Chapter 6
Dark and Deep Webs– Liberty or Abuse

Lev Topor
https://orcid.org/0000-0002-1836-5150
Bar Ilan University, Ramat Gan, Israel

ABSTRACT

While the Dark Web is the safest internet platform, it is also the most dangerous platform at the same time. While users can stay secure and almost totally anonymously, they can also be exploited by other users, hackers, cyber-criminals, and even foreign governments. The purpose of this article is to explore and discuss the tremendous benefits of anonymous networks while comparing them to the hazards and risks that are also found on those platforms. In order to open this dark portal and contribute to the discussion of cyber and politics, a comparative analysis of the dark and deep web to the commonly familiar surface web (World Wide Web) is made, aiming to find and describe both the advantages and disadvantages of the platforms.

INTRODUCTION

In June 2018, the United States Department of Justice uncovered its nationwide undercover operation in which it targeted dark web vendors. This operation resulted in 35 arrests and seizure of weapons, drugs, illegal erotica material and much more. In total, the U.S. Department of Justice seized more than 23.6$ Million.[1] In that same year, as in past years, the largest dark web platform, TOR (The Onion Router),[2] was sponsored almost exclusively by the U.S. government and other Western allies.[3] Thus, an important and even philosophical question is derived from this situation- Who is responsible for the illegal goods and cyber-crimes? Was it the criminal[s] that committed them or was it the facilitator and developer, the U.S. government?

The key advantages and disadvantages of the deep and dark web are discussed in this article with a constant comparison to the their commonly known sibling- the surface web. Moreover, this article explores the methods by which deep and dark web users can stay almost totally anonymous and secure.

DOI: 10.4018/978-1-7998-2466-4.ch006

In contrast, these users can be maliciously exploited by hackers, money-launderers, drug dealers, human traffickers and other cyber-criminals, users can even be exploited by foreign governments and terror groups. On the one hand, these non-regulated platforms can facilitate many malicious, offensive and illegal activities. On the other, the anonymous platforms can provide anonymous and secure ways of communications for intelligence operatives but more importantly for oppressed regime oppositions and promoters of human rights in authoritarian states (Finklea, 2017; Gehl, 2016).

As assumed and argued in this article, the deep and dark web is a double-edged sword, it enables free speech while spreading extremism. In this case, the scale and trends of the deep and dark web are worrisome. While our commonly known surface web holds tremendous amounts of web pages and data, the deep and dark webs are in fact estimated to be about 400-500 times larger than the surface world wide web (Rudesill, Caverlee & Sui, 2015). This fact raises the questions about deep and dark web activities, specifically malicious and criminal activities. If we all encounter concerning articles in our newspapers from time to time about terror cells or child pornography on the web, is that only the tip of the iceberg? Is there 400-500 times more crime and exploitation on the deep and dark web?

The simple arithmetical answer is no. The deep web is larger than the surface web, but it stores mostly private data such as personal and public undisclosed information; financial information, health documents, legal documents, governmental data assets and more. Everything not accessible to the public and password protected or restricted is in fact the deep web, even your (the reader's) bank account. However, the problem lies in another layer of the web- the dark web. The commonly used dark web (TOR) was designed by the U.S. Naval Research Laboratory to allow an anonymous and secure method of communication while avoiding monitoring, indexing and regulation. These military and intelligence benefits are exactly the social deficiencies, criminals, terrorists and other foreign states also use the anonymity and security for malicious and illegal activities. This argument is discussed throughout the article and the conclusion is derived from the combination of technical network aspects, social regulations and desirable norms.

DARK AND DEEP WEB: WHAT, WHY AND HOW

The deep web is every set of data that is not indexed or controlled in the public surface web and is not publicly accessible. The dark web is an alternative routing infrastructure that hosts web platforms and requires special software for use. Before the explanation and discussion regarding these platforms, it is important to understand when and why the internet, as we know it today, was established. The surface web internet originated from a U.S. Department of Defense project known by the name of ARPANET-Advanced Research Project Agency Network. In 1983 the ARPANET project switched from being a closed network, named Network Control Protocol (NCP) to an open one, the Transmission Control Protocol/ Internet Protocol (TCP/IP) (Hurlburt, 2015).

Effectively, this transition led to the expansion of protocols and communication types. The networks grew each month since the early beginning of the network project in the late 1960's and quickly expanded. As the number of networks and users grew, a classification of network types begun; National (Class A), Regional (Class B) and Local (Class C). Nowadays, governments and individuals can design and install their own networks (Hurlburt, 2015; Bradley & Currie, 2015). As illustrated in Figure 1 and Figure 2, early ARPANET networks designs connected only a few computers together, but these networks grew quickly. At the beginning, only a few nodes[4] (crossroads) were designed and used for the