The Dark Side of the Internet

At the far end of the web lies a dark world of war, crime, and espionage. All you have to do is know where to look to find it

By Dr. Gil David

One of the most common sayings in the Internet world is "if something doesn't come up in a Google search, then it doesn't really exist." While this may seem true to the ordinary Internet user, reality is vastly different. Google and other search engines barely scratch the surface of the Internet. In truth, the Internet's core holds a wealth of information and interesting content, as well as a more sinister side of intrigue, war, crime, and espionage.

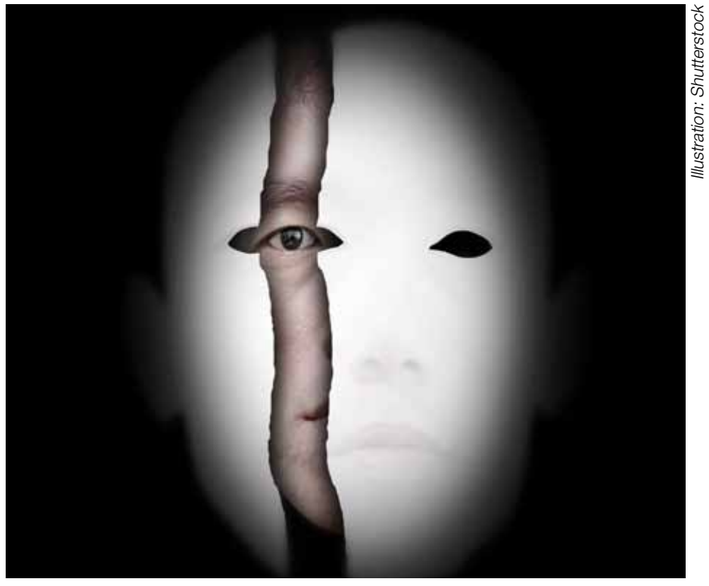


Illustration: Shutterstock

The Internet is traditionally divided into several layers. The top one, known as "Surface Web," is the one we are all familiar with. The inner layers, known as the "Deep Web," comprise the dark side of the Internet.

Surface Web is the layer of information that contains all the pages accessible through the major search engines, like Google, Yahoo, and Bing. These engines scan the Internet and yield an index – a map of sorts – of all of the pages and websites that they find. This method enables them to collect all the information directly accessible to search engines, thereby creating the first layer of the Internet.

According to several assessments, the Surface Web is comprised of several dozens to hundreds of terabytes of information, across tens of billions of web pages accessible through search engines. This layer, however, contains only a fraction of the information that exists online. To get to the rest of the information that is out there, one must delve deeper into the dark side of the Internet.

The Deep Web, also known as "Invisible Web" and "Hidden Web," contains all the parts of the Internet that are not accessible to search engines. It is believed that this layer contains several thousands of terabytes of information, spanning across hundreds of billions of web pages; meaning the dark side of the Internet is thousands of times larger that the Surface Web, and it is growing at a much faster rate.

Deep Web is usually divided into two sublayers: the Deep Web layer – the lion's share – is comprised of various kinds of pages, websites, and information. One type of page in this layer is the unlisted pages that are not indexed by search engines.

One reason information may not be indexed is because of a specific request by the page's owner, who can post a site with a restriction detailing that only those with a direct link to the website can have access.

Other types of pages in the Deep Web layer are those that search engines cannot access. These pages hold content that only certain, authorized users can see. For example, email and bank accounts are password protected so that only the person with the password can access the information.

The potential hidden within the Deep Web layer is enormous. The ocean of information that the majority of users are not exposed to is vast, so anyone who is able to dig around for it can achieve a significant advantage, especially in business and intelligence sectors.

The Anonymous Web

On the very bottom of the dark side of the Internet awaits the second layer of the Deep Web. The Anonymous Web makes up a fraction of the Deep Web, but it holds a wealth of information for intelligence, crime, and terror organizations.

Unlike the top layers of the Internet, where websites and their content can be associated with their owners and virtual users can be identified, anonymity is everything in this layer of the net.

These pages' owners and users are completely anonymous and even virtual payments made in this layer are done so with virtual currency. Naturally, where near-complete anonymity exists you can find a variety of users from government, security, and intelligence elements, to hackers, spies, and researchers, to drug dealers, mobsters, and guns for hire.

It is important to stress that accessing the Anonymous Web should be done only by those versed in its dangers and in the ways of online anonymity and cyber security, and are willing to take the risks lurking at almost every corner of the Anonymous Web.

Accessing this layer of the Internet is impossible through a standard browser. One way to access the Deep Web is by using The Onion Router method (TOR), which allows every Internet user to surf the web anonymously. Surfing the web this way lets the user find the website he is searching for through several coded servers scattered in different places around the world.

The user enters his request into a TOR server, from which it passes to other servers on the network until it finds its destination, all while allowing TOR users to remain anonymous, without exposing their IP address to either the website's owners or anyone else that might be monitoring the website's traffic (like government bodies that monitor Internet service providers).

A large portion of the content available on the Anonymous Web is stored on servers that disguise their location by using TOR, meaning both users and website owners use TOR to maintain their anonymity. A Deep Web user must use TOR in order to access it.

The user's premise when venturing into the Anonymous Web should be that he may find himself – unbeknown to him – under attack at any given moment by some of the best hackers out there using some of the most sophisticated cyber weapons available. For that reason, logging onto the Anonymous Web should be done from either a designated station or a virtual computer, which is completely independent of any network, and one that is used solely for that purpose. It is also best to disconnect any external devices, such as GPS, Bluetooth, a microphone, or a webcam.

Once you have logged on to the Anonymous Web, you will find an entire world, which may seem similar to the regular Internet, but is actually a very different playing field. There is no censorship, no rules, and no law enforcement in this part of the web, which means that anything and everything goes – even if it is illegal.

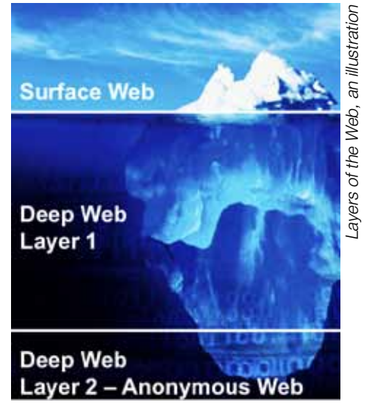
Take the Silk Road marketplace for example: this platform is similar to e-Bay and allows users to buy and sell anything, from drugs to spyware and weapons. Payment is done via BitCoin – a virtual currency that is completely anonymous. For instance, a Glock gun is sold for 200 BitCoins – the rough equivalent of $2,400. There are also various websites that let users create completely anonymous forums and message boards. These websites offer vast information, from source codes from Trojan horses to detailed manuals on bomb making.

The complete anonymity of this layer makes it a natural breeding ground for the distribution of intelligence or sensitive, leaked government information, be it by hackers, disgruntled employees, or whistleblowers. It is believed that the hundreds of secret US military documents about Guantanamo Bay that were posted on WikiLeaks came from the Deep Web; however, while the content of WikiLeaks can be blocked, Anonymous Web pages are immune to any censorship.

It is important to note that some of the information found in these layers is deliberately embedded there by government elements as bait for criminal elements, with the goal of catching them as they access the information, thus revealing their identity.

Monitoring and Counterattack

The Anonymous Web is also a breeding ground for a variety of cyber-security operations, both defensive and offensive. This layer poses significant challenges for security entities that wish to use it for their own needs.



Layers of the Web, an illustration

There is, for example, great importance in monitoring anonymous Deep Web websites to detect illegal activities by terrorists, hackers, and criminals in advance. However, the monitoring tools used on the Surface Web are invalid on the dark side of the Internet.

Intelligence organizations that would be wise to probe and monitor the Anonymous Web will undoubtedly find various treasures, from terror organizations to the trafficking of advanced cyber weapons. In most cases, this information is available only on that level of the Deep Web, and not on the upper levels of the Internet.

It is possible that part of the cyber-war arena will move to the Anonymous Web in the future, when offensive tactics will emanate from that layer to the Surface Web, and botnet command and control centers might be hidden in the inner parts of the Anonymous Web. In such cases, identifying the origin of the attack and blocking them would be a complex challenge for defense systems.

Dr. Gil David is the owner and CEO of the Brainstorm Private Consulting firm, which provides cyber and intelligence consulting. He also serves as a guest lecturer in Israel and worldwide, as well as a consultant to security, commercial, and academic bodies in Israel and abroad.