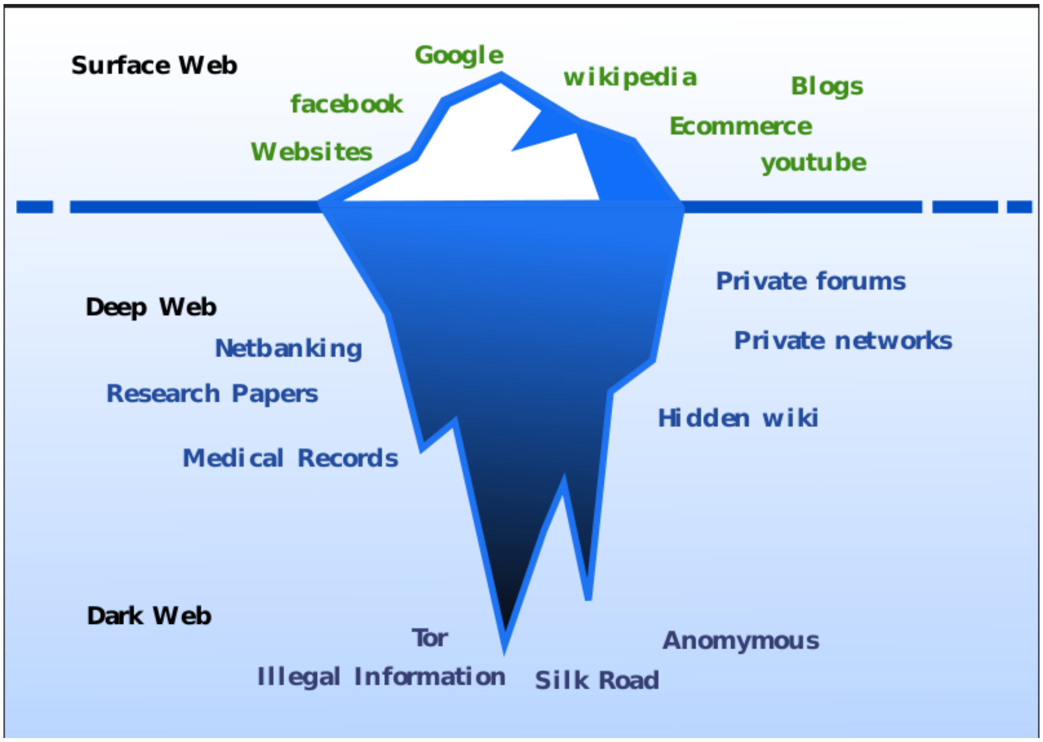
Darknet and Clearnet Sites, Hacker Goods for Sale

All the websites and data available on the internet can be categorized into 3 parts **Surface Web**, **Deep Web,** and **Dark Web**.



**Clearnet** is a term that typically refers to the publicly accessible Internet. Clearnet is the synonym for the surface web. The World Wide Web is one of the most popular distributed services on the Internet, and surface web is composed of the web pages and databases that are indexed by traditional search engines. Clearnet is just 4-5% of the whole internet and almost 90% of the people access surface web only for almost all their needs. Typically accessed websites on Clearnet are Google, Facebook, Wikipedia, YouTube, Blogs, and e-Commerce websites. We can access them using any general web browser like Mozilla Firefox, Google Chrome, and Safari.

Now, coming to the under the surface web, the terms we commonly hear are “deep web” and “dark web” they are sometimes used interchangeably, but they are not the same. Both deep web and dark web together constitutes about 95-96% of the total internet websites and webpages. **Deep Web** is an umbrella term used to access the data that is unindexed, censored by the standard web search engines. It can still be publicly accessible and can be located and accessed by a direct URL or IP address, but may require a password or other security access to get past public pages. It includes web portals to databases that require text searches, and interactive web sites that require more user input than simply clicking hyperlinks. The content of the deep web is hidden behind login forms and includes uses such as web mail, online banking, restricted access social-media pages and profiles, some web forums and code language that require registration for viewing content, and paywalled services such as video on demand and some online magazines and newspapers. It offers the opportunity to bypass local restrictions and access TV or movie services that may not be available in their local areas. Others go somewhat deeper to download pirated music or steal movies that aren't yet in the cinema.

**Dark Web** is a hidden part of the world wide web that can only be accessed using a special browser known as Tor. Dark web pages don’t appear when you look for them in a search engine, so you need to know the exact address of the website you want to visit. Specific browsers, such as Tor Browser, are required to reach the dark web. It consists mostly of illegal products or content that could be harmful to organizations or the public. Some examples include stolen credit card numbers, fake IDs, drugs, illegal weapons, stolen/ fake merchandise, child pornography and cannibalism related stuff and you can hire Hitman here as well. To access the dark web, a user needs to download darknet software, the most popular being Tor. All the dark web websites have an extension ‘. onion’ which normal browsers can not only browsers like Tor can. They are either invite only websites or are encrypted as websites to remain hidden deep in the world of the internet. Tor, which stands for “the onion routing project,” was developed by the U.S. Navy for the government in the mid-1990s. It was open sourced in 2004, and that’s when it went public. Today, Tor is the dark web browser that most people use to surf the internet anonymously. To do this, Tor hides a user’s IP address (or the unique address that identifies an internet-connected device or network) by bouncing their search request to multiple different locations. These bounces also referred to as relays, make it much harder for people to find users on the dark web. Today, it is funded by many big organizations like DARPA, Mozilla, US Department of Bureau of Democracy, Human Rights and Labor, Google Summer of Code, Ford Foundation and many more.

## Hacker goods for sale

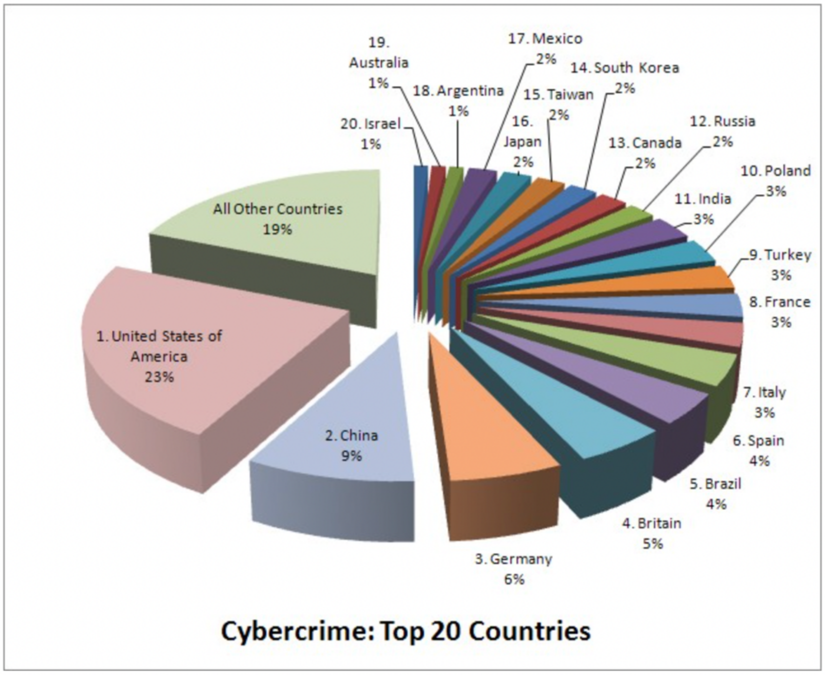
The tools used by hackers are custom made and some of them are the ones which were created for research purposes but looking at its potential harmful effects than its benefits they were never released to the public but are somehow common in the underground world and are used by miscreants to do notorious stuff.

“S in IOT stands for security”. When you look deeper into an IOT device or any embedded device for that matter, what do you see? You see windows of opportunities. Opportunities to modify it. To edit it. To exploit it. To hack it. IOT devices are full of vulnerabilities.

These are cheap and easily accessible hacking tools which is available. So far, Kali Linux has been the best and most widely Operating System, filled with an awesome collection of hacking tools which can be used to Web Application penetration testing, network security testing, WiFi attacks; best of its kind. It is the most famous and most useful Operating System used by security enthusiasts, hackers – both white hat and black hat, as well as hobbyists who like to tinker around with Linux OS.

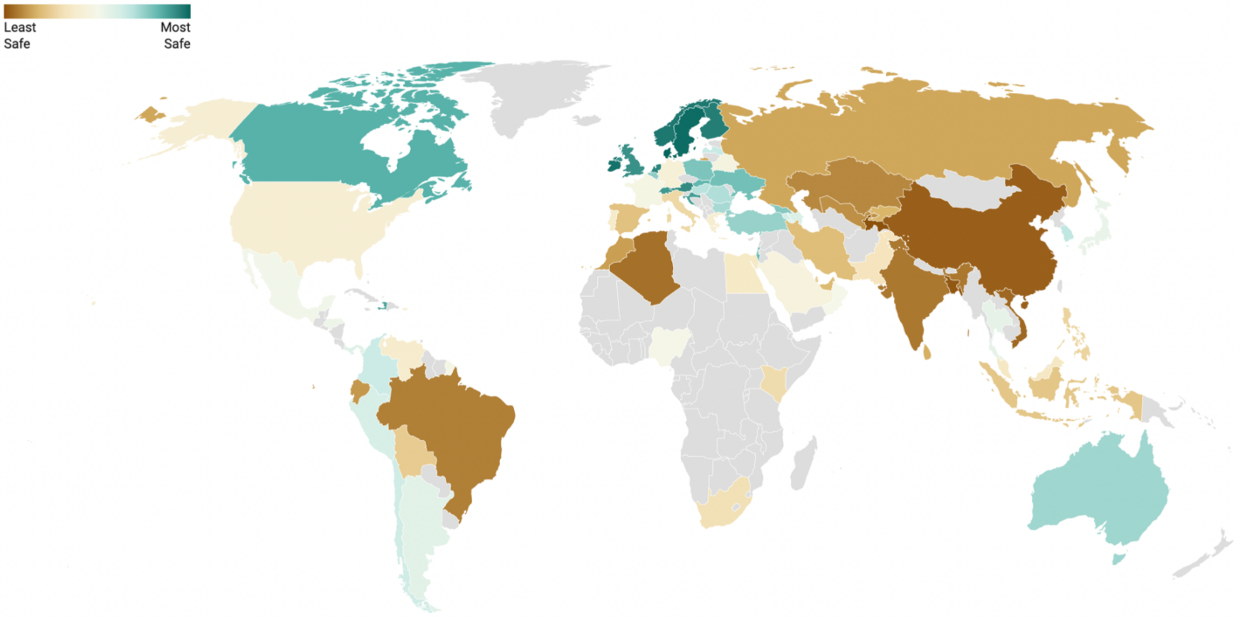
There are many hardware tools which can be used with this software and few of them are Ubertooth One: for Bluetooth hacking, Alpha USB Wi-Fi adapter: for illegal wireless activities. Raspberry Pi: is a minicomputer on which you can install hacking OS. Plastic Card Clone: for cloning debit/credit card information, RFID reader: for reading all the information from RFID equipped devices in the vicinity of this reader and many more other things which are a bane to the society rather than a boon.

Below is a pie chart indicating the most cybercrime affected countries



Cybercrime: Top 20 Countries

Which countries are the least cyber-safe in the world?



Map: Comparitech • Source: Kaspersky, ITU • Get the data • Created with Datawrapper