitcoin, purchasing PayPal accounts, and smart money services. Fourth is Drugs purchase, CashApp mafia (Sending money for illegal services), and Pathfinder (buying killing viruses for your device). And with the last level, purchasing poison and Sinaloa Cartel (hitman services).

Even though it may sound pretty vicious and there is no bright side to it, but usage of dark web intelligence helped in competing with the cybercrimes that might happen.

Security analysts and investigators are frequently competing with cybercriminals to close security gaps before they are exploited. Many vulnerabilities are frequently leaked online before they are listed in the official vulnerability database. This allows cybercriminals to successfully exploit it before organizations can mount a defense. In such cases, monitoring the dark web for exploits for sale can be critical in preventing a large-scale attack. With proactive intelligence gathering, cybersecurity professionals can focus on addressing security flaws in a timely and effective manner. It is commonly assumed that the Deep Web and Dark Web together constitute the vast majority of the internet. According to some estimates, it accounts for up to 96% of the web. Regardless of the exact figures, it is clear that a large portion of the web is not visible to ordinary users and hosts a massive amount of data. As a result, the need for gathering intelligence from the deep and dark web is obvious.

There are different applications of dark web intelligence, from them:

- Operations to collect intelligence on cyber criminals
- IRC chatrooms and closed forums are being monitored.
- Monitoring the dark web for any compromised employee credentials or customer data for sale
- Monitoring the dark web for the sale of any compromised products Data from credit/debit cards
- Tracking hacktivists and intelligence correlation in relation to the bank
- Operations aimed at combating new or existing cyber threats
- Obtaining intelligence on threat attack vectors that are geo-specific, industry-specific, and infrastructure-specific.
- Exploits targeting unpatched vulnerabilities are being monitored.
- Keeping an eye on a specific malware or botnet that is targeting the organization
- Tracking down compromised assets and data leaks
- Monitoring the risk of third-party exposure
- Operations for risk management in business
- Monitoring dark web recruitment efforts for hiring insiders and rogue employees
- Search for brand names, top executives, email addresses, trademarks, copyright, and sensitive assets.

From all of this, the conclusion is that the dark web is not illegal the point is what you do inside it. There are different ways to sign up for the dark web, but none of them are recommendable. Levels of danger inside the dark web differ and are categorized into different five according to the services provided in them. Even though it is pretty dark and dangerous but dark web's intelligence helped in preventing many cybercrimes and has different applications that help us.

1.2. Difference between deep web and dark web:

Defining the difference between the deep and dark web can be confusing in different terms. As said that deep down is like a house of the dark web and initially is the main part of it, but after looking closely totally distinct.

To make everything clearer, different points will be presented in order to compare between the deep and dark web and pinpoint the difference between them. Points of comparison will be scope, operations, size, applications, and security.

1- **Scope**: The scope of the deep web is much broader than the dark web, as known that the deep web represents more than 90% of the whole internet. The deep web covers a wide range of content that cannot be accessed through web search engines (Google, Safari, Firefox, etc.). Either login credentials or an IP address will be needed in order to access the deep web. On the other hand, the dark web cannot be entered with normal browsers, it needs a special one, that we can open through the deep websites. Simply, the dark web is a smaller part of the deep web which is narrower in scope.
2- **Operations**: In terms of accessing, definitely deep web is much easier than the dark web. Accessing the deep web doesn't acquire special browsers, just login credentials or an IP address. Just the opposite in the dark web which could only be accessed with special web browsers like Tor, onion, and I2P. On the dark web, all sites end with “. onion," as opposed to ".com" or ".org" on the surface web. This is a deliberate ploy to limit access to those sites to browsers using specific proxies. It's also difficult to memorize the URLs of dark websites, which is another way for them to remain anonymous.
3- **Size**: Both deep and dark web represent about 96% of the internet and 90% of it for the deep web. To make it more visualized, let's put it into numbers. The deep web is about 400 to 500 times bigger than the surface web, making the dark web about 0.01% of it and 5% of the whole internet.
4- **Applications**: The deep web is more commonly used than the deep web. In fact, the deep web could be used in our day-to-day activities. To make it simpler, the deep web can be used while checking your email, going through your bank balance and information, buying something, entering an educational portal, etc. On the contrary, dark web users are distinct. They could be criminals, political dissidents, users of anonymity for work, and other forms that are quite the same.
5- **Security**: Even though both have their dark sides, but deep web is much safer and more secure to be used. There is an owner for each website or online service on the deep web that maintenance of security is super critical for them. On the other side, just scrolling through the dark web is not that dangerous but the real risk comes from trying to take part in any of the activities on it, like downloading illegal materials that may contain viruses or malware.

2. The origin and history of the dark web

By looking through this picture, the history and important events for the dark web will be understood in much easier way.

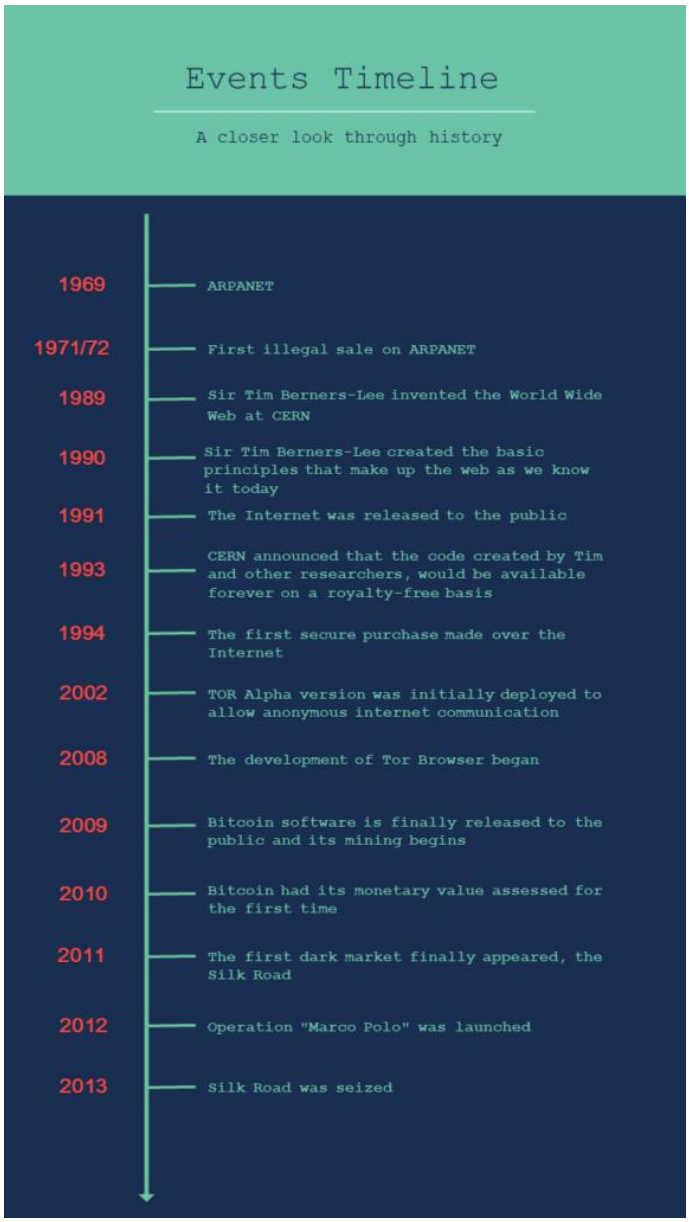

Figure 4: Events timeline of the internet and the dark web

2.1. Creation of the dark web:

United stated army wanted to develop a system to keep the communication system as invisible and anonymous as possible. They tried to develop an anonyms system that could achieve this function. They developed a system to communicate through it, and then it was deprived to other purpose of use which led to the arise of the dark web.

2.1.1. U.S department of defense and ARPANET attempts.

Apart from the dark side that is always appearing for the dark web, it has an initial purpose that was helping in providing anonymity for the users. Originally, U.S department of defense and Arpanet attempts tried different ways in order to make an anonymous and encrypted network for different governmental purposes. In order to understand the purpose and the attempts of developing behind, we need to break the topic into different parts.

- **Attempts of the U.S department of defense**

Initially the U.S department of defense were the first users for the perk of anonymity on the dark web. They used it to communicate through it and exchange secrete governmental information. After that they started to fund Advanced Research Projects Agency in order to develop a new system to be used in the communication process which is the APRANET. But what is the APRANET?

- **ARPANET**

After we understood what the layers of the internet are and how to know whether this part is deep or dark, it is time to know how all of this began.

The History of the dark web is so big and almost as old as the internet, it has never been what it is now from the beginning. It had so many changes and modifications.

The Internet made the world smaller as every device is linked by an IP address and every move you make is known on the internet making everyone has a unique identity and features on the internet, so it's easy for advertisers to hop over your pieces of information to know what advertisements to show you. It's easy for governments to know a lot of information about their citizens and can perform law enforcement by trafficking them. Therefore, there was a big lack of anonymity for bigger users, and from here sneaks the role of the deep and the dark web.

It all begins in October 1969 before the internet even existed, with the Advanced Research Projects Agency (ARPA), a branch of the U.S Department of Defense developed a computer communications network based on data packet switching. This network was known as ARPANET. The ARPANET was initially used by US universities for internal communications and by the time it became the internet as we know it. This technology was later used in the 70s to hide some secrets. Actually, the first successful online sale was made by ARPANET, and it was cannabis (weed) sold to MIT students by students at Stanford University in 1971 or 1972. Although many people think it's not the first official online sale because it was completed in person and by cash without using any paying platform.

- **The Internet launching**

After around 17 years in 1989, Sir Tim Berners-Lee, a British computer scientist, began working for CERN (European Organization for Nuclear Research) in Switzerland. He did research that

helped establish the world wide web as (WWW). By merging hypertext documents into a networked information system that is reachable from any node, he came up with the amazing idea that you can access any document from any node or area of the internet.

In 1990 he made the basics of the web – HTML, URI / URL and HTTP. In the same year, he developed the first browser and web server as well as the first-page editor. The worlds culture and communication and technology were heavily affected by the revolutionary fiber optic cables of the internet by increasing communication throughout the world through the electronic mails (emails), messages, voice over internet protocol (VoIP) calls, online articles, news, and blogs.

Later in 1991, the internet was released publicly. The creators of the internet tried hard to make the internet free for everyone until in 1993, CERN announced that the code of the web is now on a royalty-free basis (which means that it will be free for everyone to use).

By the way, in terms of historical time, the Internet quickly dominated the world of communication. In 1993, it only transmitted 1% of the information flowing through two-way telecommunications networks, but by 2000, it had increased to 51%, and by 2007, it had reached more than 97% of all information transmitted.

In 1994, Dan Kohn created a website called Net Market that had the first safe online purchase which was a CD by the artist Sting and cost US$12.48. It was something revolutionary in that it was the first transaction protected by encryption.

Jumping to 2002 the Tor Alpha version (the first dark web browser) was published. After a year Tor was released to the public with 12 volunteer nodes (nodes will be explained later). The people behind “The Onion Router” technology (from which Tor got its name) have a philosophy that users should access the internet privately to an uncensored web and have the right to dive into the internet without being watched hence the anonymity feature of the dark web.

From the previously mentioned services, a new door was opened a door for launching the special browsers for the dark web. Even more, the everyday enhancement in technology made it possible to build these browsers. There are few browsers specialized in accessing the dark web, the most important and used are the Tor browser and the onion browser, which we can call the providers of anonymity.

2.2. Initial purpose of the dark web

The initial purpose of the dark web was to provide anonymity for different governmental activities. These activities can be but not limited to: Sharing governmental information, Law enforcement, military and intelligence, etc. But how they were able to get or provide this type of anonymity.

2.2.1. Providing anonymity:

ARPANET was initially made to provide the type of anonymity they were seeking. It also provided close communication environment for organizations like universities. The ARPANET made the foundation for the anonymity feature that was supposed to be only used for organizations and governments to share sensitive political reports or to communicate within the different ministries and the military of a country. Its initial purpose was pure and not malicious regardless of its usage. Later, when everyone could access the internet, the concept of anonymity was misapplied.

In the meantime, APRANET cannot be used by locals, it is a service dedicated for the government but there are other providers for anonymity as Tor, onion, and I2P.

2.2.2. Browsers of anonymity:

Most commonly used browsers for the anonymity are Tor and onion. Each has its own work frame, history, and initial purpose; all will be discussed in the next subsections.

2.2.2.1. Tor browser:

The Tor browser, referred to as the Onion Router, offers anonymous internet browsing. The computer scientists Michael G. Reed and David Goldschlag and the mathematician Paul Syverson, who are employees of the United States Naval Research Laboratory, created Onion routing, the fundamental idea behind Tor, in the middle of the 1990s to protect internet communications for American intelligence and was subsequently given the acronym "Tor". The first public release of their project happened a year after its initial launch on September 20, 2002. The United States Naval Research Laboratory made the source code for Tor available under a free and open-source software license, allowing other groups and organizations to contribute to the project. And Since 2006, the Tor Project, a non-profit organization, has been maintaining Tor and the Tor browser. Google and other companies and groups like Human Rights Watch provide them with financial support.

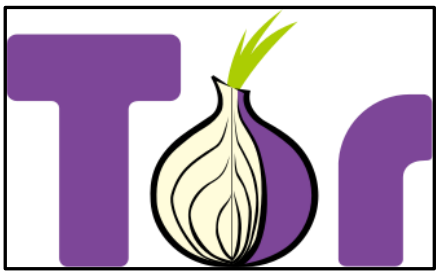

Figure 5: Tor browser

- **Onion routing**

You may ask what onion routing is and why it was called an "onion." Tor tries to anonymize your online activity by encasing your data traffic in multiple layers of encryption and then sending it to a number of nodes (also called onion routers) that peel back those layers one at a time, hence the onion nickname.

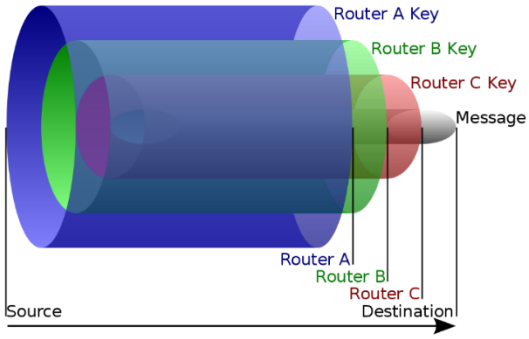

Figure 6: Onion routing

And each node only decrypts enough information in the packet to know where to send it next, so none of the nodes know both your identity and the identity of whatever website or server you're trying to connect to, and this high level of encryption and repeated bouncing of network traffic makes Tor quite secure.

- **Tor nodes:**

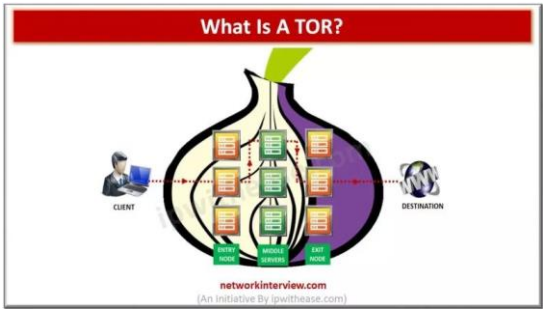

Figure 7: Tor nodes

- **The Entry Node:**
  It also goes by the name "guard node." Your Tor client connects to it as the first node. The entry node can view your IP address but not the website or server that you are trying to access. To protect you against specific attacks, the Tor client will randomly pick an entry node and carry on using it for two to three months.

- **The Middle Node:**
  The second node that your Tor client connects to is known as a middle node. It is able to see from where the traffic came (from the entry node if it's the first chosen middle node) and which node it goes to next. Your IP address and the domain you are connecting to are hidden from all middle nodes. Out of all the Tor nodes that are available, the middle nodes are chosen randomly.

- **The Exit Node:**
  The exit node is the very last stop your data travels through to be forwarded to your desired destination. The exit node is unable to see your IP address, but it does know what website or server you're trying to connect to.
  Tor isn't entirely foolproof due to the fact that at some point your data has to leave the Tor network to get to wherever it's going through the exit node it is no longer necessarily encrypted and unencrypted personal information can be read both by the operator of the exit node and whatever website or server you're trying to connect to. And Although Tor has a reputation within cybersecurity as the dark web's best browser of choice, we shouldn't discredit this powerful privacy tool just because a few apples use it.

2.3. Deprivation of the initial purpose:

As mentioned, that the initial purpose of the anonymity feature and dark web services were dedicated to the government, this purpose didn’t stay as it is. Now, dark web is considered a cover for illegal activities, as drugs, weapons, child pornography, money laundry, etc. Since we're talking about that, we should talk about the first illegal website on the dark web.

2.3.1. The appearance of the first dark net market: Silk Road

- **Back history of The American Kingpin:**

On March 27, 1984, in Austin, Texas. Ross Ulbricht was born. He was a boy scout, attaining the highest rank of eagle scout, just like his dad had done. Ulbricht had a happy childhood growing up an easy-going hipster and a serious student who scored 1460 on his SATs within the 96th percentile. Ulbricht got a full ride to the University of Texas at Dallas, where he studied physics; he then had another full scholarship at Penn state, where he evolved into a hardcore libertarian and followed the political philosophy that advocates individualism and minimal government involvement in people's lives. He was a fan and follower of libertarian economist Ludwig Von Mises, who opposed government interference in the economy.

Then the presidential candidate Mitt Romney asked what America's greatest challenge is and his response was, "I think the most important thing is getting us out of the United Nations.". He wanted to create a world free from institutional or government control, and that mindset led him to create Silk Road in January 2011.

2.3.2. Arise of crimes:

- **Silk road's crimes**

Ross Ulbricht created the largest and most advanced internet illegal drug market in history. He called it Silk Road referencing the trade routes that connected China and Europe in the 2nd century BC.

He had a note on his computer stating," I want to create a website where people can buy anything anonymously with no trail whatsoever that could lead back to them." So, he became the biggest kingpin on the internet. He wanted to set up his own modern marketplace, except his would sell narcotics and other illegal goods. And over the two years and two months during which Silk Road operated, it processed nearly 214 million dollars in sales using bitcoin, and it operated on a hidden part of the internet called the dark web. Ulbricht ultimately had no choice but to tell his friends and girlfriend about his plans, and he showed her the psychedelic mushroom he had been growing and selling as a starter product on his new website. Silk Road would eventually become a place for all kinds of drugs: Weed, Cocaine, LSD, Heroin, Ecstasy, and many other substances and services. That fit Ulbricht's libertarian mindset. He also believed that whatever someone decided to put in their body was their choice and not anyone else's, least of all the government. He also thought that everyone had the right to self-defense, which led to weapons showing up on Silk Road. After he got his business up and running, he focused on bringing customers to the website.

So he started going on different forums pretending to be someone else who happened to come across Silk Road and stated" I'm thinking of buying off it but wanted to see if anyone here had heard of it and could recommend it," and he added a link with instructions on how to access Silk Road, and he did the same on a bitcoin community forum about buying and selling heroin and described Silk Road as" an anonymous amazon.com" and it wasn't long before the buyers showed up. Ulbricht operated the site under the alias "Dread Pirate Roberts," named after the fictional character in The Princess Bride.

And to limit scams, there was a rating system like Amazon's reviews if a seller sold bad products or services and got a poor rating, it would hurt their sales.

The drugs arrived by mail with fake return addresses, and they'd be slipped inside CD and DVD cases; in addition, the package had printed mailing labels instead of handwritten ones to look like they came from a legit business. Ironically, that backfired and attracted the suspicion of authorities.

2.3.3. Silk Road's shutdown

Operation Marco Polo, so named in honor of the medieval adventurer who traveled the Silk Road to China, came to a successful conclusion last month with a massive takedown that resulted in arrests on three continents and the confiscation of assets worth tens of millions of dollars. Agents sneaked inside a San Francisco public library to arrest Ulbricht. They started draining internet accounts linked to the site and added a warning over the login screen for Silk Road that said, "This hidden site has been seized, read the notice with images of shining special agent's badges below." Ulbricht was scheduled to appear in federal court in Manhattan to request his release while the case was still being heard, and the attorney for Ulbricht had stated that he intended to refute claims that his client was the Dread Pirate Roberts.

But unfortunately for Ulbricht, he did leave a trail of digital breadcrumbs that would ultimately take him down, and his empire with him. Following a trail of network records, they had collected through court-ordered warrants, detectives identified Ulbricht as a suspect. On October 1, 2013, the FBI arrested Ulbricht and confiscated his laptop for drug trafficking, money laundering, and computer hacking. A judge gave Ulbricht a life sentence in prison in 2015.

Due to the existence of similar websites on the Tor network, the closing of Silk Road is unlikely to put an end to the trading of illegal goods on the Dark Web.

3. Dark web is properly named:

From the previously mentioned points, it is easy now to pinpoint why it is named “Dark web”. Not only it is a cover for illegal activities, but that in the worst-case scenarios also entering it and participating in its activities could end your life. It is a cover to illegal actions like drugs, weapons, fake identities and nationalities, child pornography, money laundry, and many other things.

3.1. Criminal activities on the dark web:

There are a lot of crimes that happen on the dark web and one of the famous crimes on it is the markets for prohibited substances that were previously mentioned. Now let’s get deeper into these illicit websites.

One of the most famous sites that host these illegal actions is the Silk Road is one of these markets that sell these prohibited substances such as cocaine and other types of drugs.

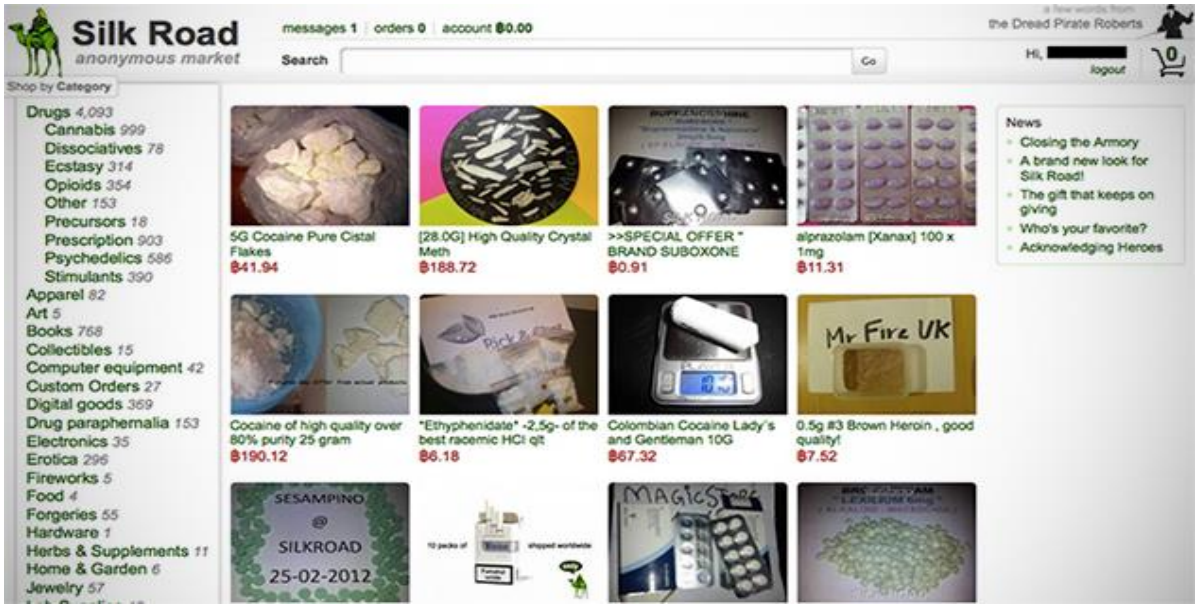

Figure 8: What silk road looks like

And not only drugs there were also steroids, fake ID’s, stolen credit cards and any type of weapon you could possibly dream of.

3.1.1. How are they widely spread on the dark net’s platforms?

The silk road was launched in February,2011. They had been developing this website since August,2010. This website was run by “The pseudonymous”. At first, there were only limited number of sellers on the website. Little did they know that there were a lot of people who want to be sellers on this website, so these people have to buy an account in auction. An auction is the process in which the goods or the products are sold for the highest bidder. In June,2011 Gawker (an American blog that is founded by Nick Denton and Elizabeth Spiers that focuses on media) posted an article about the website which led to an increase in the number of users on the website.

Based on the data that is collected from 3 February,2012 to 24 july,2012 amount of the transactions estimated was about 15 million dollars which was a very huge amount then because they were only using bitcoins. The FBI was trying to shut down this website because of how many crimes done on it. In May 2013 The Silk Road was shut down for a short period by a sustain DDoS attack(it is a cyber-attack in which the attacker seeks to make the network surface unavailable for the user)after this attack and on 23 June,2013 it was claimed that 11.02 bitcoins had been seized and they were about 814 dollars at the time and that was a great step into shutting down this website . the FBI said that the IP address of the server's website had been found and it was in Reykjavik (the capital of Iceland) but at that time the IT experts doubted the FBI claims because the technical evidence suggests that there was nothing that could lead to the leak of information of the IP address of the server. In October,2013 the FBI closed the website and arrested the operator (Ross Ulbricht).

Figure 9: ross Ulbricht

In November 2013, the Silk Road 2.0 had been launched, run by the former administrators, and was also shut down. The operator was arrested on 6 November 2014 as the part of "Operation Onymous". In November 2020, the United States government caught about 1 billion dollars' worth of bitcoins connected to the silk road. Ulbricht was sentenced to spend his life in prison without possibility of parole. Based on the data from 3 February 2012 to 24 July 2012 about 15 million in transaction in the form of bitcoins were made annually on silk road. About a year later Nicolas Christin said in an interview that an increase in volume from 30 million to 45 million would not surprise him at all. They did all these transactions with bitcoin which is a form of cryptocurrency which gives the user a degree of anonymity (being anonymous) like his name is not seen and his address that's why they use to buy their forbidden substances. The silk road held the buyer's money in escrow (means that there is a third-party program that stall the buyer's money) until the order is received and there is a mechanism that allowed sellers to opt(choose) for the value of bitcoins held in escrow to be fixed to their value in dollars at the time of this sale to relieve against bitcoin's volatility.

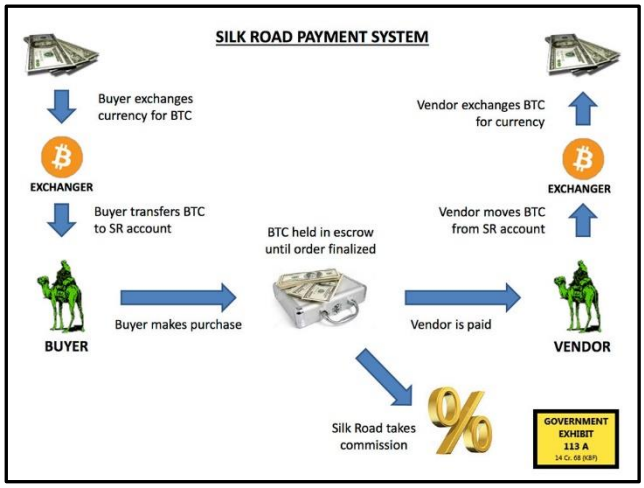

Figure 10: Silk Road payment system

The idea is dark web offer things that cannot be reached easily. It provides anonymity, ability to put hands on things that are unreachable that could get you arrested. For these reasons, there are a lot of crimes on it. Metamorphically, it can be described as door to hell where every activity in it considers as a crime even if you are taking action in it with good intention.

It is not easy to shut all the services offered by the dark web at once. It is a whole business and there are a lot of people who benefit from it. So whenever attempt to close it, you will others who try to reopen it. And as long as it is a service, that the government use it, there will be always hackers who try to deprive the initial purpose of usage.

3.1.2. Why is it so hard to stop these activities?

There was a complaint that is published at the time when Ulbricht was arrested. This complaint included information the FBI gained of the Silk Road server on July,2013 it said that from February,2011 to July,2013 there were about 1,229,465 transactions completed on the site. The total profit from this about 9,519,664 and the commissions that the website took were about 614,305 bitcoins. Those sales were about 183 million dollars and involved 146,946 buyers and 3,877 sellers.
The silk road wasn't the only site that sell these forbidden things there are also similar sites like" The Farmer's Market". This website didn't use bitcoins, but it used payment methods like PayPal and western union. It was shut down in 2012 easily because they could track down the buyer and the seller. When the silk road was still running there were also other sites like it. The Guardian, which is a famous newspaper, predicted that there are other websites that would dominate the market after the silk road and these websites named" Atlantis" and these websites were also shutdown in September,2013.

The crimes that happen on the dark web is not only limited to a marketplace that sells forbidden substances. The crimes on the dark web can be represented as a sea which you cannot see its end. And one of these crimes that is spreading very fast lately is child sexual abuse. The child sexual abuse material is plenteous online despite the tries of the tech companies and governments, but these materials will always be there, and it started to increase since covid-19 pandemic. As long as the amount of Tor users increases ever year the amount of people that are exposed to this type of material increases also. About 2.6 million users that use Tor network daily only 2% of them use onion services. They use onion services to get their online privacy. The same study said that about 80% of the users of the onion services are directed to illegal porn and child sexual abuse material. Another study showed that about 53.4% of 170,000 contain legal content while the other 46.6% contain illegal content. Only about 7.5% from this material is only profitable. So, most of these materials are not here for the money. And there are services started charging people for this content. One of the websites that contain this content is "Playpen".

Playpen was a darknet website that is filled child abusing and pornography materials. This website was working from August 2014 to March 2015.After 6 months from running the website. The FBI managed to arrest website owner Steven W. Chase. After that the FBI didn't shut down the website till 13 days as a part of Operation Pacifier. When it was closed the site had about 215,000 users and hosted 23,000 sexually explicit images and videos of children.

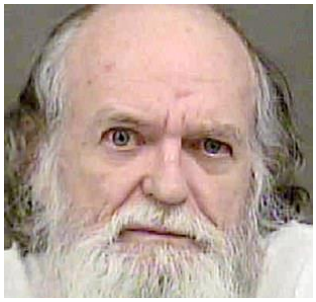

Figure 11: Steven W. Chase

To sum up, it is not easy to shut all the services offered by the dark web at once. It is a whole business and there are a lot of people who benefit from it. So whenever attempt to close it, you will others who try to reopen it. And as long as it is a service, that the government use it, there will be always hackers who try to deprive the initial purpose of usage.

4. Contributions towards stopping these illegal activities:

Many steps have been taken into action in order to stop the illegal activities present on the dark web. Most important of them is the FBI's and governments' contributions. Most of the attempts were successful and were able to catch who are behind these illegal actions. But in order to understand how they were able to track them and stop these illegitimate actions.

4.1. FBI's contributions:

The FBI is a law enforcement organization in the US that's in charge of looking into a variety of federal crimes, including those that happen on the dark web. A portion of the internet known as the "dark web" is inaccessible without specialist software, such as the Tor browser, and is not indexed by search engines. It is frequently linked to criminal activity like drug trafficking, smuggling of firearms, and child exploitation.

The FBI has a number of resources at its disposal to stop these unlawful operations on the dark web. Utilizing informants and undercover agents is one of the primary ways the FBI looks into crimes committed on the dark web. These people have access to forums and markets on the dark web, where they can gather facts and proof of illicit conduct.

The FBI additionally employs cutting-edge technology to locate and capture offenders using the dark web. This comprises tools for decrypting encrypted messages and other data, as well as software for tracking and analysing dark web activity. The FBI also collaborates extensively with other law enforcement organisations on a national and worldwide level to share intelligence and resources in the battle against dark web crime.

Overall, the FBI is essential in putting an end to illicit activity on the dark web. The FBI is able to locate and bring to justice people who participate in illegal conduct on the dark web because to the employment of undercover agents, cutting-edge technology, and international cooperation.

Many governments across the world have been motivated by the rise of illicit dark web transactions to combat crime by enhancing the powers of domestic law enforcement organisations like the US Federal Bureau of Investigation (FBI). For instance, it is rumored that the FBI has carried out operations that enable them to "de-anonymize" Tor servers. The FBI accomplishes this by setting up nodes in the network that provide the organisation access to information about the owners and whereabouts of select nefarious Tor-based websites. The FBI's takedown of "Silk Road 2.0," the top illicit dark web bazaar in 2014, was the first notable action. During the site's two and a half years of existence, the investigation found that thousands of drug dealers and other criminal vendors utilized it to sell hundreds of kilograms of illegal drugs and other items and services to more than 100,000 customers. Hundreds of millions of dollars from these illegal activities were laundered through the website. Overall, the website had made sales totaling more than 9.5 million Bitcoin valued at almost $1.2 billion at the time. Two of the main Silk Road substitutes, Hansa Market and Alpha Bay, were discontinued in 2017.

Dark web enforcement skills have increased, and most recently, a Dutch operation took control of a well-known dark web business, ran it anonymously for a month, and then used the data gathered to shut down dozens of other dark web businesses.

4.2. Operation DisrupTor:

In Sunland, California, the storage building next to the modest yellow stucco house was neat and well-maintained. A huge box contained goods that were addressed and prepared to be dropped off at the post office, while materials such as tape, mailing supplies, and other supplies were stacked or organised into labelled bins. It appeared to be a typical mail-order company. until the scope of the search was extended. Agents from the FBI, USPS, and Homeland Security Investigations (HSI) discovered there roughly 50 pounds of methamphetamine as well as bags and containers containing thousands of Adderall tablets. Scales, package sealers, and three guns were also present. In the United States, where a person is now more likely to die from a drug overdose than in a car accident, each of those parcels that were already filled or were waiting to be filled would bring narcotics to someone there.

A second location where the same business packaged drugs was searched, and another enormous amount was found. Agents searched the two locations and found over 100 pounds of methamphetamine as well as almost 30,000 pills—a hazardous drug haul worth several million dollars. Multiple people connected to a drug trafficking organisation operating online and selling its products under various names on the darknet were apprehended as a result of the two search operations and subsequent law enforcement efforts in other places and at different times. Currently, the defendants are accused of many offences, including drug trafficking, conspiracy, money laundering, and possession of a handgun, which could result in penalties of 10 to 25 years in federal prison.

According to Load Investigators, the organisation sold drugs on more than 18,000 different darknet marketplaces. Users can access the darknet, a portion of the internet that offers a higher level of anonymity, with a customised browser. According to law enforcement, this could be one of the largest darknet suppliers of bulk methamphetamine ever discovered. According to the investigators, the evidence suggests that in addition to transporting drugs to individual customers across the U.S. and internationally, the organisation was also supplying other darknet vendors and street drug traffickers.

The partner agencies that make up the Joint Criminal Opioid Darknet Enforcement (JCODE) team conducted these operations in the Los Angeles region, along with comparable activities across the United States and Europe. This coordinated effort was known as Operation DisrupTor. 179 people were detained by law enforcement as part of Operation DisrupTor, and more than 500 kg of illegal substances were seized. JCODE, which was established in 2018, brings together the efforts of the FBI, USPIS, HSI, Drug Enforcement Administration (DEA), U.S. Customs and Border Protection, Department of Justice, Financial Crimes Enforcement Network, Naval Criminal Investigative Service, Department of Defense, and Bureau of Alcohol, Tobacco, Firearms, and Explosives. Europol is a crucial international partner in JCODE's efforts to combat darknet drug trafficking because many of these markets are cross-border. The FBI Director Christopher Wray stated during a news conference today presenting the outcomes of Operation DisrupTor that "the law enforcement officials assigned to JCODE specialise in threats where traditional criminal behavior meets with advanced technological platforms." Every day, they are striving to demonstrate to these criminals that they can no longer rely on using the darknet to hide out because we will hack into their networks, shut down their online black markets, and use all means necessary to bring them to justice. However, what appears to be an impenetrable cycle of remote and anonymous encounters has several weaknesses. According to Siliciano, "the vendors still have to convert their money into cash, pick up the narcotics, and transport the drugs." "Not everything that occurs does so online."

The JCODE team in Los Angeles is supported by HSI Special Agent Christopher Hicks, who said that darknet buyers are also susceptible to vulnerabilities. "You have to open the mailbox, even if you're having things mailed to a post office box using a false name. You must handle that packet.

4.3. Government's contributions:

In addition to carrying out disruption operations, governments and international organisations are attempting direct regulation of the cryptocurrency powering dark web marketplaces. For instance, the Financial Action Task Force released recommendations in June 2019 urging businesses handling bitcoin transfers to identify both the source and the recipient of funds. The advice comes in response to the 2018 G20 Summit's request that global regulators take into account policy responses for crypto assets, especially in relation to know your customer, anti-money laundering, and preventing the financing of terrorism. Supervisors need to start building the basis for further inspection even though the startup ecosystem of exchanges, wallets, and other crypto payment facilitators lacks the infrastructure required to embrace such norms similar to those in the financial industry. This issue will become much more urgent with the upcoming introduction of Libra, Facebook's cryptocurrency, as adoption barriers for its more than 2 billion users will be lowered.

An NIJ-supported group of experts identified the primary dark web difficulties and opportunities for law enforcement, as well as the highest priority needs for addressing them, in order to increase awareness of the dark web among law enforcement agencies and suggest technologies that can help them police it. Experts from federal, state, and local agencies, as well as university researchers and civil rights activists, were there. The experts' workshop, which was organised on behalf of NIJ by RAND and the Police Executive Research Forum, produced high-level suggestions centered on the following:

- Officers and investigators will receive training on how to recognize pertinent dark web evidence.
- Information-Sharing – enhancing information-sharing between organisations on a national and worldwide level.
- Examining the advantages of creating cross-organizational structures for cooperation is New Structures for Cooperation.
- Creating new standards for forensic tools to gather evidence from the dark web on computers is known as "New Forensic Standards."
- Researching ways to update legislation that allow for the inspection of packages sent by mail or other services. New Laws for Package Inspection.
- Identifying and addressing both highly visible traditional crime and the less obvious criminality on the dark web requires research on the increasingly interrelated nature of crime.

In order to investigate illegal behavior on the dark web, law enforcement officials highlighted the following needs as priorities:

- educating state and local officials about the dark web.
- forming collaborations between agencies that span jurisdictions.
- providing more and better training to better prepare cops to recognise dark web activity and evidence.
- providing superior knowledge of dark web techniques and operations to special investigating groups. Due to the dark web's secrecy, many state and local law enforcement authorities are generally ignorant of its presence and its potential to fuel crime in their areas.

5. Dark web and cybersecurity:

First, let's get to know some of the terminology and ideas that people confuse, and after that, we'll discuss about the relationship between the dark web and cybersecurity.

5.1. What is Cyber Security?

Cyber security is a combination of different skills and tools, which combines together to provide of the protection of computer systems, networks and data from penetration that may lead to the disclosure of confidential information, theft or destruction of hardware, software, or data. Therefore, there will be no information security without information penetration (Hacking). cyber security is a type of penetration (Ethical Hacking), where people will not be able to protect their information without knowing the methods of data penetration so that they can protect data and systems from hackers.

There are a lot of misconceptions that people get mixed up about Hacker, Hacking So I wanted to get into this, and I like blowing up these myths and misconceptions here first of all what a hacker is basically and what a hacking, so he has a great and interesting story about it.

In the early 1970s, the largest computer network available to the general public was the telephone system. At that time, people used to use phones on the street that needed coins, and the phones were run by an automated system that used specific analog frequencies to make calls and that's where the hacking started. So, what the hackers did was they analyzed the system very carefully and understood how it was working and then they tried to copy that tune using a toy whistle. And when they have to call someone, they use this to make international calls and free international calls; Hence the term hacker and piracy have been identified.

So, Hacker is the one who can find the holes in the system. This process is called hacking. we got to know the difference between hacking and hacker, but what is ethical hacking?

5.1.1. What is Ethical Hacking?

Let's say you have a system and you have established all the security controls to protect it. But how can you ensure that the system is completely secure and that no one can bypass the security systems? You will definitely have to test it against all security breaches and check if the security controls protect your system.

Well, the process of testing the system against all possible security breaches would be known as ethical hacking. Ethical hacking is a part of cyber security, which mainly deals with finding a security flaw in a system and resolving it before any hacker exploits it. Hence, cyber security professionals are also known as penetration testers.

5.2. What does the dark web mean for cybersecurity?

I know that when you reach this part in the article, you will know what the dark web is, but the dark web from the point of view of cybersecurity experts is interesting, so we will learn about the dark web from another point of view.

Experts call the dark web the name "Land of Hidden Services" or "Dark Web", through which various secret commercial transactions take place, and it is possible to navigate to it and roam its sites without the person leaving any traces, meaning that he will be hidden, and his activities are not registered on No search engines, and cannot be tracked. That is why its name did not come from a vacuum, and as it has risks, it has advantages, so organizations such as cyber security companies, the FBI and banks want to

It also contains everything that requires a login such as content from: online banking, payment sites, Netflix, and Amazon Prime, and the reason for that is the benefits they reap from it, which are:

- It is difficult for anyone to access it, as it needs software, settings, and special authorization to access it.
- People who use the dark web can maintain their privacy.
- The dark web refers to encrypted online content that is not indexed by traditional search engines.
- Complete concealment and encryption of information, which makes it a safe place.

5.3. The Relation between Dark web and cyber security

Is there a relationship between the dark web and cybersecurity? People are confused that the dark web has nothing to do with cybersecurity other than hacking the systems that cybersecurity experts are trying to protect, as the term dark web is associated with an illegal context for good reasons for the average internet user. But from the point of view of cybersecurity experts, through the correct use of this and other technology, cybersecurity experts can open new doors of opportunities and enormous possibilities to improve the security situation of organizations.

5.3.1. Why are cybersecurity experts interested in the dark web?

Before cybersecurity experts are interested in trying to take advantage of the dark web, they must know how to protect against cyber intrusions on the dark web before entering and taking advantage of it, and therefore cybersecurity experts use methods and tools to infiltrate the Centers of activity of cybercriminals, as they are monitoring them so that they can find out and discover the methods of hacking and anticipate cybersecurity threats so that they can counter them and Understand how hackers and exploiters operate in order to combat the risks they pose to systems. And as you know it, the dark web is the best place to communicate with hackers. Cybersecurity professionals can use the dark web to increase the security and privacy of information as it is not a place for cybercriminals only.

5.3.2. Some ways that cybersecurity professionals use to enhance the security of systems:

We will now learn about some ways that cybersecurity professionals use to enhance the security of systems

- **The gathering of dark web threat intelligence**: Browsing the dark web never stops. Hacking groups often discuss potential risks and major threats to cyber security, and hacker websites on the dark web also share lists of email addresses and account credentials to enable hackers to compromise systems and steal data. By joining the right group, your organization can take advantage of you are learning. As a security analyst, you can use knowledge from the dark web to defend against all security attacks. Learn about potential attack vectors and how to prevent similar attacks. You will also learn some new ways to handle security by talking to hackers and gathering relevant information about their activities.

- **Using hackers to access information**: Members of the hacking group will share important details about their activities and the hacking tools they use. This information can be collected and scrutinized to help you prevent similar attacks. To prevent threats from entering your company's systems, cybersecurity professionals also need to understand how these hackers operate. Knowing the details of hacking activity can help you take necessary steps to improve the security of your system

- **Keeping information secure from hackers:** Organizations of cyber security can protect themselves from hackers in a number of ways. These hackers can also try to

gain access to a company's confidential information by breaking into the company's computer systems. You cannot prevent such attacks. However, you can take steps to prevent cybercriminals from accessing your important data. With a comprehensive end-to-end security roadmap that includes monitoring, detecting, and controlling risks from dark web threat intelligence, you can take certain precautions to prevent sensitive information from being stolen and used for criminal purposes. With the dark web, you can create an online security barrier for the data in your company. This reduces the security risk posed by hackers.

- **Maintain confidentiality of mission data:** On-the-ground safes also protect confidential documents and files from unaccompanied visitors in place. It is also important to put in place procedures for shredding confidential information and high paperwork to reduce the risk of information theft. Similarly, the same principle is done here. Important, highly confidential data is uploaded and stored in certain places. There are specific ones, and no one is allowed to enter and access them except through specific methods. Even when some information is erased, it is not that easy, as we must make sure that it is not retrieved yet. Clear it my way. And there are some other tricks, including encryption of information and other things.

- Another way to protect system data via the dark web is to keep tabs on user activity and accidental leaks of corporate data. Security professionals can reduce the likelihood of a data breach by proactively browsing the dark web and removing company information.

- **Prevent Data from Being Exposed on the Internet**: You must always keep information about your system confidential. Otherwise, it can lead to various types of attacks on the systems used by your company. By removing or hiding your data before posting it online, you can prevent such attacks. This reduces the chances of hackers stealing your data.

5.3.3. Some the tools that network admins use to monitor the dark web:

As you know him about some of the methods used by cyber security professionals to enhance the security of systems, but we did not delve into how this works and the tools they use. So, we will learn about some of the tools that network admins use to monitor the dark web, and although some of these tools are used by cyber security experts, they use much more complex and specialized things, and most often they work under secret organizations. They do these things with secret devices and tools.

5.3.4. Dark Web Scanners:

According to IndentityGuard article titled What is a Dark Web Scanner? the formal definition is: "A Dark Web scanner is a tool that searches through the Dark Web for your Personally Identifiable Information (PII). "

As we all know, browsing the dark web never stops. Hacking groups on the dark web often share email address lists and account credentials with hackers to enable hackers to break into systems and steal data, so dark web scanners look for stolen information.

In simple terms dark web scanners are services that identify and scan websites for buying, selling, and sharing stolen data. Stolen identity data can include sensitive information, including personally identifiable information (PII), non-public information, encrypted and password-protected illegal content, and other sensitive data posted on the dark web.

5.4. Personal information and dark web:

There is always a question come into mind which is: how did your personal information end up on the dark web?

There are many types of identity theft to be wary of. Anything from phishing email scams to data breaches to malware on your computer can expose your personal information (credit card numbers, CVV codes, or social security numbers) to hackers.

Dark web scanners use your personal information, such as your email address, to scan the dark web for matches. Most scanners first search illegal marketplaces or forums that lack sophisticated privacy protections.

Dark web monitors offer a similar service to dark web scanners but differ in one key respect: They continually scan the dark web to determine whether cybercriminals have leaked your personal information. The scanner provides a one-time scanning service.

Despite their breadth, no dark web scanner can cover all stolen data that exists on the dark web due to criminal activity. That's because much of the stolen data is privately traded. However, if you suspect that your personal information has been compromised, a dark web scan may be a good resource for reassurance. It is these tools:

- **CrowdStrike Falcon Intelligence Recon:** is a research service that searches dark web sources for mentions of your company's assets. This includes branding, company identity, email addresses of people in your company, and mentions of key executives and employees.

Up until this point, we've gotten to know some complicated terms and I've tried to correct some misconceptions. We have also learned about the dark web from the point of view of cybersecurity experts, what is the relationship between them, some of the methods that security experts use to enhance the security of systems and some of the tools that network administrators use to monitor the dark web.

6. Bright side of the dark web:

I know after what I said you now think that the dark web doesn't have any uses except for illegal things like selling guns, drugs, and other criminal activities. In addition, you wish to prevent the existence of the dark web, but what if there is a small light in the dark? A bright side of the dark web.

6.1. Anonymity:

Think about it: can we use a dark web filled with crimes for a good thing? the answer is yes, by using the same tool with the right purpose. Anonymity like what I said in the second section was the initial proposal of the dark web, it makes your IP address cannot be tracked and it gives you secure and private browsing and you can use a VPN for more secure due to the possibility that the Tor browser itself could be hacked. Because they can enter the dark web anonymously it encourages the freedom of speech, especially in a country that does not have freedoms. The dark web allows you freely to say what you want and publish anything without being afraid of the government or anyone as your IP address is protected and no one can get you as your identity is unknown. And I think it is good also to the government to know the real opinion of its people about the performance of the government and to know their opinion in their country.

The most famous example of this is the TOR browser. For certain reasons, TOR is used to provide private, anonymous, and secure communication and activities. Following are a few instances that relate to the above:

- Political and anti-censorship initiatives. TOR characterizes it as a suitable solution for getting around censorship and accessing websites or content that is in some manner prohibited. People can access materials that could be restricted in some regions of the world thanks to it. Some governments have put restrictions on using TOR or blocked access to it during certain times in an effort to prohibit it. Political dissidents also utilize TOR to protect and preserve their anonymity in their conversations and movements. Dissident movements in Iran and Egypt are examples of this.
- Private conversations. TOR makes it possible for people to visit chat rooms and forums and conduct sensitive interactions for either personal or professional reasons. When children browse the Internet, it is utilized to safeguard them from harmful activities (by hidden IP addresses of their devices). Businesses can use this tool to safeguard their initiatives and to keep spies out of the hands of their rivals.
- Leaks of information. Journalists can use TOR to securely connect with informers and dissidents. Through TOR, such as the New Yorker's Strongbox, people have the option to connect and share documents in an anonymous manner with publishers. The anonymous operating system Tail, which is based on TOR, has been utilized by Edward Snowden. In order to reveal the sensitive information concerning American defense programmes, he has informed and talked with journalists. The National Security Agency (NSA) attempted to utilize the TOR browser to de-anonymize users, according to a top-secret document that Snowden leaked.

6.2. knowledge:

we live in the century of information who have information have the money and the power. dark web and deep web are huge libraries of information you can find information in things that you can't find through regular search engines like: (google, Bing, ….). often this information is added by scientists or researchers and this information was kept far from the normal web you can easily find it on the dark web. Journalists like to get information from the dark web because it sometimes goes to a specific place and gets information like wars or a far place and because they can find information that is not in the regular search engine. Also, the dark web gives a double-faced feature which is pirated scientific research and books, you can get any paper or book you want through the dark web although it is something illegal and that's why I said it's a double-faced feature.

6.3. Cybersecurity (hiding information):

For cyber security experts, there are many benefits from the dark web to improve their skills, there is a continuous chat between the hackers in a hacker group the right group can be very useful to get information about the hackers and their new techniques that they use and know how the hackers think. This information can help you to protect your organization from hacking.

The dark web is used to hide the client's details like bank details, imagine that anyone can open google and search for your visa number or bank account, so this information is hidden in the dark web. Of course, you can't stop the hacker's attack, but you protect it.

Whenever you use the internet, you put yourself a target for hackers. So, you must know how to protect yourself. You can protect sensitive information by implementing strong privacy protections. As a result, your b security will be improved, and security threats will be minimized.

In the end, yes dark web has many disadvantages but there are some advantages like the anonymity that help in freedom of speech, and there is an ocean of information that you can find in the dark web, hiding information, and protecting it from hacking. The dark web is not full of dark, the idea that in what you use it.

7. Dark web trap:

“Caution is the parent of Security “As we know the dark web users’ identities are not known and you can do and access almost everything. And that makes it a very good environment for hackers to live on this special feature of the dark web browsers, so taking precautions and caution is a necessity in the dark web.

First let’s understand what hacking is: Hacking is the act of gaining unauthorized access to a computer or network in order to steal, alter, or destroy data or to use the system for malicious purposes.

Hacking can be done for a variety of reasons, gaining unauthorized access to a computer or network with the intention of stealing, destroying, or altering data or using the system for nefarious reasons, such as monetary gain, espionage, activism, or even just to check the system's security.

In the context of computer security, a vulnerability is a weakness or flaw in a computer system or network that an attacker can use to gain access, steal data, or do other harm.

Systems with vulnerabilities can be detected in their software, hardware, or other components, and they can be taken advantage of via malware, social engineering, or other methods. To defend against prospective assaults.

7.1. Instances of famous people being hacked:

- **In 2008,** the email account then-Presidential Barak Obama was hacked by a hacker who claimed to be working for the Chinese government.
- **In 2011**, the email account of former US Secretary of State Colin Powell was hacked, and the hackers released a number of private emails and documents.
- **In 2014**, a number of celebrities, including Jennifer Lawrence and Kate Upton, had their iCloud accounts hacked, resulting in the online disclosure of their private images.
- **In 2017**, hackers broke into the email account of HBO CEO Richard Plepler, leaked a number of previously unreleased TV programs, and demanded a ransom.
- **In 2021**, the Twitter accounts of several high-profile individuals and organizations, including Barack Obama, Joe Biden, Elon Musk, and Bill Gates, were hacked as part of a cryptocurrency scam, it's critical to regularly discover and fix vulnerabilities.

There were also many cases of penetration of international companies, for example:

- Google has been the target of numerous hacking attempts over the years:
    - **In 2010**, the company discovered that Chinese hackers had breached its corporate infrastructure and accessed the Gmail accounts of Chinese human rights activists.
    - **In 2013**, the company revealed that it had suffered a similar attack.
    - in December 2009, which it dubbed "Operation Aurora.
    - **In 2014**, it was revealed that Russian hackers had breached Google's security systems and gained access to the accounts of several hundred million users.

- In 2016, the company disclosed that it had discovered a vulnerability in its Android operating system that had been exploited by hackers to gain access to users' personal data.

These are just a few examples of the many hacking attempts that Google has been exposed to over the years.

7.2. Vulnerabilities exploited by hackers:

It can be simpler for hackers to guess and access accounts if users use weak passwords or the same password across several accounts. Hackers can easily take advantage of outdated software that is attack prone,

Hackers may use malicious websites or phishing emails to trick users into clicking on links or downloading attachments that contain malware, if a device doesn't have a firewall installed, hackers may be able to access it without authorization.

Hackers can access data from a device in a variety of methods without the owner's awareness. Typical techniques include:

- **Phishing ruses:** Hackers can send phony emails or texts that look like they are coming from reliable sources, deceiving the recipient into clicking on a dangerous link or disclosing personal information like passwords or bank account details.
- **Malware:** A device can be infected with malware by hackers via a number of techniques, such as email attachments, websites, and software downloads. Once installed, the malware gives the hacker the ability to remotely manipulate the device or collect information from it covertly.
- **Unsecured networks:** If a device joins to an unprotected public Wi-Fi network, hackers may be able to acquire confidential data by intercepting data being sent over the network.
- **Physical access:** If a hacker has physical access to a device, they may be able to bypass security measures and extract information directly from the device, such as by connecting the device to a computer and copying files.

7.3. Examples of security used by Google:

Google has a number of security systems in place to protect against users to provide a second form of authentication, such as a code sent to their phone, in addition to their password when logging into their accounts. This helps to prevent unauthorized access even if a hacker has obtained the user's password.

- **Encryption:** Google uses encryption to protect data in transit and at rest. This means that data is scrambled and can only be accessed by someone with the correct decryption key.
- **Security Key:** Google offers a physical security key that can be used as an extra layer of protection when logging into Google accounts. This key generates a unique code that must be entered in order to access the account, making it more difficult for hackers to gain access.
- **Firewalls:** Google uses firewalls to protect its servers and networks from unauthorized access. These firewalls act as a barrier between the internet and Google's networks, blocking unwanted traffic and protecting against cyber threats.

- **Security Audits**: Google regularly performs security audits to identify and fix any vulnerabilities in its systems. These audits are conducted by both internal and external security experts.

Overall, these security systems work together to provide a strong defense against hacking and other cyber threats, helping to keep Google users' data safe and secure.

7.4. Protection against hacking:

A form of cyber security technology called a "dark web trap" is used to find malicious behavior on the dark web. It operates by keeping an eye out for unusual behavior on the dark web and notifying the user when it does.

Malicious conduct, like phishing, malware, and other illegal actions, can be found using it. It can also be used to monitor the dark web for any suspicious activity that could be used to target the user or their organization. Dark web trap is an important tool for any organization that wants to stay safe online.

7.5. Methods of defending oneself from hacking:

These include creating strong, one-time passwords for each account, avoiding using the same password across numerous accounts, using a combination of letters, numbers, and symbols, and, when practical, enabling two-factor authentication.

keeping software and devices up to date with the latest security patches and updates, being cautious when clicking on links or downloading attachments, especially if received from unfamiliar sources, using a reputable antivirus and firewall program to protect devices and networks, avoiding the access of sensitive information on public Wi-Fi networks, and using a virtual private network when connecting to the internet to encrypt online activity and protect personal information.

Being vigilant and aware of potential threats is an important part of staying safe. It is important to be aware of your surroundings and to pay attention to any suspicious activity.

It is also important to be aware of any potential threats, such as cyber security threats, and to take steps to protect yourself from them. Being vigilant and aware of potential threats can help you to stay safe and secure in any situation.

By following these steps: The risk of being hacked can be significantly reduced and personal and financial information can be protected from being accessed by unauthorized.

Here are some protection methods:

- **VPN:** If you are willing to use the dark web and want to browse in a dark web browser like tor you can use a VPN. Even though you are anonymous, there are hackers who can see your activity and use those pieces of information. Your activities can be shielded from prying eyes with the use of a VPN. You can give the impression that you are in the same region as the server you are using by connecting to an external server and adopting its IP address.
- **Password manager:** Use a password manager and regularly update your passwords to offer yourself the highest chance possible of securing your sensitive data. The common

practice of having the same password across all of our accounts can make your information more accessible. Your online account passwords should all be unique, strong, and separate from one another. For instance, your online banking password and your Instagram password shouldn't be the same. A simple approach to prevent this is by using a password manager. You won't ever have to worry about forgetting another password again thanks to password managers, which create secure passwords for you.

- **Enable Two-factor authentication:** Using two-factor authentication is one of the greatest ways to safeguard your online accounts from the dark web. A second authentication step combines two factors as a manner of confirming authorization, either your username or password and then your phone number or even something physical like a fingerprint, making it far harder for a hacker to access your accounts. This additional security step can further shield you from identity theft if your login or email address has been hacked.

Some browsing tips to protect yourself:

- Avoid illegal access to forums, do not try to circumvent the authorization criteria if you discover a forum on the dark web that needs a credential for access.
- Don't pretend to be someone else.
- Do not use someone else's identity (name, picture, contact information, email address, etc.) without that person's permission if you require a persona to access or engage on the dark web. In addition to putting the other person at danger of experiencing targeted malicious activity from criminal actors with whom you have engaged, pretending to be someone else can get you into legal problems. The greatest strategy for the dark web is to make a completely fictitious persona that cannot be linked to you or your company.
- Do your research with a plan in mind if you will use the dark web in your research.
- There are two reasons why this is crucial. First of all, having a set of written standards will aid in maintaining the focus of your research efforts and keeping them within the parameters of your organization's risk appetite. Second, having written plans, rules, and processes might be useful if law enforcement starts looking into you or your business.

Conclusion:

The layers of the internet are finally something we have a decent understanding of. We walked through each layer and presented its function, applications, type of data found on them, and ways of accessing them. We have been able to pinpoint how sinister and Dark it is. We have also been able to draw why it is called the Dark web. The dark web was initially created to serve military purposes and other institutions by the anonymity feature. This initiation was started by the U.S department of defense with different attempts until creating ARPANET.

To understand why it has been this dark and dangerous, deprivation of the Initial purpose has been presented, and we have been able to conclude from it how this happened, the events, and their timeline. We also cleared the confusion of why the Dark web is legal to access but could be considered illegal. Throughout this report, we have been able to understand why the crimes have raised and why it is so hard to stop even though there are numerous contributions to stop these illegal activities. You will also get a glimpse of these inhuman activities; even though it might appear that everything related to the Dark web is illegal and dark, but it has a bright side. It has presented the Initial uses of the Dark web, why and how they use it. Also, to complete the understanding, we presented the relation of the dark web with cybersecurity and why it is needed. Finally, we would be able to learn how to protect ourselves and our information from the top of the Dark web in different ways.

To sum up, this report tends to let you learn about the world of the internet that you are unaware of. Also, to clear the misconception of the idea that the Dark web is only dangerous and there isn't any benefit behind it. Everything has its own black-and-white side, same for the internet; it totally depends on how you use it. You should be aware of the negatives and try to be as safe as possible in order to get the highest benefit from it.

Recommendations:

It is important for you as a reader to gain consciousness and awareness of that unknown world so that your curiosity won’t let you dive into it without knowing the consequences or without a certain noble goal from diving deep into it.

It's crucial for you to understand how using dark web browsers could harm you and expose you to potentially dangerous situations like life-threatening hacking.

This study didn't set out to reveal what to look for on the dark web in order to engage in such illicit activity there, but rather to objectively present everything there and raise awareness of it. This report is the key to your understanding of the layers of the internet and give a view for the whole picture of the dark web.

References:

ACSC. (2020, October 19). *Defending against the malicious use of the Tor Network*. Defending Against the Malicious Use of the Tor Network. Retrieved January 3, 2023, from https://www.cyber.gov.au/acsc/view-all-content/publications/defending-against-malicious-use-tor-network

Beshiri, A. S., & Susuri, A. (2019, March 4). *Dark web and its impact in online anonymity and privacy: A critical analysis and review*. Journal of Computer and Communications. Retrieved January 3, 2023, from https://www.scirp.org/journal/paperinformation.aspx?paperid=91242

Broadhurst, R., & Ball , M. (2022, August 4). *How the world's biggest dark web platform spreads millions of items of child sex abuse material - and why it's hard to stop*. The Conversation. Retrieved November 9, 2022, from https://theconversation.com/how-the-worlds-biggest-dark-web-platform-spreads-millions-of-items-of-child-sex-abuse-material-and-why-its-hard-to-stop-167107

Carreiro, A. (2020, February 10). *8 common hacking techniques that every business owner should know about*. OceanPoint Insurance. Retrieved November 9, 2022, from https://www.oceanpointins.com/ri-business-insurance/cyber-liability-insurance/8-common-hacking-techniques/

Cooper, S. (2022, December 13). *10 best dark web monitoring tools for network admins*. Comparitech. Retrieved January 3, 2023, from https://www.comparitech.com/net-admin/best-dark-web-monitoring-tools/#The_best_dark_web_monitoring_tools_for_network_admins

Farivar , C. (2017, May 5). *Creator of infamous Playpen website sentenced to 30 years in prison*. Ars Technica. Retrieved January 3, 2023, from https://arstechnica.com/tech-policy/2017/05/creator-of-infamous-playpen-website-sentenced-to-30-years-in-prison/

Finklea, K. (2017) Dark Web. Congressional Research Service, Washington DC, 10 March 2017, 1-19. https://fas.org/sgp/crs/misc/R44101.pdf

Fraudwatch, A. (2021, August 3). *Expert explanation: History of the dark web - digital brand protection*. FraudWatch. Retrieved November 9, 2022, from https://fraudwatch.com/expert-explanation-history-of-the-dark-web/

Gupta , A., B Maynard, S., & Ahmad, A. (2019). The Dark Web Phenomenon: A Review and Research Agenda . Perth; Abhineet Gupta, Sean B Maynard and Atif Ahmad. From https://arxiv.org/ftp/arxiv/papers/2104/2104.07138.pdf

Hiley, C. (2022, October 4). *Brief history of cybersecurity & hacking*. Cybernews. Retrieved January 3, 2023, from https://cybernews.com/security/brief-history-of-cybersecurity-and-hacking/

Janson Media. (2021). *Full Documentary: Dark Web*. *YouTube*. Retrieved January 3, 2023, from https://www.youtube.com/watch?v=cL3pEe47qyk&t=32s&ab_channel=JansonMedia.

Kastner, E. (2020, February 7). *History of the dark web* . Managed IT Services, Copiers, Telephony. Retrieved November 9, 2022, from https://www.soscanhelp.com/blog/history-of-the-dark-web

Kayyali, A. (2022, August 16). *How cyber security experts can make dark web threat intelligence*. Inside Telecom. Retrieved January 3, 2023, from https://insidetelecom.com/how-cyber-security-experts-can-make-dark-web-threat-intelligence/

Mash, S. (n.d.). *Onion Routing explained - privacy HQ*. PrivacyHQ. Retrieved November 9, 2022, from https://privacyhq.com/documentation/onion-routing-explained/

Newsthink. (2022). *One Mistake Took Down this 29-Yr-Old Dark Web Drug Lord*. Retrieved January 3, 2023, from https://www.youtube.com/watch?v=HBTYVVUBAGs&t=1047s&ab_channel=Newsthink

S. Beshiri , A., & Susuri, A. (2019, March 4). *Dark web and its impact in online anonymity and privacy: A critical analysis and review*. Journal of Computer and Communications. Retrieved November 9, 2022, from https://www.scirp.org/journal/paperinformation.aspx?paperid=91242

Srivathsav, R. (2022, June 24). *Tor nodes explained*. Medium. Retrieved January 3, 2023, from https://medium.com/coinmonks/tor-nodes-explained-580808c29e2d

Staff, F. L. (2021, December 21). *Dark web crimes*. Findlaw. Retrieved November 9, 2022, from https://www.findlaw.com/criminal/criminal-charges/dark-web-crimes.html

Wilson, C. (2022, February 11). *How does dark web help cyber security experts improve business security?* System Soft Technologies. Retrieved November 9, 2022, from https://sstech.us/blogs/dark-web-cybersecurity-business-security/

Youngren, J. (2020, June 15). *The bright side of the dark web*. Dark Reading. Retrieved November 9, 2022, from https://www.darkreading.com/risk/the-bright-side-of-the-dark-web

Toohil, R. (2022, September 8). *What is a dark web scanner? get a free scan today*. Identity Guard. Retrieved January 3, 2023, from https://www.identityguard.com/news/what-is-a-dark-web-scanner