Committee: Security Council

Issue: Cyber Security in the dark web era

Student Officer: Martina Sánchez Medina

Position: Deputy President

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, heist 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.[1]

[1] Hornby, Albert Sydney., Sally Wehmeier, Colin McIntosh, Joanna Turnbull, and Michael Ashby. *Oxford Advanced Learner's Dictionary of Current English*. Oxford: Oxford UP, 2005. Print.

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.[2]

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.[3]

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.[4]

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).[5]

BACKGROUND INFORMATION

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).

[2] "The Impact of the Dark Web on Internet Governance and Cyber Security" <https://www.ourinternet.org/research/impact-dark-web-internet-governance-and-cyber-security>
[3] "The Impact of the Dark Web on Internet Governance and Cyber Security" <https://www.ourinternet.org/research/impact-dark-web-internet-governance-and-cyber-security>
[4] "The Onion Router Tor" <https://www.techopedia.com/definition/4141/the-onion-router-tor>
[5] "Darknet Market" <https://en.wikipedia.org/wiki/Darknet_market>

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.[6]

As stated above, ensuring these rights can be hard due to their controversy. In the list above the dark bullets support openness of the web and the white the right to privacy and anonymity. The way in which these rights are implemented vary from nation to nation, yet some parameters are already set by the international declaration of human rights.

However, the existing precautions do not completely secure all rights e.g. the lack privacy if we take the measures taken by the United States of America after the catastrophe on September 11th into consideration. Having viewed this example, it is only fair to take into consideration that democracy and participation in Internet governance are also a right. By that is meant that since all citizens of the world use the Internet, all nations are equally responsible for the actions undertaken on the dark web. No nation should act as police nor be given responsibility for actions online since the Internet is 'nationless'.

[6] Burch, Sally. "The Global Governance of the Internet." *Foreign Policy Journal JAN/APR 2015*. Vol. III. Quito: Ministry of Foreign Affairs and Human Mobility of Ecuador, 2015. 21-33. Print.

Refocusing to the main point of human rights, several agreements have been decided in the past to promote human rights on the Internet. Such a document is Declaration of Principles of the World Summit on the Information Society (WSIS) held in Geneva which in its Article 4 recognizes that:

> "Communication is a fundamental social process, a basic human need and the foundation of all social organization. It is central to the Information Society. Everyone everywhere should have the opportunity to participate and no one should be excluded from the benefits the Information Society offers."[7]

However, the Geneva Declaration of Principles did not progress enough due to the lack of social equality as well as the fact that it could not adapt to the constant technological developments.

Another example for human rights measures is the Brazilian Civil Rights Framework for the Internet, which clearly answers the question of what right comes ahead of the other, privacy or cyber-security, recognizing cyber-security as the most important without forgetting the latter. Some conditions set by the Framework are that companies are compelled to provide the technical facilities to offer privacy to its users and that it is illegal to share user data, without clear consent.

TOR and the Hidden wiki

The Onion Routing Project (TOR) is a free software first created by the US Naval Research Laboratory. TOR does not provide anonymity per se, but it allows the exchange of information to be anonymous. The exact way in which TOR allows this to happen is not necessary for the purposes of this paper, but it is important to know that TOR is the key to the Dark Web. TOR helps journalists get in contact with whistleblowers or victims that prefer their identity to be respected. It also allows people working for NGO's to work without being traced.

However, TOR has also a negative face that is the Hidden Wiki, which is only accessible with this software. It is the platform through which most hidden commercial services can be found; they vary from drug dealing, pedophilia, to drugs etc. The Hidden Wiki also hosts search engines that look for the hidden content or messaging websites that

[7] Burch, Sally. "The Global Governance of the Internet." *Foreign Policy Journal JAN/APR 2015*. Vol. III. Quito, Ecuador: Ministry of Foreign Affairs and Human Mobility of Ecuador, n.d. 21-34. Print.

can be used by terrorist organizations. In the following sections, more information is provided concerning the connection of the hidden wiki and criminal acts.

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.

One thing should be clear and it is that there are two types of pedophiles on the Dark Web. Some, who contribute to this illegal activity by using its content, but are not active outside of the web, and others, who are active in finding new ways to live their sexual attraction. The latter is more likely to be active in discussion forums as well.

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. An example of a cyber-attack is the attack against the Catalan Police by Phineas Fischer. After practicing his moves for weeks, Fischer managed to hack the passwords of Catalan police authorities. He later uploaded a video about the procedure and even wrote a guide for other hackers.[8]

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.

However, Pierluigi Pagani from the European Union Agency for Network and Information Security assures the "near-absence" of terrorism on the Dark Web. According to him and other experts, terrorists prefer the usage of the surface web. This is for the following two reasons: Firstly, terrorist propaganda on the surface web gets more attention from a larger audience. Secondly, the Dark Web is both unstable and slow.[9] Although these characteristics of the Dark Web seem to be a reason why terrorism is not yet promoted through it, it can for sure serve as an alternative if the current methods of terrorist get detected.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

Internet Corporation for Assigned Names and Numbers

The Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization responsible for the IP-addresses on the Internet. ICANN is responsible for the assignment, country code and server management functions. This gives ICANN full control over the Domain Name System (DNS), which basically controls content representation on the Internet. As ICANN is incorporated under the US law it is criticized for acting as the mean for the US to control the web. However, the existence of the Regional Internet Registries (RIR) controlling ICANN as well as the seven keys around the world given to online security experts ensure that ICANN does not abuse its power.

[8] "Hacker Teach How He Hacked Spain's Catalan Police Union Website" <https://www.deepdotweb.com/2016/05/26/police-catalan-hack/>

[9] 'Terrorists and dark web, what is their relationship?", Pierluigi Paganini <http://securityaffairs.co/wordpress/45755/terrorism/dark-web.html>

United States of America (USA)

The power that countries have over the Internet is important as cyber-governance goes hand in hand with cyber-security. According to the Global Cyber-Security Index the USA, followed by Canada, has got the best 'readiness' for a cyber-attack. But it is not only the power to defend itself that involves the USA, but also the power it had to control the Internet in the past through ICANN, whose privatization was put on hold after 9/11. Pressure from the international community led a slow separation between USA and ICANN assured by the "Affirmation Commitments" in 2009. However, in 2013 Snowden's revelations about NSA surveillance over the Internet contradicted these documents. Shortly after that, the US government announced that it would give up state control of ICANN.

Malaysia

According to the ITU Malaysia ranked third in the Global Cybersecurity Index 2014. This makes her a leading country in the cybersecurity field of Asia-Pacific. However, the country faced various incidents of attacks during the previous years. With the aim of fighting cyber-attacks the Malaysian governments supported in its 2016 agenda the improvement of cyber security measures through regional cooperation as well as collaboration between governments and various agencies.

New Zealand

New Zealand is one of the counties that are most linked to the Internet with over 80% of its population having access to the Internet at home. Recognizing the various threats in the internet New Zealand has invested a lot in the improvement of its cyber security infrastructure. Their efforts have been recognized by the International Telecommunication Union ranking it 4th in the Global Cybersecurity Index of 2014.

Global Commission on Internet Governance

The Global Commission on Internet Governance (GCIG) parameters for the Internet is openness, safety, trust and inclusion. One the one hand, GCIG advocates for freedom on the Internet. In other words, it fights for freedom of expression and net-neutrality. According to GCIG, the Internet is under pressure by terrorist and criminals who exploit it, but also by "unthinking, opportunistic and unprincipled corporate and government activities". Hereby, GCIG condemns full surveillance online coming from governments or the private sector while it strongly warns about cybercrime. With regard to the "privacy vs.

cyber security" dilemma GCIG supports that end-to-end encryption, that enables anonymity, should be regulated by law-enforcement.

The International Telecommunication Union (ITU)

The ITU is the United Nations specialized agency for information and communication technologies. ITU takes a human rights approach on the issue of cyber-security. Its vision and aim is to connect all citizens around the world through the World Wide Web. Hereby they fight for the right of access to the Internet. According to ITU's statistics Europe, North America (USA and Canada), Brazil and the Commonwealth nations are most committed to cyber-security. Furthermore, ITU provides guidelines and information related to cyber security.

TIMELINE OF EVENTS

Date	Description of Event
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)
2000	ILOVEYOU worm attack governments and private systems, such as the "Financial Services Information Sharing and Analysis Center". In the search for common computer crime laws, the US supports the Council of Europe Cybercrime Treaty.
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.
2005	World Summit on the Information Society is held once again
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

UN INVOLVEMENT: RELEVANT RESOLUTIONS, TREATIES AND EVENTS

- 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

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

In the crimes committed on the Dark Web, there is never only one guilty side. Both website admin and website visitor are equally responsible for the crime. That is the reason why measures have been taken addressing both groups.

An example in which the website creators were punished, is the case of Silk Road. Silkroad existed as one of the first online drug markets on the Dark Web. On October 2nd, 2013 the FBI Seizure Notice replaced the Webs login. Later the admins of Silk Road

[10] "30 years of risky business: A cybersecurity timeline" <https://gcn.com/articles/2013/05/30/gcn30-timeline-cybersecurity.aspx>

reestablished the web-site in 2013. Silk Road 2.0 was hacked and many of it employees were imprisoned. Since then, other websites have decided to take the name Silkroad 3.0, due to its fame. Nowadays, the number of people visiting centralized markets like Silkroad is decreasing for their instability. However, this approach has managed to multiply the number of darknet markets.

Another attempt has been that of impersonating a darknet market to reach the visitors of such. From February 20th, 2015 to March 4th, 2015 an FBI agent with the pseudonym “Playpen” hosted their own pedophilia website. From 215.000 subscribers 137 were charged with the crime. This measure has punished more people for their crime than the first one.

POSSIBLE SOLUTIONS

The complexity of the issue as it has been described previously requests a variety of specified and effective solutions. Improving the international legislation related to the issue of cyber-security is a number one priority for the international community. The constantly changing technological facts require an update to international law. Stricter and clearer punishments for criminals are also necessary in order to discourage potential criminals.

One should also bear in mind that a consensus related to the dilemma of privacy vs. cyber-security needs to be found. Apart from that measures aiming at allowing the accumulation of information about the dark web users and their actions need to be discussed. Furthermore, as stated above one of the main bones of contention of the current cyber-security policies is the issue of surveillance of individuals. Delegates need to decide to what extent a surveillance of citizens is necessary as well as solve the issue of ICANN by proposing a way of ensuring an unbiased control of the internet.

Experts have also proposed the idea of an overall security system for accessing the internet where users will need an identification using a unique password and further information to access the world wide web. Though this idea will help in the easier identification of users it goes directly against the right of privacy.

Aiming at deanonymizing the TOR network experts have also proposed the creation of voluntary nodes for the TOR databases. Considering the fact that newly established criminal platforms search for databases to “advertise” their websites, the authorities’

establishing of their own nodes to mislead and arrest criminals would be an efficient way of tackling the creation of future dark websites.

Last, but not least, an analysis of the data collected related to dark web transactions as well as the activity of suspicious users on various platforms is pivotal since this way authorities will be able to identify criminals and move to their apprehension.

BIBLIOGRAPHY

"Beautiful People Data Has Been Leaked on to the Deep Web. Where? We Explain All." PC Advisor. N.p., n.d. Web. 9 July 2016. <http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-joc-beautfiulpeople-3593569/>.

Bergman, Michael K. The Deep Web: Surfacing Hidden Value. Place of Publication Not Identified: BrightPlanet, 2000. Bright Planet. Web. 9 July 2016. <http://brightplanet.com/wp-content/uploads/2012/03/12550176481-deepwebwhitepaper1.pdf>.

Burch, Sally. "The Global Governance of the Internet." *Foreign Policy Journal JAN/APR 2015*. Vol. III. Quito, Ecuador: Ministry of Foreign Affairs and Human Mobility of Ecuador, n.d. 21-34. Print.

Chertoff, Michael, and Tobby Simon. PAPER SERIES: NO. 6 — FEBRUARY 2015 The Impact of the Dark Web on Internet Governance and Cyber Security (n.d.): n. pag. The Impact of the Dark Web on Internet Governance and Cyber Security. Chatham House, Feb. 2015. Web. 9 July 2016. <https://ourinternet-files.s3.amazonaws.com/publications/GCIG_Paper_No6.pdf>.

"Dark Net Markets Comparison Chart." Deep Dot Web. N.p., n.d. Web. 9 July 2016. <https://www.deepdotweb.com/dark-net-market-comparison-chart/>.

"Darknet Market." *Wikipedia*. Wikimedia Foundation, n.d. Web. 26 Aug. 2016. <https://en.wikipedia.org/wiki/Darknet_market>.

"The Dark Web and Cybersecurity: Let There Be Light?" Security Intelligence. N.p., n.d. Web. 9 July 2016. <https://securityintelligence.com/news/dark-web-cybersecurity-let-light/>.

Farrell, Maria. "Quietly, Symbolically, US Control of the Internet Was Just Ended." The Guardian. Guardian News and Media, 14 Mar. 2016. Web. 13 July 2016. <https://www.theguardian.com/technology/2016/mar/14/icann-internet-control-domain-names-iana>.

"FBI Hosted Images of Child Sexual Abuse on Dark Web to Hack Pedophiles around the

World." The Next Web RSS. N.p., 24 Jan. 2016. Web. 10 July 2016. <http://thenextweb.com/insider/2016/01/24/fbi-hosted-images-of-child-sexual-abuse-on-dark-web-to-hack-pedophiles-around-the-world/ - gref>.

"5 Things I Learned Infiltrating Deep Web Child Molesters." Cracked.com. N.p., n.d. Web. 10 July 2016. <http://www.cracked.com/personal-experiences-1760-5-things-i-learned-infiltrating-deep-web-child-molesters.html>.

"GCI Charts & Tools." ITU Committed to Connecting the World. ITU, n.d. Web. 11 July 2016. <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2014_charts_and_tools.aspx>.

"Hacker Teach How He Hacked Spain's Catalan Police Union Website." Deep Dot Web. N.p., 26 May 2016. Web. 9 July 2016. <https://www.deepdotweb.com/2016/05/26/police-catalan-hack/>.

Harbison, Cammy. "Deanonymizing Tor Hidden Service Traffic Through HSDir Is A Cake Walk, Say Researchers: HITB Presenters Showcase New Threats." IDigitalTimes.com. N.p., 29 May 2015. Web. 13 July 2016. <http://www.idigitaltimes.com/deanonymizing-tor-hidden-service-traffic-through-hsdir-cake-walk-say-researchers-hitb-445328>.

Hornby, Albert Sydney., Sally Wehmeier, Colin McIntosh, Joanna Turnbull, and Michael Ashby. *Oxford Advanced Learner's Dictionary of Current English*. Oxford: Oxford UP, 2005. Print.

"The Internet Is the World's Most Important Infrastructure." The Report. N.p., n.d. Web. 11 July 2016. <https://www.ourinternet.org/report>.

An Introduction To The Internet Assigned Numbers Authority (Iana) Function. "The IANA Functions An Introduction to the Internet Assigned Numbers Authority (IANA) Functions." The IANA Functions (n.d.): n. pag. Icann.org. ICANN, Dec. 2015. Web. 11 July 2016. <https://www.icann.org/en/system/files/files/iana-functions-18dec15-en.pdf>.

"Jihad and Terrorism on the Dark Web." Dark Side of the Web. N.p., 11 May 2012. Web. 11 July 2016. <https://davidenewmedia.wordpress.com/subcultures/jihad-and-terrorism-on-the-dark-web/>.

"Lyn Ulbricht Speaks about Other People Involved In Silk Road." Silk Road Drugs. N.p., n.d. Web. 12 July 2016. <http://silkroaddrugs.org/>.

"Pedophiles Seem to Make Up a Huge Chunk of Anonymized Web Traffic." Smithsonian. N.p., n.d. Web. 10 July 2016. <http://www.smithsonianmag.com/smart-news/pedophiles-seem-make-huge-chunk-anonymized-web-traffic-180953793/?no-ist>.

"Robert Hannigan." *Wikipedia*. Wikimedia Foundation, n.d. Web. 26 Aug. 2016. <https://en.wikipedia.org/wiki/Robert_Hannigan>.

Schneier, Bruce. "Schneier on Security." Blog. N.p., n.d. Web. 10 July 2016. <https://www.schneier.com/blog/archives/2007/04/cyberattack.html>.

"Terrorists and Dark Web, What Is Their Relationship?" Security Affairs. N.p., 29 Mar. 2016. Web. 11 July 2016. <http://securityaffairs.co/wordpress/45755/terrorism/dark-web.html>.

"Tor (Netzwerk)." Wikipedia. Wikimedia Foundation, n.d. Web. 9 July 2016. <https://de.wikipedia.org/wiki/Tor_(Netzwerk)>.

Tor Project: Anonymity Online. The Onion Router Project, n.d. Web. 10 July 2016. <https://www.torproject.org/index.html.en>.

"What Is The Onion Router (Tor) - Definition from Techopedia." *Techopedia.com*. N.p., n.d. Web. 26 Aug. 2016. <https://www.techopedia.com/definition/4141/the-onion-router-tor>.

“Malaysia ranks third in Global Cybersecurity Index”, *ITU* <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/MALAYSIA-RANKS-THIRD-IN-GLOBAL-CYBERSECURITY-INDEX.aspx>

“Malaysia's 2016 Cybersecurity Agenda”, *Bank Info Security* <http://www.bankinfosecurity.asia/malaysias-2016-cybersecurity-agenda-a-8766>

“Top countries best prepared against cyberattacks”, *World Economic Forum* <https://www.weforum.org/agenda/2015/07/top-countries-best-prepared-against-cyberattacks/>

“New Zealand’s Cyber Security Strategy”, *New Zealand Government* <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/nzcybersecuritystrategyjune2011_0.pdf>