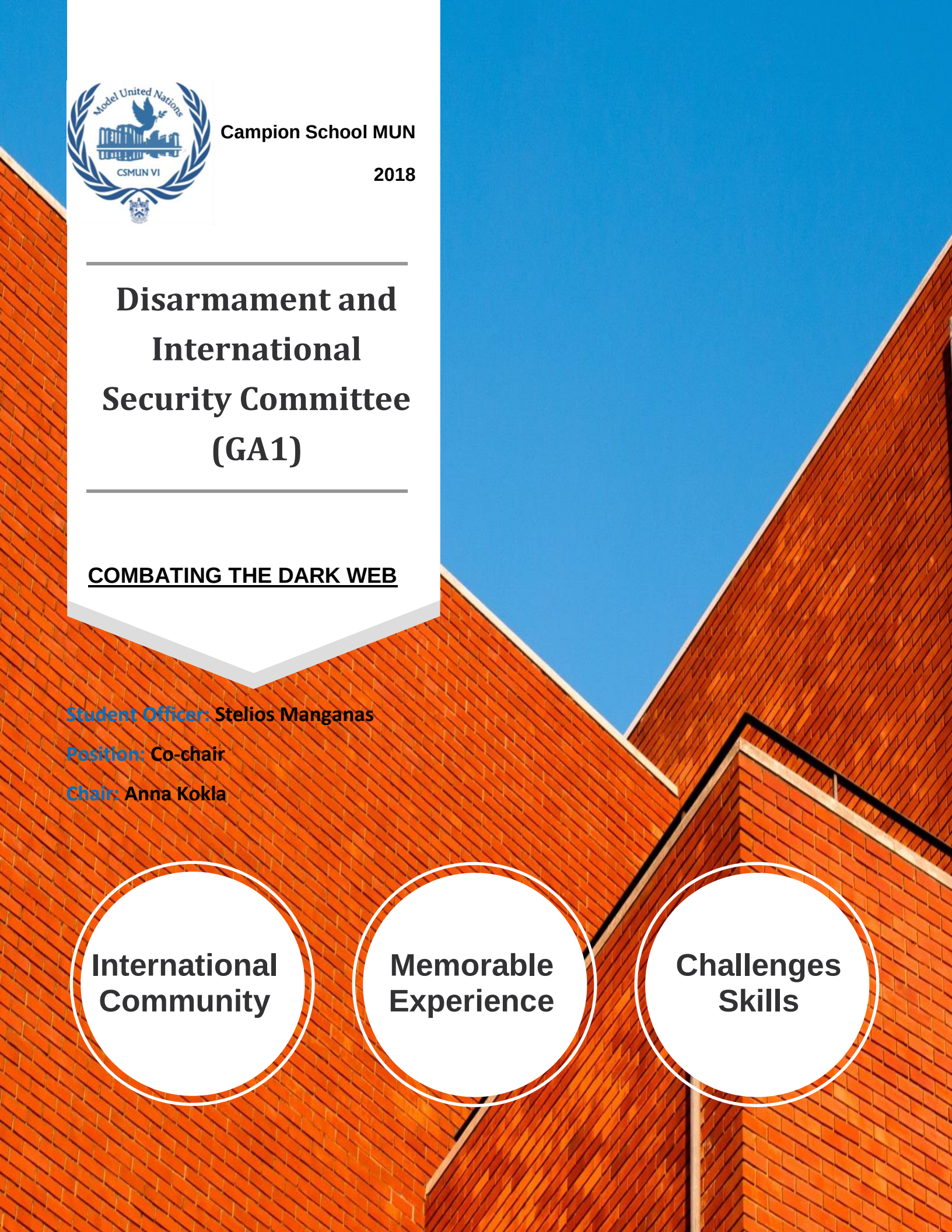

Campion School MUN

2018

Disarmament and International Security Committee (GA1)

COMBATING THE DARK WEB

Student Officer: Stelios Manganas

Position: Co-chair

Chair: Anna Kokla

International Community

Memorable Experience

Challenges Skills

Table of Contents

INTRODUCTION

The Dark web is a subpart of the world wide web accessible only by special means of software. It is nicknamed “dark” because sites or entities on it cannot be indexed by a web crawling browser, such as Google. That makes it hard for ordinary people, and law enforcement, to find specific websites and data strings.

The dark web has been misused by criminal organisations to act as a “black market” sales floor. This is an issue that has to be addressed. Furthermore, the anonymity created by the dark web has created a space where people can express ideas and communicate freely without fear of government interference.

The existence of such a cyberspace is not prohibited but what is prohibited is the illegal actions that it hosts and the Human Rights on the World Wide Web that its existence violates. Nevertheless, the Dark web also provides a space of free speech and communication of ideas for individuals that live in oppressed countries or under totalitarian regimes. Furthermore, “whistleblowers’ also spread information through platforms on the Dark Web.

DEFINITIONS OF KEY TERMS

- **Search Engine**

A program used for finding particular sites on the World Wide Web.

- **World Wide Web**

The information system on the Internet which allows documents to be connected with hyperlinks

- **Deep Web**

The deep web can be defined in the easiest way as an unlisted database of websites that are not registered to any search engine and have their virtual address hidden. These websites are of course not “hosted” by huge mega servers but instead by local small or medium sized isolated server units. The deep web can be alliterated to a street of houses within a city but each house does not have a house number, which makes it hard to access.

- **Dark Web**

A subpart of the World Wide Web inside the deep web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable. Criminal/terrorist activities are organized and planned/funded through here. Most common program for surfing the “dark web” is TOR and recently I2P programing

- **TOR Program**

The most typical program used for browsing the dark web safely and anonymously (uses Onion Routing)

- **Onion Routing**

Onion routing is a technique for anonymous passing of data over a network. In an onion network, messages are encrypted in layers of encryption and then decrypted at the receiving end.

- **Dark Web Markets**

Dark Web Markets are online hidden platforms that all sorts of organized crime take place. For example, sale of illegal narcotics and weapons, hiring professionals to carry out assassinations or create disruption to organisations / countries using cyber tools. Other crimes committed are the sale of child pornography and human trafficking / high-end prostitution. Personal data of individuals can be sold and bought in Deep Web Markets

- **World Wide Web**

The World Wide Web (WWW) is the combination of all the data on the Internet that are using HTTP .

- **Hyperlinks**

A link from a hypertext document to another destination, activated by clicking on a highlighted word or image.

- **Silk Road Market**

Silk Road was an online black market and the first modern darknet market, best known as a platform for selling illegal drugs.

TIMELINE

Date	Description of Event
2000	Freenet networks begin hosting content
2002	TOR network developed by US naval research laboratory
2003	I2P connections were made possible for the first time
2006	TOR becomes a non-profit orginisation
2009	Bitcoin starts (used in exchange in deep web traders)
2011	Silk road market opens up
2012	Other Silk Road competitors shut down, making Silk Road huge
2013	Silk road is shut down after the arrest of its owner
2015	Founder of Silk Road sentenced to life
2016	Multiple other sites “fill in the gap” displayed in the black market

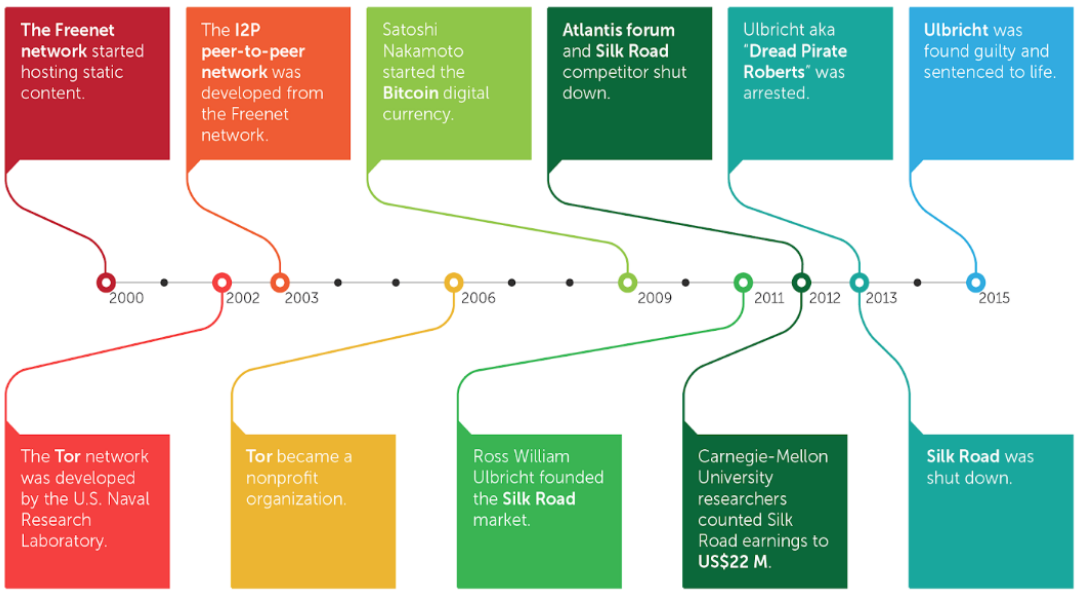

Figure 1: Timeline of the Dark web and the major organisation involved in the rise of its popularity and use.

TOPIC DISCUSSION

The aim of this committee will be to resolve the problems created by the existence of uncharted data spaces such as the “Dark web”.

In a few words, the Deep Web is anything a search engine cannot find. It is NOT only used by criminals or for illegal things. The Deep Web contains content that cannot be indexed by traditional search engines like Google/Yahoo/Bing. In order to clarify, **the Dark web is a subpart of the Deep web which is itself a subpart of the World Wide Web.** A number of problems come along with such a platform.

The problems include:

- Unlabelled or mislabelled links, or sites that are disguised as one thing and turn out to be much worse.
- Purchase of drugs, cloned credit cards, and guns in the dark web is typical.
- No record or paper trail of anything that occurs in this cyberspace. This anonymity has several dire implications such as lack of respect and no fear of the law, anarchy.
- The deep web has become a corrupted hub of criminal activity.
- Illegal bidding market places similar to Ebay have been set up on the deep web to sell these illegal goods or services.
- It was until October 2013 that the general public really began to become aware of it. This was due to the primary deep web marketplace, ‘The Silk Road’

The Dark Web is a difficult entity to monitor because of the vastness of incoherent data, the very high levels of encryption and all the security and identification precautions taken by the owners and administrators of dark web marketplaces.
In addition the existence of the deep web violates some of the Human Rights on the World Wide Web.

- **Additional Information:**
  - Deep web consists of mostly incoherent digits or letters
  - All sorts of dead or not properly set up web pages become unlisted and end up there
  - Everything made “off the books” was purposeful in an effort to hide evidence
  - This vastness of meaningless and unlisted data is being exploited
  - In practise the dark web cannot but MUST be regulated

The Human Rights on the World Wide Web basically exist in two sectors, the rights of privacy and the rights of open access. The Dark web not only hosts criminal activities but it also breaks both these principles.

- **Activities**

1. Drug dealing
2. Extortion/Scams
3. Funding of criminal/Terrorist organisations
4. Proliferation of Prohibited content-material
5. Sale of weapons
6. Human trafficking and prostitution
7. Hire of illegal services “Hacker4sale” “Hire_your_hitman.com”
8. Sale of private data
9. Money laundering

CAUSES

The causes of the existence of the Dark Web are not clear or simple but can be explained as "A need for the virtualisation and technological modernistation of cyberterrorism and any sort of lucrative criminal activity housed in the already existing Deep web"

- **Drug dealing**

Traditionally narcotics trade happens through direct contact of the buyer with the seller. In the dark web markets narcotics can be purchased without human interference. Once a purchase is complete the narcotics are shipped to ones house through mail disguised as another unsuspicious item.

- **Extortion/Scams**

Many websites on the deep web that appear to be providing services or sell contraband are in fact a scam where Dark web users are tricked into buying non-existing items. Furthermore, communication between extortion gangs happens in the Dark Web, also data required for extortion is also acquired with the help of Dark web services

- **Funding of criminal/Terrorist organisations**

Terrorist organisations use cyberspaces such as the Dark web to raise funds in order to continue running their operations. This can be in the form of trading of captured loot or human trafficking. Other criminal organisations sell their services or their contraband online.

- **Proliferation of Prohibited content-material**

The anonymity created by the Dark web can allow for the sale and purchase of blueprints or live nuclear weapons. Such weapons can be purchased by third party organisations or countries seeking to develop their nuclear arsenal. This goes against the nuclear non-proliferations act.

- **Sale of weapons**

The sale of weapons is made easier in the Dark Web since illegal weaponry can be purchased online and then picked up at a designated location or parts of the weapon are shipped individually and then the buyer has to construct the weapon. Such weapon dealerships go against policies that countries may impose on their weapon laws.

- **Human trafficking and prostitution**

Such activities are organised and run through the Dark Web since the high-ranking members of a gang involved in this can give out orders and requests without the fear of law enforcement. Same goes with human trafficking networks.

- **Hire of illegal services**

Illegal services can be ordered in the dark web to carry out certain tasks. For example, there have been accounts where hacking teams can be hired *for a reasonable price* to shift election tides or to cause trouble to rival corporations or even target specific individuals with Denial of service attacks. Other services include the theft of online accounts or bank account details. Some websites that have now been shut down even claimed to provide hitmen for hire in order for assassinations to be carried out.

- **Sale of private data**

Private data of individuals can be gathered on sold upon request of the buyer. This sale of data limits the right of one's privacy and is highly illegal in many countries.

- **Money Laundering**

Money laundering happens in the Dark web through virtual casinos or so called “advisory services” where the individual can gamble with non-taxable money (presumably from illegal activities) and the casinos have a fixed win rate, meaning that at least 95% of the money put in is guaranteed to come back. This money can now be put into taxable income and is now considered legal since it was “won” in a virtual casino. The advisory services exploit works by the individual setting up an advisory service in the Dark web and then registering it to himself. Following that the individual makes a huge payment of the illegal money to his own advisory service, then the money earned in the advisory service are considered legal and can be registered into one's taxable income and can therefore be spent legally without the fear of tax services not finding “justifiable source of income”.

POSSIBLE SOLUTIONS

- **Creation of "Tools"** – Specific investigation technologies and methods to analyse online criminal activities, primarily the Dark Web Monitor. Funding for these activities should not be neglected.
- Efforts to continuously disrupt criminal activities effectively. INTERPOL can significantly contribute to those efforts.
- **Threat analysis** – Reports about understandings of current cyber threats based on deep understanding of internet phenomena with criminal or terroristic intentions
- Experts have also proposed the idea of an overall security system where people will need an identification in order to access it. This however goes against their privacy.
- Efforts to deanonymize the TOR network
- International law enforcement foundations, such as the International Criminal Court, can create an information pool with all the necessary data for the prosecution of the criminals.
- Cooperation between the UN member states, and major organizations is of vital importance. The United Nations Office on Drugs and Crime (UNODC) can supervise and monitor any actions taken by the respective member states.

MAJOR COUNTRIES & ORGANIZATIONS INVOLVED

Organizations

IASAP- International Association of Security Awareness Professionals

CSA- Cloud Security Alliance

International Association for cryptologic research

NCSA- National Cyber Security Alliance

ISF- International Security Foundation

Countries

Colombia

Colombia is one of the main countries responsible for the production of the illicit drug-cocaine.

European Union

The European Union has a long-standing policy on protecting its citizens rights and guaranteeing their safety from all sorts of crime. Since the Dark web has a become a hub of criminal activity it is a sensible idea for all EU countries to stand for solutions in the Dark Web issue.

Japan

Japan has firmly taken a stand against the proliferation of nuclear weapons and acquirement of weaponry from non-legal sources. Since the

Mexico

Mexico is notorious for many people accessing drug markets through the dark web. In fact, over 15 darknet drugs were found in Mexico.

Russia

Many of the services provided in the Dark web are housed in servers in Russia, along with most of the hackers for hire

United States of America

The USA, being a country very determined to win the “war on drugs” is greatly interested in taking actions that would limit or put a strain to drug cartels and other criminal organisations to operate in their countries.

UN INVOLVEMENT: Relevant Resolutions & Treaties

At a debate of the Security Council in June, the UN Under-Secretary-General of Disarmament Affairs, Izumi Nakamitsu, expressed concerns regarding non-proliferation issues. One of the growing threats, she explained, was that of a non-state actors obtaining Weapons of Mass Destruction from the darknet.

- Council of Europe Cybercrime Treaty, 2000
- Creation of global culture of cybersecurity (A/RES/57/239)
- European Parliament Resolution of 29 October 2015 on the follow up to the European Parliament Resolution of 12 March 2014 on the Electronic Mass Surveillance of EU citizens (2015/2635(RSP))
- Report on 'Human rights and technology "the impact of intrusion and surveillance systems on human rights in third countries' (2014/2232(INI))
- European Council Resolution of 28 January 2002 on a Common Approach and Specific Actions in the Area of Network and Information Security

Research Questions

Although the study guide should provide sufficient guidelines and information on the topic, further research is needed. Different views on this must be represented, but must always remain accurate, realistic, creative and within topic. The delegates should research the topic in depth in order to effectively conceptualise the information. Concerning the countries they represent, they should conduct thorough research so as to learn their countries policy and stance in terms of the issues debated in the committee.

Bibliography

- Digital Journal (2017 November) -http://www.digitaljournal.com/pr/2160139
- Wired (2018) -https://www.wired.com/2015/06/dark-web-know-myth/
- Trend Micro Dark Web timeline photograph- https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/from-tor-to-ulbricht-the-deep-web-timeline
- Deep Dot Web (Public open discussion group used as a means to estimate public opinion of the deep web)- https://www.deepdotweb.com/marketplace-directory/categories/top-markets/
- What Is (Information on what the WWW is)- https://whatis.techtarget.com/definition/World-Wide-Web
- MDN web docks (Information on hyperlinks) https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_are_hyperlinks
- Freenet Project (information site on Freenet project)- https://freenetproject.org/pages/about.html
- Silk Road Drugs (silk Road related information)- https://silkroaddrugs.org/guide-on-how-to-access-the-silk-road-3-0/
- The Japan Times (Information on Japanese state views on the dark web)- https://www.japantimes.co.jp/news/2017/06/19/reference/sinister-world-dark-web-just-clicks-away/