THE DARK NET AND HOW TO LEVERAGE IT

AUTHOR BY | COL HARPREET SINGH

For most of us, the web is limited to less than 100 websites and majority of this limited collection is in the form of Google sites and services. In reality, the internet is enormous, and it has around four billion websites existing on servers around the globe. However,an enormous chunk of the internet is still untouched by the ordinary world and the World Wide Web we see is only the tip of an iceberg.It is believed that this unknown internet is about 500 times the size of the surface web. We address the unknown part by the names Deep Web, Dark Netor Dark Web.

Dark Net is a type of network not accessible using normal modes of internet browsing and is not known to most people.Those who know about the Dark Net often confuse it with Deep Web, whereas both are different in many aspects. Deep Web – which includes Dark Net as a subset – is the part of the World Wide Web not indexed by normal search engines like Google, Bing,DuckDuckGo, etc.These standard search engines search only about 0.03% of the internet. To give clarity regarding Deep Web and Dark Net, their salient features are given in succeeding paragraphs.

Deep Web

Deep Web means list of websites your things your typical search engine is unable to find. Government databases, libraries, writings of activists in countries with strict internet control, etc, form part of the Deep Web. To understand the Deep Web an analogy of comparing the internet with the ocean may be drawn. When technology became advanced, humans built machines capable of diving to the depths of the oceans. That’s how we were able to discover secrets of the subterranean world including the remains of RMS Titanic. The search engine crawlers do the same work as done by the explorer submarines. They dive into the internet and take a note of whateverthey find so that they can return when required.We might have found Titanic, but there is a lot to discover in the bottomless oceans. Also since there are very deep parts of the oceans which have not been explored yet due to limitations of technology and accessibility which does not allow diving below certain depths. Similar is the case of the search engine crawlers and they haven’t identified large swathes of the World Wide Web which we call the Deep Web.For instance, the search engines won’t be able to access the servers and websites hosting data about some government-led secret alien mission.

However, the Deep Web isn’t as mysterious as it sounds. A private network that is not within reach of standard search engine crawlers,which can be right next to your house, will be tagged as Deep Web. For instance, the network maintained by some paid streaming service is a type of Deep Web asobviously, the search engines won't be opting for a monthly subscription to index the catalog of such websites.

Most of Deep Web contains nothing sinister and consists mainly of data bases, libraries and academic writings. The Dark Web or Dark Net is a small portion of the Deep Web that is intentionally hidden and made inaccessible via regular search engines. Most of the illegal activists, criminals and terrorists are found on this portion of the internet

Dark Net or Dark Web

Architecture of the Dark Net originally developed by the US Navy and it was originally created and funded as a project of the US Naval Research Laboratory in 2004, as a means of helping overseas political dissidents and democracy activists safely organise and communicate with each other.It is an encrypted network built on top of the existing internet, and specific software or tools are required to access the Dark Net asconventional protocols used on the internet do not work on it.

Exploring the Dark Net. Anyone can access this hidden internet,and it is surprisingly easy, but there is a lot of unsavoury content as well as a large number of criminals. There is nothing illegal in exploring till one starts asking for or giving the hidden services offered or sought.Since this space is full of shady elements, for an amateur it is best to be careful as you do not know where you might end up, what you might see, or whom you might meet.

There are numerous methods of exploring the Dark Net. The most popular is through a browser known as Tor or The Onion Router. Tor can be used to visit normal internet websites, but it also has numerous hidden websites and services which cannot be accessed on the regular internet. Tor powers them using its protocol known as Tor Hidden Service Protocol instead of the Hyper Text Transfer Protocol (http). The websites limited to the Tor network have a special .onion address. Due to this, Tor's Dark Net is also known as onionland. Onion is a metaphor for security layers which need to be peeled off as in an onion.

Friend-to-Friend (F2F) networks are another kind of Dark Net. In this case, two familiar people communicate with each other directly over the internet. They might want to share some file over a P2P connection. Such networks, not accessible by other people, can be encrypted or password protected. So, only the concerned people have the access.

Anonymity. Within the Dark Net, both web surfers and website publishers are entirely anonymous and the IP addresses are masked by software. Whilst large government agencies are theoretically able to track some people within this anonymous space, it is very difficult, requires a huge amount of resources, and is not always successful. To achieve anonymity, data is bounced around a number of intermediaries before reaching its destination. This means that there are a large number of proxy servers in various countries and data is redirected to more than 100 servers (in some cases)each time the network is accessed making it very difficult to track. The communication registers on the network, but the transport medium is prevented from knowing who is doing the communication. TOR users are supposedly tracked by US and other intelligence agencies but there have been very few successful interventions. There is no open source data available on tracking by Indian agencies.

Websites. The websites on the Dark Net are generally poorly designed. They are not visually appealing and many of them appear as basic excel sheets. The websites are extremely slow and it may take upto an hour for some of them to open regardless of the speed capability of the user's network. The emphasis is on functionality and not on aesthetic appeal. Website addresses are generally composed of a random-looking strings of characters followed by .onion, e.g. http://dppmfxaacucguzpc.onion/. This link will take you to a directory of Dark Net websites if you have Tor installed. However it is difficult and time consuming to find exactly what you are looking for and requires practice and patience.

Users. Tor has a large number of perfectly legitimate users including cyber experts, journalists, activists, whistle blowers, etc, who communicate with other experts/agencies in various fields.Website security experts and criminal hackers sharing the same forums to discuss their common interests in computer security even though their aims are different. Security agencies, government and law enforcement organisations are also amongst the main users of the hidden internet. It is popular amongst journalists, anarchist writers and political bloggers, especially those living in countries where censorship and political imprisonment are commonplace.Use of Dark Net for illegal activity is very popular as the biggest lure of this part of the internet is the anonymity it provides to the users. Terrorists also use it for anonymity, and so do the Dark Net's most publicized users—criminals. A number of reports have indicated that terrorist groups routinely use Tor and leverage the secrecy and anonymity afforded by Tor's encryption protocols to communicate, recruit new members, raise funds,procure weapons, spread propaganda and even plan operations. Terror organisations have posted training material and videos encouraging members to use Tor for all on line activities, especially after Edward Snowden leaked the interception techniques used by policing agencies.It is a fertile ground for violent groups and individuals to find each other and share their experiences, tips, and targets.

Services Offered. Most commonly traded illegal items appear to be for use by criminals like hacked mobile /internet banking accounts, drugs, fake passports and other IDs, child pornography, etc. However there are a lot of items of interest to terrorists like detailed resources on the preparation of explosives and toxins, forums, chatrooms and a number of websites belonging to extremist groups, guides to various forms of cybercrime, weapons for sale and video tutorials on how to use them, and of course, killers for hire.Individual hitmen market their services as well, along with detailed manuals on how to commit a murder, get rid of a body and/or frame somebody else. Many black market weapons shops operate through the anonymising Tor network, where the location and identity of their service is masked, allowing sellers and buyers to remain hidden. Deliverable hardware, like a weapon, is delivered to doorstep like a normal courier but disguised to look like a regular package.

Payment for Services. The underground currency is bitcoin and it was invented in 2009. It is a crypto currency andlargely behaves just like any other monetary system.A few websites such as Search Bitcoin behave as customized engines for locating items around the Web. There is no central banking group which manages and loans out these coins. They are created through computer processing – theoretically nothing more than time and GPU(Graphics Processing Units) compression. This also means no central authority is issuing "clearing" for bitcoin transactions. Thus you can transfer bitcoins anonymously between addresses in just a few hours. Anonymity and speed make it an ideal currency for illegal activities.

Bitcoin is used for both legal and illegal transactions and you can purchase perfectly legal items likeiphones with it.It can be exchanged and traded for dollars and other currencies.In the bitcoin marketplace, digital exchanges are held between buyer and seller and there is no need of any bank account or ID.A private key is given to each bitcoin user and this coin archive can either run through a desktop software or a third-party browser solution using online wallets, like Mt Gox. Currently the bitcoin exchange rate ranges from 700 USD to about 1100 USD, and it is traded like any ordinary currency with profits being made based on exchange rate fluctuations. Purchasing through the Tor/Onion network adds an extra layer of security and tracing the money trail is a very complex process.

Feasibility of Tracking/Shutting Downthe Dark Net

The Dark Net was created for good but has been increasingly used for clandestine operations due to its powerful abilities Tor has been downloaded nearly 150 million times and is used by more than by 2 million people daily. Value of a communication network is proportional to the number of users which makes it a very valuable network.

On the face of it, the Dark Net appears to be a handy tool for criminal, terrorists and anti social elements, and it is being exploited quite effectively. There have been a few arrests based on tracking the Dark Net but that does not seem to have affected operations on the network. A case in point being the Silk Road Black Market which is discussed below.

Silk Road Case. For nearly three years (2011 to 2014), Dread Pirate Roberts(DPR) operated the largest online criminal marketplace in the world known as Silk Road. It attracted one million users to create accounts on it, without any police intervention, and no one knew how to stop it. It used the Tor software, all parties buying and selling illicit goods were anonymous and used only made-up screen names. The only form of payment was Bitcoin which allowed parties to exchange funds on line with strong privacy protection. It dealt with illegal drugs, weapons, ammunition, computer viruses, compromised facebook accounts, fake documents and hitmen for hire. DPR was caught as he made a number of rookie errors including frequent log ons at the San Francisco Library. He is currently under trial.

However, after Silk Road, a new generation of Dark Net bazaars has risen in its place.Examples are Black Market Reloaded, Open market, Agora, etc. These markets are decentralised, which means that there is no leader to arrest and hence they are very difficult to shut down. As security forces get better at tracking the Dark Net, so do the defensive techniques. It is impossible to police the entire internet because people are always developing new ways of staying off the grid and, in all probability, the authorities will always battle with the Dark Net and the Internet. Shutting down the Dark Net is not possible currently unless the entire internet is shut down, which of course is not feasible. Hence the only possibility for security agencies or governments is to leverage the system to the best of their abilities.

Leveraging the Dark Net

Since most activities on the Dark Net are illegal, when government agencies use the Dark Net they have to be prepared to go into,at least, grey zones if not completely dark ones. Issues of ethics and values need to be set aside when leveraging the Dark Net and only the desired end result needs to be factored in. Most security agencies already do work in such domains without being overt about it. Kidnappings, political assassinations, use of illegal and untraceable weapons, blackmail, coercion, quid-pro-quo deals and other illegal means are used in a clandestine manner. The Dark Net may just make it easier for security agencies to operate in the grey zones without much fear of any comebacks. However there do need to be checks and balances to avoid misuse by own agencies.Nevertheless, it needs to be kept in mind that though entering the Dark Net is easy, navigating it is very challenging and it is very difficult to find out the exact service you need. Hence in-house expertise is required to be developed to successfully take advantage of the Dark Net. Once ‘services’ required are outsourced to professionals on the Dark Net, it is relatively easier for security agencies to remain anonymous, de-link and deny such links. Some options for leveraging the Dark Net by government agencies are given below.

Hiring of services/detectives to bring pictorial/video evidence in public domain/social media to discredit anti-government public figures. These services can include hacking into personal computers and stealing videos, pictures and data which can be used to coerce organisations or key individuals.This has been used very effectively by the Syrian government. Syrian opposition activists have been targeted using several Trojans, including one disguised as a Skype encryption tool and others disguised as revolutionary documents. More than a dozen of these attacks have installed versions of the same remote access tool, DarkComet RAT. Pro-Syrian government hackers now appear to have moved on to another remote access tool i.e.Blackshades Remote Controller, whose capabilities include keystroke logging and remote screenshots.Once it is downloaded,computers of these activists were essentially owned by the Syrian government, betraying their every move online. Their microphones captured everything they said, their keyboards gave away the most sensitive passwords and messages they typed, and their personal accounts were stolen and used to spread the attack to the next unsuspecting victim. In fact, the Blackshades Remote Access Tool (RAT)recently led to the arrests of some underground hackers around the world who had been using it to illegally take over thousands computers for their own gain.Blackshades has infected over half a million computers.

Hiring of hackers to facilitate identity theft of leaders of various echelons of terror organisations/ criminals/ anti social elements can be facilitated through Dark Net. Hackers can also be used to hinder functioning of anti national organisations through various cyber techniques, which can include bank account manipulation, stealing personal data, spamming, psychological conditioning through compromised data, email accounts and other social media campaigns.

"Need prices for grenade launchers"; "Buying bulletproof vests in bulk"; "Explosives how-to manuals"; "How to blow up a car"; "Need instructions on how to blow up a bridge" – these are just a few of the underground forum topics. The Dark Web provides an easy path to this type of information and discussion and people participating in such discussions are always suspect.

Trained manpower to trace illegal digital transactions is always at a premium for any government agency and the same can be hired from the Dark Net. Underground professionals can be scouted to give information on people undertaking shady deals/discussions in our area of interest or constantly seeking information which a normal citizen would not want. For the right price, almost anything is feasible hence the funding aspect also needs to be looked into.

Weapons which cannot be traced, including military grade weapons, can be procured.These weapons come in shielded packages to look like other products when shipped to clients. From the onset of the civil war raging in Eastern Ukraine, Russian language Dark Web forums have become hotbeds of information and service exchange on both sides in the conflict. One such store, operated by a former member of the Russian government apparatus, sells sniper rifles, machine guns, and military-grade assault weapons. It features crude photographs of its weapons, some of which show scrapes and scratches from use. Also offering free and guaranteed shipping worldwide, this store accepts bitcoins for its very inexpensively priced killing tools.

Hired hitmen are available in huge numbers on the Dark Net from sites such as ‘Killer for Hire’, ‘Quick Kill’, etc. Services are available for targeting specific strata including government officials, politicians and leaders of organisations. In exceptional cases, these services may be used against criminals or terroristswanted by the state for heinous crimes or those who are residing in other states or in inaccessible places for a specific price.

Using professional hackers from Dark Net sites can help to identify vulnerabilities in critical national networks. However since this can be a double edged weapon as hired hackers may also leak data to anti government organisations in case any vulnerabilities are detected and the same should be resorted after due diligence and strict access control.

Offensive zombification drugs like Scopolamine leaves victims coherent but with no free will and completely wipes victims memories of the incident. This can be a useful tool for secret service operations and such drugs are available on the Dark Net.

Specific forums are available to get ideas on topics related to the underworld and terrorism.

Exchange of ideas with the digital underworld to get solutions ‘from the other side’ can give new solutions to perpetual problems.

Conclusion

Law enforcement agencies across the world are, in all likelihood, already using the Dark Net in a covert manner. However the exact nature of their involvement is not clear due to the anonymity provided by the network. How far each state allows its agencies to interact on the network actually depends on the geo-political realm and the EVR (Environment, Values and Resources) congruence in which each state functions. However, the advantages of anonymity and reach of the Dark Net needs to be exploited to reduce the operating space of criminals and anti national elements.