The nature of censorship and regulation of the darknet in the Digital Age

Petya Peteva[1]

Latest data from Freedom House shows that, up to date, over 3.8 billion people have access to the Internet[2]. With the advance of the Information Age and with the ever-growing number of Internet users worldwide, multiple heated debates continue taking place on whether cyberspace should be regulated and/or censored, and to what extent, so that it strikes the right balance between respecting fundamental human rights, such as freedom of expression on the one hand, and ensuring public security and safety on the other. While cyberspace censorship has turned to be a political hot potato, there are still corners of cyberspace that, in the meantime, are practically unregulatable due to their anonymity and intractability of their users. This so-called „darknet", while not without its benefits, has also infamously posed a considerable obstacle for law enforcement authorities in combating crime and has provided a safe haven for nefarious individuals and illegal activities to take place with impunity.

Introduction

„Cyber-space", understood as a concept, is a borderless and timeless, fully-digitalized dimension, which has even been considered as a „consensual hallucination"[3], where people can express thoughts and opinions and be connected through a global „network of networks"[4]. It is a revolutionary communication platform that has given rise to a "network society"[5].

The term became synonymous with the Internet and the World Wide Web in the 1990s[6], and when we refer to „cyberspace" in the context of whether it can be censored or not, we generally do not perceive it as an abstract idea on its own but rather conceive it to be the same as its content. Thus, when we debate the issue, we seem to prefer the use of the term „*Internet* censorship" instead.

The believes of „Net Utopians"[7] – that cyberspace/the Internet is nearly impossible to censor – have shifted in the last two decades and have not held up in the face of current and more restrictive practices, recent years being replete with examples, some of which we'll take heed of below.

The notion of cyberspace/Internet censorship itself has been contentious for years and can be regarded in the light of the libertarianism/paternalism debate surrounding it. For example, as Spinello[8] observes, the roots of cyberspace are clearly libertarian, defending the classical liberal approach adopted by Mill[9], thus endorsing a censorship-free Internet. On the other hand, censorship can be defended from a paternalistic point of view, in that it aims to prevent possible harms from occurring, which in turn justifies strengthening state interference and surveillance, and restricting free speech to an extent.

Regardless of the stance one can take on the matter, however, the reality remains that in purely practical terms, cyberspace/the Internet is not entirely „censorship-proof" and various censorship techniques exist that have been utilized in multiple contexts in order to support this view.

Censorship techniques

The so-called man-in-the-middle (MITM) attacks that disrupt the connection between web browsers and servers have been stated to be in the heart of all censorship methods utilized[10]. The OpenNet Initiative lists four different possibilities for censorship of cyberspace[11]: first, technical methods (blocking IP addresses, DNS and URLs, as well as dynamic content analysis and DOS attacks, transparent proxies); second, search result removals by ISPs after being required by the authorities or justified under the „right to be forgotten"

[1] Author is a Legal Projects' Expert at the Law and Internet Foundation in Sofia, Bulgaria.

[2] *A. Shahbaz*, *A. Funk*, The crisis of Social Media, Freedom on the Net 2019, Freedom House, https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf (accessed 15.9.2020).

[3] *W. Gibson*, Neuromancer (Ace Books 1984) 69.

[4] *R.J. Deibert*, Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace' (2003) 32 Millennium 501.

[5] *M. Castells*, The Rise of the Network Society: The Information Age: Economy, Society, and Culture Volume 1 (2nd ed., Wiley-Blackwell 2009).

[6] New World Encyclopedia contributors, Cyberspace, New World Encyclopedia (2014), http://www.newworldencyclopedia.org/entry/Cyberspace#cite_note-0 (accessed 2.11.2016).

[7] *Y. Jewkes, M. Yvonne*, Introduction: the Internet, cybercrime and the challenges of the twenty-first century, [in:] *Y. Jewkes*, *M. Yvonne* (ed), Handbook of Internet Crime, Willan Publishing 2010.

[8] *R.A Spinello*, Regulating Cyberspace: The Policies and Technologies of Control, Quorum Books 2002, p. 34.

[9] *J.S. Mill*, On Liberty, *J.W. Parker* and Son 1859.

[10] *A.A. Niaki* et al., ICLab: A Global, Longitudinal Internet Censorship Measurement Platform, 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2020, pp. 135–151, DOI: 10.1109/SP40000.2020.00014.

[11] OpenNet Initiative, About Filtering, https://opennet.net/about-filtering (accessed 2.11.2016).

granted by the CJEU[12]; third, taking down the problematic website or deregistering the domain; and fourth, induced self-censorship by netizens and journalists due to fear of being prosecuted or adversely affected in some other way.

DPI (Deep Packet Inspection) is another technical possibility and is an established practice by ISPs in China, it has also been attempted by a US company in the UK[13].

Justifications for censorship

Examples of censorship justification include national security arguments, especially in the post-9/11 world which marked the age of strengthened government surveillance all around the world[14]. The perceived looming threats to national security stemming from terrorist attacks, as well as external cyberattacks, have been perceived as valid reasons for states to strengthen encryption techniques and boost cybersecurity[15]. It is a rather onerous task to define the science itself behind cybersecurity due to its constantly evolving nature, however, the „access controls and authentication protocols", utilized within its context, have been likened to the physical barriers of fortress walls that protect users from existing cyber threats[16]. Also, cybersecurity is identified with the provision of dynamic defenses, such as predictive analytics[17], which operate on a proactive basis so that they would be able to detect and negate possible future security risks.

Public safety, and particularly that of minors, is another major factor – a harrowing case in point being the Elysium platform, which has resulted in four convictions[18]. Cyber-bullying is another prominent example – it led, for instance, to the proposal of the Megan Meier Act in the US[19]. There's an emerging concern about the supposedly increased rate of suicides and homicides attributed to the Internet, even with little to no empirical data to back it up[20].

The potential harm of online harassment and hate speech is taken into consideration, some of the claims being that it incites violence, especially with „hate sites" on the rise[21].

There are also arguments on the basis of a loss of reputation, especially by the commercial world as it has the most to lose, however, the CJEU did try to provide a balance, requiring „a sufficient level of seriousness", in order to impose censorship on free speech[22] and national legislation as well, such as the Defamation Act 2013[23] in the UK, for instance, which seems to adopt a similar approach.

The views on the necessary protection of moral standards are not homogenous either, however, the line clearly seems to be drawn at child pornography[24]. Furthermore, there is „a general consensus" that the right to freedom of speech should be restricted if such „invariably illegal content" is involved[25].

Censorship as oppression

While many democratic countries struggle with striking the right balance between freedom of expression on the one hand and its proportionate restriction on the other, non-democratic ones often blatantly use censorship in an oppressive manner, in the form of the so-called „digital authoritarianism"[26].

North Korea has been ranked the leading country in Internet censorship, where any disseminated information to the public is government controlled and heavily censored in its entirety[27]. China is ranked the second place, which has created an extremely effective method for censoring cyber-space materials through its so-called „Great Firewall" that blocks „undesirable content from its „netizens"[28] and, as Deibert states, „China… is a „hard case" for those who

[12] *J. Vincent*, Hidden From Google' website lists articles removed from search results, Independent (16 June 2014,) http://www.independent.co.uk/life-style/gadgets-and-tech/hidden-from-google-lists-articles-removed--from-googles-search-results-9608692.html (accessed 2.11.2016).

[13] *D. Geere*, How deep packet inspection works, Wired (27 April 2012), http://www.wired.co.uk/article/how-deep-packet-inspection-works (accessed 2.11.2016).

[14] Patriot Act 2001; Regulation of Investigatory Powers Act 2000; Anti--Terrorism, Crime and Security Act 2001; Terrorism Act 2006.

[15] Directorate-General for External Policies, Policy Department, Surveillance and censorship: The impact of technologies on human rights (European Parliament 2015), https://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU(2015)549034_EN.pdf (accessed 15.9.2020).

[16] American Association for the Advancement of Science, What is the Science of Cybersecurity?, AAAS (21.2.2014), https://www.aaas.org/news/what-science-cybersecurity (accessed 12.9.2020).

[17] *Ibidem*.

[18] *R. Fuchs*, German child porn network 'Elysium' founders sentenced to lengthy jail terms, DW (7.3.2019), https://www.dw.com/en/german--child-porn-network-elysium-founders-sentenced-to-lengthy-jail-terms/a-47794610 (accessed 17.9.2020).

[19] *S. Kotler*, Cyberbullying Bill Could Ensnare Free Speech Rights', FoxNews (14.5.2009), http://www.foxnews.com/politics/2009/05/14/cyberbullying-ensnare-free-speech-rights.html (accessed 2.11.2016).

[20] *M. Wykes*, 'Harm, suicide and homicide in cyberspace: assessing causality and control' in Y Jewkes and M Yvonne(ed), Handbook of Internet Crime (Willan Publishing 2010).

[21] *M. Yar*, Cybercrime and Society (London: SAGE 2006) chap. 6.

[22] Axel Springer AG v. Germany [2012] 55 EHRR 183, para. 83.

[23] Defamation Act 2013, p. 1.

[24] *Y. Akdeniz*, Governance of Pornography and Child Pornography on the Global Internet: A Multy-Layered Approach, in *L. Edwards, C. Waelde* (eds.), Law and the Internet: Regulating Cyberspace (Hart Publishing 1997) 223.

[25] *Ibidem*.

[26] *A. Shahbaz*, *A. Funk*, The crisis of Social Media, Freedom on the Net 2019, Freedom House, https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf (accessed 15.9.2020).

[27] *P. Bischoff*, Internet Censorship 2020: A Global Map of Internet Restrictions', Comparitech (15.1.2020), https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/> accessed 15 September 2020.

[28] *J. Lee*, *C. Liu*, Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China (13, Minn. J.L. Sci. & Tech. 2012) 125.

argue that the Internet cannot be controlled"[29]. In its 2015 Report, Freedom House displays numerous topics that are being censored[30].

Other countries, such as Russia with its „blacklist law"[31] and Vietnam with its Decree 72 law that criminalizes government opposition[32], are other instances of increasing attempts at filtering content and oppressive censorship. A recent example is the turbulent political situation in Sudan, where authorities imposed severe restrictions on social media in order to prevent people from sharing and receiving information in regard to the now ousted President Omar al-Bashir[33]. Also, concerns are currently on the rise in regard to the new Hong Kong security law which significantly limits free speech and increases surveillance[34], as well as the newly passed legislation in Turkey which would expand government control over content on large social media platforms on its territory[35].

What is more, oppressive regimes have not only utilized a multiplicity of censorship techniques but they have also vastly manipulated information on social platforms, as well as frequently undertaken unregulated mass surveillance, therefore grossly infringing on both individuals' fundamental human rights and data protection rights.

We should bear in mind, however, that as vast as the regular Internet is, it doesn't constitute all of cyberspace. In fact, censorship is not limitless and there are still some parts of the Web where filtering practices don't work as they are hidden under the main surface. This „censorship-free" world frequented by anonymous users[36], referred to as the „darknet", is precisely what we turn to next.

What is the darknet and how does it work?

The darknet is a term used to separate it from the Clearnet, or the cyber-space with the websites we're using on a daily basis. Its so-called hidden services constitute a part of the deep web, which is simply content that is not indexed by mainstream search engines such as Google and Yahoo![37]. It can still be accessed through standard technologies (e.g. HTML, CSS) and web browsers (e.g. Chrome, Firefox), however, only with special rerouting software[38], which hides the IP addresses of their servers[39]. Thus, the darknet conceals its users' identities, provides them with anonymity and makes them virtually untraceable.

Its roots stem from the US Naval Research Laboratory, where a team of experts, using the work of *D. Chaum* as a guiding light[40], created the revolutionary onion routing and its most popular application – TOR (The Onion Router). Its initial purpose was „to protect overseas American operatives and dissidents"[41].

Just like the onion is multi-layered, the IP address of the end-user is hidden under layers of encryption. This means that all data traffic from an individual's computer passes through a multiple number of volunteering relaying computers called „nodes", changing their IP address with a different one on the TOR network. Each time data goes through another „relay", it loses one layer of encryption until it reaches the exit node[42].

TOR is arguably the most popular method of accessing the darknet, it is, however, not the only method, and others, such as the Invisible Internet Project (I2P)[43] and Freenet[44], are also used as alternatives.

Different uses of the darknet

As we can see from the research of what the darknet constitutes, the concept of *anonymity* is at its core.

The primary purpose of onion routing is still relevant today and a substantial part of the users are „military, gov-

[29] *R. J. Deibert*, Dark guests and great firewalls: the Internet and Chinese security. (58 (1), Journal of Social Issues 2002) 143.

[30] Freedom on the Net, Freedom House, 2015, https://freedomhouse.org/sites/default/files/resources/FOTN%202015_China%20%28new%29.pdf (accessed 2.11.2016).

[31] Russia internet blacklist law takes effect, BBC News (1.11.2012), http://www.bbc.co.uk/news/technology-20096274 (accessed 2.11.2016).

[32] *E.E Schmidt, J. Cohen*, The Future of Internet Freedom, The New York Times (11.3.2014) http://www.nytimes.com/2014/03/12/opinion/the-future-of-internet-freedom.html?_r=0 (accessed 2.11.2016).,

[33] Freedom on the Net, The Crisis of Social Media', Freedom House, 2019, https://freedomhouse.org/report/freedom-net/2019/crisis-social-media (accessed 31.7.2020).

[34] *G. Tsoi*, *L.C. Wai*, Hong Kong security law: What is it and is it worrying?, (BBC News, 30.6.2020), https://www.bbc.com/news/world-asia-china-52765838 (accessed 31.7.2020).

[35] *M. Santora*, Turkey Passes Law Extending Sweeping Powers Over Social Media, The New York Times (July 29 2020), https://www.nytimes.com/2020/07/29/world/europe/turkey-social-media-control.html (accessed 31.7.2020).

[36] *J. Bartlett*, How the mysterious dark net is going mainstream' (TEDTalks 2015) https://www.youtube.com/watch?v=pzN4WGPC4kc (accessed 2.11.2016).

[37] *J. Pagliery*, The Deep Web you don't know about, CNN (10.3.2014), http://money.cnn.com/2014/03/10/technology/deep-web/index.html (accessed 2.11.2016).

[38] *R. Gehl*, Illuminating the Dark Web (Scientific American, 21.10.2018), https://www.scientificamerican.com/article/illuminating-the-dark-web/ (accessed 17.9.2020).

[39] *C. Fulton*, *C. McGuinness*, Digital Detectives: Solving Information Dilemmas in an Online World (Chandos Publishing 2016) 105.

[40] *D. Chaum*, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms (1981] 24 ACM 84.

[41] *T. McCormick*, The Darknet. Foreign Policy, FP (9.12.2013), http://foreignpolicy.com/2013/12/09/the-darknet-a-short-history/ (accessed 3.11.2016).

[42] Darknet Series: What is the Darknet?, OWL Cybersecurity (26 August 2016), https://www.owlcyber.com/blog/2016/8/26/the-darknet-series-what-is-the-darknet (accessed 2.11.2016).

[43] The Invisible Internet Project < https://geti2p.net/en/ (accessed 3.11.2016).

[44] Freenet, https://freenetproject.org/index.html (accessed 3.11.2016).

ernment and law enforcement organizations"[45] within which sensitive information is often discussed and it would certainly be dangerous if it fell into the wrong hands.

The darknet can be and *is* used for legitimate purposes – it is, for instance, utilized by whistleblowers, such as Edward Snowden who used TOR with a piece of technology called TAILS to inform the media and the public about the government surveillance[46]. The new WikiLeaks submission system is also exclusively accessible through TOR[47].

It also plays a major role in some more restrictive countries with oppressive governments, where anonymity is not an opportunity[48] but a necessity if one wants to have their voice heard. Jardine[49] supports the rhetoric that all points of view must be considered in order for democracy to flourish, views previously expressed by Mill[50] as well. In Russia and China, for instance[51], Internet censorship is nothing new. All Chinese ISPs are required „to register with the police and all Internet users must sign a declaration that they will not visit forbidden sites"[52]. China's „Great Firewall" project was also able to censor TOR, however, ways to circumvent that hurdle have been discovered[53].

TOR has been associated with the Arab Spring that took place in the Middle East in 2011 – David Appelbaum explains how it was used by the political dissidents and journalists as well as the general public to give birth to the revolution[54].

The shroud of anonymity that the darknet provides is also a desired alternative by young people, such as the Youth Liberation Front (YLF), members of the LGBTQ+ community, as well as other disenfranchised minorities, which use it as a sanctuary in which they can feel comfortable and secure without any of the pressures and constraints of the Clearnet[55].

Still, primary due to the factor of anonymity as it has been reported[56], the darknet is largely associated with nefarious and illegal practices. It provides for a large number of crypto markets for drugs (such as Silk Road[57]), child pornography, weaponry, and, allegedly, the services of professional hitmen[58], all the more easy to purchase as it operates with cryptocurrencies. This means that, even if censorship is applied as a safety measure and is justified on the Clearnet, this step is undermined by the crime that reigns freely on the darknet. This brings us to the inevitable question – how impenetrable is the darknet?

Conclusions

While currently it is rather difficult to see how the darknet can be regulated in the same manner as the Clearnet, due to its very nature, including through legislative provisions and government control, to say that it is a cyberspace that lies entirely outside the limits of the law would be incorrect. For instance, even though the darknet protects its users through providing them with anonymity in terms of their identities and geographical locations, any data that is provided by an individual is visible by anyone that has accessed the specific website as it can potentially be used to identify them[59].

The darknet also serves as an incitement for law enforcement to keep up with technological advancements in order to tackle the criminal activities reported to be taking place there. Examples of this are the FBI taking down a major child pornography website by using a new hacking method called NIT[60], Operation Shrouded Horizon[61] and Operation Hyperion[62]. More

[45] *D. Walsh*, A Beginner's Guide to Exploring the Darknet, TurboFuture (29.8.2016), https://turbofuture.com/internet/A-Beg inners-Guide-to--Exploring-the-Darknet (accessed 3.11.2016).

[46] *K. Finley*, 'Out in the open: Inside the operating system Edward Snowden used to evade the NSA, Wired (14.4.2014), https://www.wired.com/2014/04/tails/ (accessed 3.11.2016).

[47] *R. Brandom*, 'After four years of downtime, WikiLeaks is once again accepting leaks online, The Verge (1.5.2015), http://www.theverge.com/2015/5/1/8531049/wikileaks-tor-browser-submission-page (accessed 3.11.2016).

[48] *E. Jardine*, Tor, what is it good for? Political repression and the use of online anonymity-granting technologies (2016), New Media & Society (as cited in Fuzzy, Paper: Oppressive and free countries use Tor the most, DeepDotWeb (10.4.2016), https://www.deepdotweb.com/2016/04/10/paper-oppressive-free-countries-use-tor/ (accessed 3.11.2016).

[49] *Ibidem.*

[50] Mill (n 7).

[51] *K. Paul*, Russia wants to block Tor, but it probably can't, Motherboard (18 February 2015) <http://motherboard.vice.com/read/russia-wants-to--block-tor-but-it-probably-cant (accessed 3.11.2016).

[52] *Y. Jewkes*, Crime Online (Willan Publishing 2007) chap. 1, 1.

[53] *P. Winter*, *S. Lindskog*, How the Great Firewall of China is blocking Tor, USENIX (2012), https://www.usenix.org/system/files/conference/foci12/foci12-final2.pdf (accessed 3.11.2016).

[54] *I. Zahorsky*, Interview with Jacob Appelbaum 'Tor, Anonymity, and the Arab Spring: An Interview with Jacob Appelbaum', UPEACE (August 1 2011) <http://www.monitor.upeace.org/innerpg.cfm?id_article=816 (accessed 3.11.2016).

[55] *R. Gehl* et al, Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P (The MIT Press 2018).

[56] FBI, A Primer on DarkNet Marketplaces: What They Are and What Law Enforcement is Doing to Combat Them" (1 November 2016), https://www.fbi.gov/news/stories/a-primer-on-darknet-marketplaces (accessed 21.7.2020).

[57] *W. Lacson*, *B. Jones*, The 21st Century DarkNet Market: Lessons from the Fall of Silk Road, International Journal of Cyber Criminology 10.1 (2016) 40, http://www.cybercrimejournal.com/Lacson&Jonesvol10issue1IJCC2016.pdf (accessed 2.11.2016).

[58] Daily Mail Reporter, The Disturbing World of the Deep Web, where contract killers and drug dealers ply their trade on the Internet, Daily Mail (11.10.2013), http://www.dailymail.co.uk/news/article-2454735/The-disturbing-world-Deep-Web-contract-killers-drug-dealers-ply-trade-internet.html (accessed 3.11.2016).

[59] *A. Zaunseder*, The darknet is not a hellhole, it's an answer to internet privacy, The Conversation (16.8.2018), https://theconversation.com/the--darknet-is-not-a-hellhole-its-an-answer-to-internet-privacy-101420 (accessed 31.7.2020).

[60] *M. Russon*, FBI crack Tor and catch 1,500 visitors to biggest child pornography website on the dark web', International Business Times (6.1.2016) <http://www.ibtimes.co.uk/fbi-crack-tor-catch-1500-visitors-biggest--child-pornography-website-dark-web-1536417 (accessed 3.11.2016).

[61] *D. Kushner*, The Darknet: Is the Government Destroying 'the Wild West' of the Internet?', Rolling Stone (22.10.2015), http://www.rollingstone.com/politics/news/the-battle-for-the-dark-net-20151022 (accessed 3.11.2016).

[62] FBI, A Primer on DarkNet Marketplaces: What They Are and What Law Enforcement is Doing to Combat Them" (1 November 2016), https://www.fbi.gov/news/stories/a-primer-on-darknet-marketplaces (accessed 21.7.2020).

recently, in 2017, two major darknet markets, Alphabay and Hansa, were shut down after a successful international police operation[63]. Authorities, apart from monitoring darknet websites, utilize the help of companies, such as BrightPlanet and HoldSecurity, and there are even vigilantes[64] and „hacktivists"[65] that take matters into their own hands.

Challenges, however, still remain as the illegal networks that are taken down are quickly replaced by new markets, which maintain the resilience of the overall structure[66] and thus, further national and international coordination between authorities is needed, as well as an increased understanding of the nature and *modus operandi* of the darknet itself in order to successfully tackle such criminal activities.

[63] European Monitoring Centre for Drugs and Drug Addiction and Europol (2017), Drugs and the darknet: Perspectives for enforcement, research and policy, EMCDDA–Europol Joint publications, Publications Office of the European Union, Luxembourg.

[64] *T. Holman*, How cyber-vigilantes catch pedophiles and terrorists lurking in the dark web (International Business Times, 12.12.2014) http://www.ibtimes.co.uk/how-cyber-vigilantes-catch-paedophiles-terrorists-lurking-deep-web-1479291> accessed 3 November 2016.

[65] *C. Baraniuk*, Ten Hacktivists who shook the Web (Dazed 2013) http://www.dazeddigital.com/artsandculture/article/16368/1/ten-hacktivists-who-shook-the-web (accessed 3.11.2016).

[66] European Monitoring Centre for Drugs and Drug Addiction and Europol (2017), Drugs and the darknet: Perspectives for enforcement, research and policy, EMCDDA–Europol Joint publications, Publications Office of the European Union, Luxembourg.

Key words: darknet, censorship, Internet regulation.