Dark Net: Notes for UPSC Science and Technology

Dark Net, or Darknet, is an overlay system within the internet which can only be accessed through specialised software, authorization and configuration. This article will give details about the darknet within the context of the Civil Services Examination.

What is the Dark Net?

The darknet consists of a series of encrypted networks on the internet, which are not recorded or indexed by commonly used search engines such as Google or Yahoo. They can only be accessed through specialised software like The Onion Router (Tor) or The Invisible Internet Project (I2P)

According to computer experts, there are three layers of darknet

The first layers consist of regular and mainstream websites such as Facebook, Twitter, Instagram, Yahoo, Google etc. This reportedly makes up only 4% of the internet as a whole.

The second layer consists of data stored in inaccessible databases which are beyond the reach of conventional search engines. Only a select population has access to such files which are sensitive and private in nature.

It is the third layer, located in the deepest corners of the internet that are often referred to as the darknet which in turn is highly encrypted over the internet.

Find out more about the difference between WWW and the Internet by visiting the linked article.

Origins of Darknet

The term ‘darknet’ was coined in the 1970s to distinguish certain networks that were either isolated or beyond the reach of ARPANET, (Advanced Research Project Agency Network), which was a US government-funded military/academy predecessor to the Internet. Addresses in the darknet would receive data from the ARPANET, but it would not be listed under normal networks nor answer any pings.

The term gained more prominence upon the publication of "The Darknet and the Future of Content Distribution", a 2002 paper by Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, four employees of Microsoft. In this, they argued that the darknet was a threat to the development of a functioning digital rights management technology which made copyright infringement inevitable. The paper described darknet as any type of parallel network that is encrypted or requires a specific protocol to allow a user to access it.

Usage of Dark Net

The Dark Net is used for a variety of reasons. Some are as follows:

1. Protection of privacy of citizens from mass surveillance.
2. To commit cybercrime such as hacking, phishing, file corruption etc.
3. Protection of dissidents from political reprisals.
4. Sale of prohibited and baned goods on shadow markets
5. Whistleblowing and news leak of classified information to the public domain.
6. Purchase and sale of illicit goods and services
7. Bypassing network censorship, content-filtering systems and restrictive firewall policies.

Points of Discussion Regarding the Dark Net.

The level of anonymity offered by the surface net (the term used to describe networks which are part of the mainstream internet) pales in comparison to the one offered by the darknet. Hence, the darknet is a major focal point for a wide variety of illegal activities. In other words, it can be referred to as a virtual black market.

1. Criminals and other anti-social elements have been alleged to use the darknet to carry out data breaches and other hacking activities as it helps them to avoid detection and ensure their identities are safe from law enforcement agencies.
2. The same anonymity also makes it easy for drug dealers, arms dealer and other criminal elements to offer their services for potential buyers who can purchase anything from endangered species of animals to guns and illicit drugs.
3. Darknet is also used by activists to organize themselves without giving out their identities to law enforcement agencies. Chances are that most of the activists using the darknet may not necessarily have the right intention.
4. A darknet is also a useful tool for terrorism as those who indulge in it will use it to recruit more people into their ranks, purchase weapons illegally, spread malicious propaganda, raise funds through illegal means and plan attacks on the government and the civilian population.
5. It is speculated by security experts that hackers and fraudsters offer their services through the darknet to potentially damage critical infrastructure networks of power plants, oil refineries and various other facilities across the world.

Conclusion

With the rise of virtual currency in the financial world, it is highly likely that the darknet will become an everyday feature for internet users in the future. For the moment, the anonymity provided by the darknet will provide ways and means of eluding capture while still eluding capture

But even with all the encryption put in place, true anonymity is never guaranteed as the technology to circumvent it keeps evolving.

Keeping this in mind, governments across the world should strengthen their Cybersecurity Framework to deal with the threats posed by darknet. They must cooperate with each other regarding securing the Cyberspaces worldwide through intelligence, information, technology and expertise sharing.