DEEP WEB, GOING BENEATH THE SURFACE

The “Deep Web” is not an easy subject to investigate. To begin with, the first rule of the Deep Web is: “You do not talk about the Deep Web”. And that holds true for the second rule. While the third rule of the Deep Web is: “You can talk about it, but just if this is related to drug lords, weapons, terrorism or other similar topics.”

Deep Web generally refers to a specific subsection of the net. Usually it covers any URL — including databases or intranets — that is not indexed by search engines and is therefore invisible to the majority of people. But the term Deep Web is often used to refer to that part of the web and those services built upon anonymous nets, also called darknets. It is about the so-called hidden services that allow access to resources without revealing the operator’s identity. Tor — the most popular software and network that lets surfing the web and communicating in an anonymous way — has offered hidden services since 2004. It allows users not only to surf websites anonymously, but also to run a server under a pseudonym. Its main purpose is to enable freedom of speech, even in situations where states or other powerful entities try to suppress it.

Systems allowing the anonymous and censorship-resistant distribution of content have been fostered by the increasing Internet censorship. Tor hidden websites include dissidents’ news, and sensitive, or otherwise controversial, documents or topics.

No question, an anonymous online environment can also be attractive for criminal activities. But in the end what can we find in the Deep Web? We can find there platforms and services promoting freedom of speech and whistleblowing, such as Wikileaks, Strongbox, and GlobaLeaks. For example, Strongbox is an anonymous service promoted by the Freedom of the Press Foundation, and originally coded by Aaron Swartz to receive tips and leaks. Today, many news organizations are deploying similar systems. GlobaLeaks is a platform designed by The Hermes Center for Transparency and Digital Human Rights (1) which has been implemented by many media companies and NGOs in different countries. No doubt in the Deep Web we can also find black markets such as the old Silk Road, hacking and cryptocurrency forums, websites, services used by botnets and, above all, many political websites or websites publishing content which is considered sensitive or questionable by all or some societies.

How big is this space? Tracing onion addresses, which are hidden service addresses called as such because they end with the pseudo-top-level domain host suffix “onion”, poses several challenges. Many hidden services take measures to protect location and anonymity — including changing their addresses — not

storing the entire list of onion addresses through a central entity and avoiding linking the addresses to each other.
A study conducted by the University of Luxembourg (2) in September 2013 tried to analyze Tor hidden services by exploiting an old Tor version's vulnerability. Researchers collected 40 thousands unique onion addresses and tried to classify their content. What did they find? The content was in 17 different languages, including Arabic, Basque, Chinese and Bantu. Around 44% of the resources were about drugs, adult content, weapons and counterfeit products. The remaining 56% was on anonymity, politics, reporting and human rights violations, repression, corruption, freedom of speech, leaked cables, and the technical and political aspects of anonymity. Different types of services, of a more or less shady nature, were also offered. Researchers came to the conclusion that the number of hidden services related to illegal activities was equal to the number of resources focusing on legal activities. However, when the research was conducted, some of the most popular resources were the ones linked to botnets or adult content and Silk Road was among the top 20 most popular hidden services.

This picture confirms an earlier study called Project Artemis, carried out by two researchers who analyzed thousands of Deep Web addresses. "Despite the quote related to cybercrime is remarkable — wrote the researchers — the conclusion is that the Tor network contains also mostly legal content, in particular the volume of documents related to political issues is in continuous increase." (3)

One of the most representative and up to date researches on Tor hidden service directories and Tor hidden service search engines is The Ahmia Project, (4) which is now part of the Hermes Center for Transparency and Digital Human Rights. (5)

Researchers working on the Ahmia project found 1300 working hidden services providing web content. Indubitably, the number of hidden services providing other Internet services, such as IRC, Jabber and Bittorrent is much greater. The Ahmia group detected hidden services that were running websites only. The group collected descriptive information from these services and generated a tag cloud. From this, an outline related to the types of contents that are published on hidden services was released. Many tags referred to a lot of services and tools about anonymity, Bitcoin, markets and cannabis.

While estimates and classifications of the Dark Web are not easy to obtain, nonetheless, available information shows a picture that is less black and white than the one usually portrayed. The Dark Web represents a volatile environment. Many hidden services change address often, becoming inactive in a short time. The most stable sites are hacking forums and those dealing with e-commerce. For the user, using the dark web is like surfing in an unknown sea without charts, or using charts that might be wrong and constantly in a state of flux. In the end, the best way to get information is through word of mouth.
Hidden services have been growing since 2004. The Deep Web exists for 10 years, which is a relatively short time compared to the rest of the internet.

The Deep Web became popular in 2011 when Silk Road was born and the media began reporting on the platform. The first to break the news on the Dark Web in the mainstream media was a journalist working for Gawker, Adrian Chen. (6) He interviewed one of the buyers, a software programmer, who said he was a libertarian anarchist and believed that anything that is not violent should not be criminalized.
The Silk Road administrators talked the same way, quoting agorism, an anarcho-libertarian philosophy. According to the prosecutors the founder of Silk Road would be Ross Ulbricht, a 30 years old, brilliant American student of physics and solar cells, interested in libertarian ideas and a former boy scout.

Philosophy aside, in 2013 Silk Road counted 13,000 listings of items, mainly drugs. In its two-and-a-half years of operation, it got revenues of more than 9.5 million Bitcoins, worth about 1.2 billion dollars. Silk Road's rate of commission was between 8% and 15%. The system had more than 900,000 accounts from countries all around the globe.

A recent academic study claims that Silk Road was "a paradigm-shifting criminal innovation" (7) since it was a less violent trading environment compared to offline drug markets. The researchers claim that Silk Road was not just an eBay for drugs since most of the revenues would come from business to business trade.

Silk Road was seized by the FBI in October 2013, but black markets did not disappear. Actually they proliferated. According to Deepdotweb, (8) which is a sort of Tripadvisor for black markets, today there at least 20 well established black markets.

But to understand what is really going on in this underworld, we need to understand the type of people, ideas, and softwares that are used there. Who are we going to "meet" in the Deep Web? Looking at its user base we find a very varied demographic: activists of different countries and backgrounds; journalists; hackers; cybercriminals with different specializations (carders, botmasters, scammers, etc); coders and cryptographers; Bitcoin lovers and miners; Wikileakers and hacktivists. Many of them are involved in a specific area, but there are also many dabbling in a little bit of everything. Then, of course, there are also people committing crimes other than cyber crimes, such as pedophiles. But it would be a mistake to use this latter fraction of this galaxy of users to attack the entire Deep Web.

Tor is not the only darknet, there are also other systems, although less used, like I2P and Freenet. Originally Tor was created by the United States government, developed in particular by the Navy. Its initial purpose was to protect the communication of the military, but then they opened it up to everyone. Today, Tor is an open source project run by volunteers and supported by activists, nonprofit organizations, universities and governments. Tor has been the main hurdle facing some governments' ambitions to surveil and monitor all digital communication.

Tor is a precious tool for many countries dissidents and users, and it became an important tool during the Arab Spring. In Iran, Tor usage went from 7,000 users in 2010 to 40,000 users two years later. In Syria, the number of Tor users grew from 600 to 15,000 in just two years. In Turkey, in 2014, after the government blocked Twitter and YouTube, Tor usage skyrocketed. Tor is also used by women's shelters in Boston to protect those who are escaping from abusive partners who use information technology to track their victims.

The use of Tor jumped exponentially in the last year, since the revelations of the governments' surveillance programs. Today approximately two millions people worldwide use Tor on a daily bases, but such a number accounts also for bots. (9) According to the security researcher Runa Sandvik, excluding bots, the number of users is close to a million at worldwide level.

However, the number of Tor's users is expected to increase very quickly. In a time of widespread state censorship and surveillance, and persecution of minorities and activists in many countries, even in democracies, the availability of such a platform for anonymous communication and publishing is considered by many essential to protect freedom of expression.

The author:

Carola Frediani is a Journalist and co-founder of the independent news agency http://Effecinque.org . She writes mainly about hacktivism, surveillance, privacy, net rights for Italian and US news outlets. She is the author of books on Anonymous and Deep Web. More information available at: http://bit.ly/1rHXfR0

1 http://logioshermes.org/

2 http://cryptome.org/2013/09/tor-analysis-hidden-services.pdf

3 http://resources.infosecinstitute.com/project-artemis-osint-activities-on-deep-web/

4 http://www.ahmia.fi

5 http://logioshermes.org/

6 Gawker: http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160

7 Social Research Science Network: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436643

8 http://www.deepdotweb.com/2013/10/28/updated-llist-of-hidden-marketplaces-tor-i2p/

9 A bot is a software normally used to search large amount of data (i.e. search engine).