Forum: GA3: Social, Humanitarian and Cultural Committee

Issue: Taking further action to prevent the trading of illegal goods and services on the dark web

Student Officer: Mr. Andreas Thaisen Løvengreen

Position: Deputy Chair of the 3rd committee

**Introduction:**

According to the International Telecommunication Union, 40% of the world’s population uses the web for news, entertainment, communication and other purposes. The World Wide Web for citizens in developed countries has become indispensable for daily tasks, such as research, getting informed about daily news or even ordering food online. Even though it already seems like the visible information on the World Wide Web is infinite, it only contains 0.03% of what the World Wide Web holds, this is known as the surface Web. The other 99.97% is called the Deep Web.

The Deep Web is invisible by search due to technical reasons, but there is a part of it that has been intentionally hidden, which is the Dark Web. Due to this circumstance, the Dark Web has got the potential to host illegal websites involved in crimes like pornography, terrorism, and trading of illegal goods etc.

Yet, the Deep Web is useful for positive purposes as well. Whistleblowers, journalists as well as conventional citizens that want their identity to be respected use the Deep Web. Hereby, the Dark Web sentences a dilemma between the right to privacy and cyber security.

**Definition of Key Terms:**

World Wide Web

The World Wide Web (WWW) is an information system on the Internet, in which documents are connected to other documents using Hypertext links.

Internet

The two terms, Internet and World Wide Web are often used as synonyms. The Internet is the network through which the World Wide Web can be accessed.

Deep Web

According to the Global Commission on Internet Governance, the term Deep Web is used to denote classes of content on the Internet. Search engines do not index that.

Dark Web

The Global Commission on Internet Governance defines the Dark Web as a part of the Deep Web that has been intentionally hidden and is inaccessible through standard web browsers.

The Onion Routing

Created by the US Naval Research Laboratory in 2002, the Onion Routing is a software that creates a connection between several computers at a time that facilitates to hide an encryption. Hereby, the start and end point of information traveling through the dark web remains unknown. The Onion Routing can be used for illegal purposes such as darknet markets, but also enables the right to anonymity.

Darknet Markets

A darknet market is any market on the dark web meant for illegal purposes. To access a darknet market a user needs to use software, such as The Onion Routing (TOR) or The Invisible Internet Project (I2P).

**Background:**

The surface web in contrast to the deep web can be easily monitored. The deep web is not visible due to technical reasons, such as the login into private accounts, while the dark web is even harder to trace. The reasons for its invisibility are softwares such as The Onion Routing or the Invisible Project (I2P).

The Dark Web’s use is not illegal per se; it is the potential it holds to host illegal activities, such as pedophilia, murder, heist, and trafficking that make it dangerous. These activities (if implemented online) are called cybercrime. The counterpart of cybercrime in the deep web is the right to privacy. TOR or any other software that enable the right to anonymity; they can therefore not be blamed for cybercrime as they also provide humanity with numerous benefits

Human Rights in the World Wide Web

Referring human rights in the World Wide Web includes taking into consideration of a wide range of issues. The Internet rights vary from:

* universal access to networks
* access to information and knowledge
* net neutrality, copyright and free knowledge
* diversity and participation in cultural life
* creation and sharing
* open standards to anonymity
* identity, surveillance and encryption
* communication and information security
* protection against cybercrime
* rectification of personal data

Commercial services and the dark web

A commercial service is defined as an exchange of goods. In the Dark Web, those ‘goods’ are illegal content. The currency used on the Dark Web is bitcoins, which is considered a decentralized currency. Instead of a central authority e.g. bank or government, a network of users, called miners, control and verify transactions. These transactions are directly published onto a “Block-Chain”.

The Hidden Wiki offers a wide range of darknet markets specialized on drugs, exotic animals, and weapons. Some of these websites are even specialized in continents; they may for instance only trade weapons throughout Europe. The arms on darknet markets are sent discreetly if not in pieces.

One of the most famous commercial services in the history of the dark web is the “Silk Road”. This is a darknet market that can be compared to “e-bay”. The difference is the illegality of the goods being sold.

More radical darknet markets are those for murder and heist. Such websites offer services to kill and to steal. The Assassination Market, for instance, creates a list of targets. Their assassination date is then bet upon in bitcoins. By executing the murder on the date that is bet upon, the user wins the bet and therefore the sum of money.

Pedophilia through the dark web

Pedophilia on the dark web works like a darknet market too. Yet it deserves its own section due to its broad content. Similar to a drug darknet market, pedophile pictures can be bought in exchange for bitcoins. However, the Dark Web also offers publishing and discussion forums for pedophiles.

Terrorism and cyber security

The cyberspace is a whole new dimension for military defense. An attack on a computer that controls the infrastructure can be considered as an act of war; the consequences can be political and even military failure, but also the deletion of crucial data and evidence. This raises the issue of cyber-attack and cyber defense. Cyber defense is, in any case, more expensive than the former. The reason for that is that cyber defense should never fail, whereas a cyber-attack needs to succeed only once. That is why the United States bases its cyber defense on the capacity to attack.

The concepts of the Dark Web and Terrorism seem to be made for each other. Terrorists look for messaging platforms in which they remain anonymous. Apart from that, the Dark Web offers forums in which potential terrorists or curious radical individuals can state their opinion without being suspected.

**Timeline:**

1990

Creation of Arpanet operational Network, known as the Internet. 2.6 million users connect.

1994

Concern about Internet Security triggers American computer services company, NetScape, to develop Secure Socket Layer encryption for the safety of online transactions.

1998

First World Summit on the Information Society (WSIS).

2002

Creation of TOR Project December 12th

2003

World Summit on the Information Society becomes a triparty Summit due to participation of government, private companies and civilians.

March 2006

Creation of National Security Division (USA)

2009

Aurora Attacks hit 34 companies among which is Google for intellectual property purposes.

2010

US Cyber Command goes operational.10 ‘Stuxnet’ disrupts Iran’s Nuclear program.

2013

FBI shuts down Silk Road, a popular darknet market.

3. Nov 2014

Robert Hannigan, Director of the Government Communications Headquarters of the United Kingdom, accuses US tech giants Whatsapp, twitter, and Facebook to be the command and control websites for terrorist activities.

2014

Facebook announces that it is hosted on TOR as well.

**Previous UN Involvement:**

* Creation of global culture of cybersecurity (A/RES/57/239)
* Council of Europe Cybercrime Treaty, 2000
* 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))” by the European Union
* European Council Resolution of 28 January 2002 on a Common Approach and Specific Actions in the Area of Network and Information Security