TERROR IN THE DEEP AND DARK WEB

E. DILIPRAJ

The internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had.

— Eric Schmidt[1]

HOW IT STARTED?

Starting as a mere concept named "Galactic Network" by J.C.R. Licklider of MIT in August 1962, the 'internet' has in the past few decades revolutionised the way this world communicates. Having been technically nurtured in the Defence Advanced Research Projects Agency (DARPA) from early the 1960s to the late 1970s, the internet, i.e. the then ARPANET, has undergone various phases, starting with the sending of host-to-host messages with mere packet switching technology in extreme low speed (2.4 kbps – 50kbps) in 1969, to the advancement of the host-to-host protocol of ARPANET called "Network Control Protocol" (NCP) in 1970, to the introduction of 'electronic mail' service in 1972 for an easy coordination mechanism in ARPANET which took off as the largest network application for over a decade. Later, due to the inability of the NCP to adapt to the open-architecture network

E.Dilipraj is a Research Associate at the Centre for Air Power Studies, New Delhi.

[1] Eric Emerson Schmidt (born April 27, 1955) is an American software engineer, businessman, and was the executive chairman of Google. He is a member of President Obama's Council of Advisors on Science and Technology (PCAST). In 2013, Forbes ranked Schmidt as the 138th-richest person in the world, with an estimated wealth of $8.3 billion. http://www.brainyquote.com/quotes/keywords/internet.html, accessed on March 9, 2014.

environment which would globalise the network, a new protocol called Transmission Control Protocol/ Internet Protocol (TCP/ IP) was developed.[2]

While file transfer and remote login (Telnet) were very important applications, electronic mail was probably the most significant innovation which expanded new methods of communication by providing a model in the building of the internet itself. Slowly, various proposals started pooling in that would expand the applications of the internet, including packet-based voice communication (the precursor of internet telephony), various models of file and disk sharing, and early "worm" programmes that showed the concept of malware agents. Thus, the internet, which was initially designed for one application, i.e. file sharing, became a platform for conceiving many applications in it which became a reality when the 'World Wide Web' (WWW) was introduced. While Ethernet technology was developed in 1973, this technology coupled with the widespread developments of LANs (Local Area Networks), PCs (Personal Computers) and workstations, led the nascent internet to flourish in the 1980s.[3]

While file transfer and remote login (Telnet) were very important applications, electronic mail was probably the most significant innovation which expanded new methods of communication by providing a model in the building of the internet itself.

As a result of the increase in scale of the internet, many managerial issues were faced and solved. To begin with, the hosts were assigned names (early URLs) which made it unnecessary to remember the hosts' numeric addresses. Next as the connectivity increased, the simple single distributed algorithm routing technique-based routers were replaced with the hierarchal model routing-based routers which permitted different regions to use a different Interior Gateway Protocol (IGP), so that different requirements for cost, rapid reconfiguration, robustness and scale could be accommodated. Also, with the evolving internet, a supporting operating

[2] Leiner et al. "Brief History of the Internet", *Internet Society*, 2013.

[3] Ibid.

system was also developed that helped in the widespread adoption of the internet. Soon after the transfer of ARPANET from NCP to TCP/IP on January 1, 1983, ARPANET was split into a MILNET supporting operational requirements and an ARPANET supporting research needs, thus, forming a precursor for the civilian use of the internet. Consequently, by 1985, the internet became well established as a technology that supports a broad community of researchers and developers, and was also used by other communities for daily computer communications, especially electronic mails.[4]

By 1985, the internet became well established as a technology that supports a broad community of researchers and developers, and was also used by other communities for daily computer communications, especially electronic mails.

As DARPA's ARPANET was progressing on one side, many more agencie which were able to secure a funding started developing their own networks on the lines of ARPANET. The US Department of Energy (DoE) established MFENet for its researchers in Magnetic Fusion Energy, whereupon DoE's High Energy Physicists responded by building the HEPNet. The National Aeronautics Space Agency (NASA) space physicists followed with SPAN, and the academic and industrial computer science community, with an initial grant from the US National Science Foundation (NSF), established the CSNET. Apart from these networks, one another landmark network that was developed was the NSFNET with TCP/IP which during its lifetime grew to 45 mbps links with over 50,000 networks on all seven continents and even in outer space. As a result of the successful development of various networks by the US and other international government funded agencies, commercial sectors around the world also started showing interest in this technology during the late 1980s which opened the way for commercialisation of the internet in the early 1990s.[5]

[4] Raphael Cohen, "Internet History", *International Journal of Technoethics*, 2(2), 45-64, April-June 2011.

[5] Leiner et al. n.2.

Although initial commercialisation of the internet was restricted only to the vendors and buyers of military related technology, their hard work in successfully achieving interoperability among their products widened the scope for the internet to spread to other fields as well. Therefore, on October 24, 1995 the Federal Networking Council (FNC) passed a resolution defining the term 'internet'. The definition is as follows:

- The Federal Networking Council (FNC) agrees that the following language reflects our definition of the term "Internet". "Internet" refers to the global information system that:
- is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons;
- is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and
- provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.[6]

Thus, a concept which was conceived in the era of time sharing, prolonged its stay and expanded its borders by adapting itself to function and grow along with the new developments in computer technology like the personal computer, client-server peer-to-peer computing, network computing, LANs and also by supporting a wide range of functions from file sharing and remote login to resource sharing and collaboration, and has spawned electronic mail and later, the World Wide Web. The scope for adaptability combined with the huge investment from the commercial sector into this successful promising technology made the internet become a 'commodity' from its initial state of 'luxury'. Also, "the availability of this pervasive technology (internet), along with powerful affordable computing and communications in portable form (i.e., laptop computers, PDAs, cellular phones), has created a new paradigm of widespread nomadic computing and communications."[7]

[6] Ibid.

[7] Cohen, n.4.

Even during its experimental phase, as a luxury technology, the internet had attracted thousands of users which, eventually, in due course of time as it became more commercialised, have multiplied into millions. The uses of the internet as a platform for networking, communication, knowledge gathering, research and entertainment elevated with the invention of various new applications like e-mail, websites, blogs, chat rooms, immediate messages, music and video sharing, online news media, and more recently, social networking, all of which have transformed the internet into a necessary commodity. This is clear from the fact that in just over a span of two decades since its commercialisation, the internet has gained more than 2.4 billion users around the world.[8] As the internet has drastically reduced the cost and time for communication, more and more people have embraced this technology. Especially since 2005, the number of users has increased by more than 1.4 billion mainly due to the expansion of social networking, online shopping and other forms of easy communications, including Video Voice over Internet Protocol (VVoIP) services like Skype. Moreover, the amount of information available in the indexed internet is estimated roughly to be more than 5 million terrabytes according to Google which includes texts, pdfs, images and videos.[9] But the catch here is that nobody or no search engine can either accurately calculate the amount of information available online or ascertain the exact number of websites, blogs or videos available online. This is because the once close knit internet has in time grown so big that it has become virtually impossible to be indexed. Thus, the un-indexed internet which is hidden in the darkness, deep under the indexed surface web is known as the 'deep web, hidden web, or invisible web'. The definition and the genesis of these terminologies are discussed in detail in the following sections.

WHAT IS THE 'DEEP WEB'?

During the early days of the internet, the information available in it was very little which was easily indexed and the users were also able to access it easily. But the situation changed as the usage of the internet expanded.

[8] http://www.internetworldstats.com/stats.htm, accessed on March 11, 2014.

[9] http://www.wisegeek.org/how-big-is-the-internet.htm, accessed on March 11, 2014.

As a result, indexing of information in the internet was based on queries entered in search engines. The conventional search engines were able to retrieve static pages but proved inefficient while retrieving dynamic pages. A static page is linked to other pages on the internet. On the other hand, a dynamic page is linked to a particular web page and can be retrieved only through targeted queries or keywords. This created a gap between the static and dynamic web pages in the internet and the gap started to widen as time passed. Therefore, in 1994, Dr. Jill Ellsworth coined the phrase 'invisible web' to refer to information that was 'invisible' to queries of the conventional search engines used in that time period.[10]

Later, in 2001, Michael K Bergman, a web scientist, coined another term, 'deep web' in his paper titled "The Deep Web: Surfacing the Hidden Value". His definition for the term deep web was no different from Ellsworth's term 'invisible web', but he avoided using this term because his main aim was to discover automated means for identifying deep web sites and directing queries to them in order to make these invisible pages visible on the surface web. He also aimed at quantifying the size of the deep web and at characterising the quality of content in the deep web. Since Bergman's paper was the first extensive research on the invisible/ deep web and also because it became widely famous among the web research community, the term 'deep web' prevailed over 'invisible web' to refer to the unindexed sources of the web. Therefore, the definition for the term 'deep web' would be as follows:

The information content on the internet (web pages, documents, files, images, etc) which are:

- inaccessible through direct queries in the conventional search engines;
- which can be accessed only through targeted queries or keywords;
- which are not indexed or which are unable to be indexed by the conventional search engines;
- which are protected by security mechanisms like login IDs, passwords, membership registrations and fees.

[10] Michael K., Bergman, White Paper: "The Deep Web: Surfacing Hidden Value", *Journal of Electronic Publishing*, vol 7, issue 1, August 2001.

In short, the information content on the internet which cannot be accessed directly through conventional search engines but requires a targeted approach is called the 'deep web' or 'invisible web' or 'hidden web'.

In order to better understand the concept, let us consider the example of one well known deep web resource in the internet: "JSTOR". JSTOR is a widely used academic digital library of books, journals and primary sources that started in 1995. Since then, it has got a huge collection of articles and books in various formats which can be downloaded by its users by getting access through membership and fees. Any queries on the search engines for the articles available in JSTOR would take us to the JSTOR's page but one cannot download the articles directly by just reaching those pages, without paying the fees and getting the membership. Moreover, since JSTOR became famous over the years, the search engines adapted their crawlers to accommodate the web pages of JSTOR in their results whereas there are numerous other web pages like JSTOR with immense information content which are still hidden or invisible from the crawlers and spiders of the search engines. The search engines like Google, Bing, etc are constantly altering their algorithms to make their crawlers reach the deepest point possible in order to retrieve information and, most importantly, to index it in their results. Yet, the internet is becoming bigger every minute, paving the way for deeper web resources which are hidden from the eyes of the search engines. According to the processor manufacturing giant Intel, in every minute in the internet, the following things happen:

- 639,800 GB of information is transferred globally;
- 204 million e-mails are sent;
- there are 135 Botnet infections;
- there are 1,300 new mobile users;
- 4,7000 apps are being downloaded;
- $83,000 worth sales take places in Amazon.com;
- 30 hours of video is being uploaded in Youtube;
- 6 million views in Facebook;
- there are more than 100,000 new tweets;
- 300 new photos are uploaded in flickr;

- more than 100 new linked in accounts are opened;
- there are more than 2 million search queries in Google and much more.[11]

While the above mentioned list is just a sample, the real magnitude of information being processed in a minute is much bigger than any estimate.

The dark side of the internet includes adult content web sites, forums, chats, explosives courses, hackers, assassins, human trafficking, black market of weapons and drugs, etc which are hidden in secret web links.

DARK WEB, DARK NET AND DARK INTERNET: DEFINITIONS AND CONCEPTS

The internet/ surface net which provides its users with information and entertainment also has another dark face to it. The dark side of the internet includes adult content web sites, forums, chats, explosives courses, hackers, assassins, human trafficking, black market of weapons and drugs, etc which are hidden in secret web links. This part of the internet which causes grave danger to the world cyber community and also to global security in general is a part of the deep web and is called the 'dark web'.

The 'dark web' can be defined as *the portion of the deep web which contains generally the illegal and anti-social information and can be accessed either through conventional browsers or specialised browsers for accessing the secretive web links.*

In recent years, the dark web has been moving towards more secretive locations due to the crackdown of the government agencies on it. The dark web is a lucrative location for criminals and other anti-social elements as it provides it a natural cover from the government agencies. Moreover, the unaccounted huge economy involved in the dark web is like a treasure hunt for perverted minds. Also, the black market of drugs, weapons, fake IDs, human organs, human trafficking, etc requires an anonymous location to operate without the fear of monitoring by the government agencies. Therefore, in recent years, more and more dark net sites are turning towards

[11] http://www.intel.com/content/www/us/en/communications/internet-minute-infographic.html, accessed on March 14, 2014.

secret domains like '.onion' sites which cannot be accessed through conventional browsing methods. Hence, before going into detail about the terror in the deep and dark web, it is imperative to know how to get access to these secretive dark web sites in the deep web.

Being a global public medium of interaction, any information on the internet is traceable to its point of origin or can be interrupted to cause damage to the information. This vulnerability was not acceptable to many players of the internet.

THE ONION ROUTING

Being a global public medium of interaction, any information on the internet is traceable to its point of origin or can be interrupted to cause damage to the information. This vulnerability was not acceptable to many players of the internet and, thus, the need for a secured encrypted method of networking was realised which would not only keep the data safe but also safeguard the anonymity of the users.

Thus, 'The Onion Routing Project' (Tor Project) was developed with initial sponsorship from the US Naval Research Laboratory. Its current sponsors include the US Department of State Bureau of Democracy, Human Rights, and Labour, SRI International, National Science Foundation, Radio Free Asia, Ford Foundation, Google Summer of Code, an anonymous North American Internet Service Provider (ISP), and more than 4,300 personal donations from individuals.[12] "The current Tor Project claims that it is a non-profit organisation which works towards privacy and security on the internet."[13]

Tor and its Operations

Tor is a free software bundle which can be downloaded from its official web site www.torproject.org. Its initial release was on September 20, 2002, and it is a cross-platform software which can work on almost all operating systems. The Tor bundle uses Mozilla Firefox as the embedded browser for accessing the internet. Tor gets its name from its encryption method, where layers of encryptions are stacked one above the other like an onion in order to provide

[12] "Tor: Sponsors, " http://www.torproject.org.in/about/sponsors.html.en, accessed on March 16, 2014.

[13] Ibid.

anonymity to the communications and also to hide the origination node of the communication. Any communication on the internet has two parts: the data payload and the header for routing. The conventional encryption softwares were able to encrypt the data payload but failed in hiding the header, whereas Tor is different from previous encryption softwares in a way that it can not only encrypt the data payload but can also hide the header which is used for routing, thus, erasing the cyber footprint of any communication and creating more privacy, security and anonymity for its users.[14]

When a user is connecting through the Tor bundle, the user's system becomes a Tor client and obtains a list of Tor nodes from a directory server through an encrypted link. The Tor nodes are nothing but various users (Tor clients) around the world who have volunteered their systems to act as an enroute for the Tor network.

When a request is made from the user to connect to a web site, the software builds its own encrypted random path called circuit across the Tor nodes to reach the destination. The circuit is extended one hop at a time i.e. each node only knows from where it takes the relay and where it has to pass on the relay and so no node in the entire circuit is aware of the whole path any data packet has taken. Also, each hop has its own encryption key which masks the path of the data packet. Once a circuit is established, any kind of communication can be made or several different softwares can be deployed through the Tor network. Also, in order to be more efficient, the Tor network uses the established circuit only for a certain time period and for later requests, a new circuit gets connected to its destination which delinks the data path of earlier actions of the user from the path of the new requests and, hence, erases the footprint.

Hidden Services in the Tor Network

Apart from providing the function of an anonymous browser bundle, Tor software also offers other hidden services like web publishing and instant messaging service through anonymous servers configured exclusively for these hidden service purposes. This hidden service helps the Tor users to publish a web site in the Tor network where users can publish materials

[14] Ibid.

and access the information online in these web sites without any kind of censorship. Moreover, because of the anonymity provided by the Tor network, neither will the users know the owner of the site nor the owner know who is posting information or accessing the site.

Before moving further in discussing how the hidden services work, it is essential to know why the users of the internet require such hidden services or in general, why the users wish to be anonymous while going online. The answer for this question in simple terms is "fear of being identified". In the real world, people have a personal and a professional life, likewise, in the virtual/cyber world too, the users have their own personal and professional identity which most of them would like to keep delinked from each other. This is because of the kind of activities they carry out with their personal identities. For example, a person who is working in a government establishment, may not like, or agree with, all the policies of the ruling government. But since his career is based on it, he/she would remain silent in the real world without showing dissatisfaction. When the same person goes online and when he/she knows that he/she can share anything without revealing his/ her identity, he/ she creates his/ her discrete personal online identity to share his/ her dissatisfaction through social networks, forums or chat rooms, etc. But such people may not link their other professional identity to their personal identity in order to remain clean and unnoticed. Also, more crooked minded people use this anonymity provided by the internet for unethical reasons and to be hidden from being identified in the real world. This remains the case for all other anonymous uses of the internet and its hidden services by its users around the world.

While the fear of being identified remains the main reason for anonymity by the users, the technology that allows them to be anonymous works as follows. The hidden services work on "rendezvous points" through which Tor users connect to the hidden services offered in the Tor network, each without knowing the other's network identity.

> The hidden services in the Tor network have to advertise themselves to the clients about their existence because they are hidden unlike the services in the public internet where the web sites are well connected and have a user

friendly URL. Therefore, the service randomly picks some relays, builds circuits to them, and asks them to act as introduction points by telling them its public key. The hidden service assembles a hidden service descriptor, containing its public key and a summary of each introduction point, and signs this descriptor with its private key. It uploads that descriptor to a distributed hash table. The descriptor will be found by clients requesting abc.onion where 'abc' is a 16-character name derived from the service's public key.[15]

After establishing the connection, the client downloads the descriptor from the distributed hash table. The client will come to know the set of introduction points and the right public keys to use from the descriptor for abc.onion. Simultaneously the client also creates a circuit to another randomly picked relay and asks it to act as a rendezvous point by telling it a one-time secret. When the descriptor is present and the rendezvous point is ready, the client assembles an introduce message and sends it to one of the introduction points, requesting it be delivered to the hidden service. As the communication is carried out in the Tor network, the client's IP address cannot be related with the introduced message and, thus, the client remains anonymous.[16]

The hidden service decrypts the client's introduce message and finds the address of the rendezvous point and the one-time secret in it. The service creates a circuit to the rendezvous point and sends the one-time secret to it in a rendezvous message. Finally, the rendezvous point notifies the client about successful connection establishment which enables both client and hidden service to use their circuits to the rendezvous point for communicating with each other. The rendezvous point simply relays (end-to-end encrypted) messages from client to service and vice versa.[17]

[15] "Tor: Hidden Service Protocol", in http://www.torproject.org.in/docs/hidden-services.html.en, accessed on March 17, 2014.

[16] Ibid.

[17] Ibid.

Generally, a complete connection between a client and the hidden service consists of six relays: two of them picked up by the client with the third being the rendezvous point and the other three picked up by the hidden service.

The hidden service supported by the Tor network attracts many users around the world, who wish to hide from government monitoring or bypass any kind of censorship, to publish their '.onion' websites which can be categorised under various fields ranging from encrypted mails services, hidden social networking, whistleblowers sites like Wikileaks, online shopping, to the murky sites like the black market of drugs and weapons, hitman services, adult pornography, cyber laundering, etc. Most of the .onion sites are unstable in nature as they do not exist in a particular URL for long time. Another catch here is that the proportion of the dark web is much bigger and it is growing every minute in its size, depth, number of users and also in terms of services offered by these web pages.

TERROR IN THE DEEP AND DARK WEB

As the dark web is growing in its size and usage, it is offering a variety of services to its users. But the nature of the services offered in this dark web is a threat to the real world as most of them are illegal, ranging from drugs, weapons, hitmen to pornography and money laundering. Although such services are prohibited in the real world, the natural cover provided by these hidden services increases the magnitude of their usage online. More and more users are attracted by the fact that they can anonymously use these services for their personal gains. A deeper look into the kind of terror existing in these dark web services would help understand the real danger.

Black Market

Similar to the online shopping facilities offered in the internet/ surface net, the dark net also offers its users a number of deep and dark online markets where the only difference is the products sold in them. While books, clothing, watches, footwear, jewellery are the usual products for sale in the surface net, the deep web/ dark web online markets are filled

The deep web/ dark web online markets are filled with products like drugs (stimulants, psychedelics, prescription, precursors, ecstasy, dissociatives, cannabis, steriods/ PEDs,etc), arms, weapons, ammunitions, fake IDs, stolen electronic goods, stolen or skimmed credit card details, stolen art works, banned books, and other illegal products.

with products like drugs (stimulants, psychedelics, prescription, precursors, ecstasy, dissociatives, cannabis, steriods/ PEDs,etc), arms, weapons, ammunitions, fake IDs, stolen electronic goods, stolen or skimmed credit card details, stolen art works, banned books, and other illegal products. A few dark web market pages like "Silk Road" offer a holistic service of sale of various products while a few other web pages like "Only.Cigs"[18] offer only particular products. 'Only.Cigs' is a deep web market which offers its users all brands of cigarettes around the world and 'Silk Road' is the most popular and the most notorious black market in the dark web.

'Silk Road' is dubbed as the 'ebay of the deep web' by its users as its service is similar to that of ebay of the surface net. Anybody who has a product for sale can register in the 'Silk Road' web page and post a picture of the product and the pricing in the appropriate product category. Any user who wishes to buy the product can login and purchase the product by making the payment to the web page. Every vendor has his own track record for credibility and authenticity which increases the trust factor among the buyers to buy a product from a vendor. The fact that all payments are through crypto currency, 'bitcoins',[19] makes the conditions favourable for the users in order to avoid the involvement of any financial agency to oversee the whole process. Also the products are delivered either at one's doorstep or at a pick-up point. The service is offered all around the world expect for a few constraints by some vendors for delivery in some parts of the world.

[18] http://cigs7cviqbi4bvuy.onion/, accessed on March 21, 2014.

[19] Bitcoin is a digital currency mined using cryptographic techniques. It is used as a peer-to-peer payment system and was introduced by Satoshi Nakamoto in 2009. It is now being used as the major transacting money in the internet.

During the conduct of this study, 'Silk Road' offered a variety of products under various categories like alcohol, apparel, art, biotic materials, books, computer equipment, custom orders, digital goods, drug paraphernalia, drugs (stimulants, psychedelics, prescription, precursors, ecstasy, dissociatives, cannabis, steriods/PEDs), electronics, erotica, forgeries, hardware, herbs and supplements, jewellery, lab supplies, lottery and games, medical, money, packaging, services and writing.[20] Similarly, there are many other web pages in the deep and dark web which offer similar products to users. There are also web pages like "UK Guns and Ammo Store"[21] exclusively for the sale of arms and ammunition. In general, it can be stated that almost 30 percentage of the dark web resources are filled with these online black markets of illegal products which pollute the society and can cause serious damage to its stability.

Adult Content

Although the surface net also has a number of pornographic sites, the dark web pornographic content is much bigger in size and more cruel in nature. Most of this dark web adult content can only be accessed by becoming a registered user or by paying some fees to the web pages. Apart from the web pages, there are also forums and chat rooms like "Dark Nexus"[22] in the deep web where its users discuss their evil minds with one another. The adult content pages constitute more than 40 percent of the dark web while most of its contents comprise videos.

Fake IDs, Middleman Services and Other Financial Services

The deep web is also the hub of other illegal activities like making of fake IDs, sale of counterfeit banknotes, stolen credit/ debit cards, PayPal accounts, etc. There are many web pages in which fake IDs can be ordered, made and delivered for a particular price. These fake IDs include passports, driving licences, identification cards, etc. Stolen or skimmed credit/ debit cards, counterfeit banknotes are the other products that are sold in the deep web through many web pages.

[20] http://silkroad6ownowfk.onion/login, accessed on March 21, 2014.

[21] http://tuu66yxvrnn3of7l.onion/ ,accessed on March 21, 2014.

[22] http://e266al32vpuorbyg.onion/, accessed on March 22, 2014.

A few other pages offer some sort of middleman services to their users wherein individuals offer to help the users in all sorts of illegal activities for a certain price. A few web pages are also dedicated to 'assassination services' where the user has to give the name and other details of the person to be assassinated and pay for the service or in some cases even worse, where the users are asked to bet on a few people's date of death and anybody who guesses correctly, is rewarded[23].

While many web pages do not support negotiations, a few give the option of negotiable price. In a few web pages, the buyer has to directly place the order and wait for the product to be delivered, while in others, if the vendor is an individual, the e-mail ID of the vendor is given so that the user can contact the vendor directly through e-mail and place the order after price negotiations. Web pages which offer fake IDs, counterfeit banknotes, stolen credit/ debit cards and other financial and middleman services constitute around 10 percent of the dark web resources and are mostly owned and operated by individuals or a small group of people who wish to make by money in the shortest way possible.

Other dark web contents include forums and chat rooms where like-minded wicked people discuss their evil ideas among themselves. It also includes the sale of banned books, training materials for explosives and other chemical components including RDX, etc. In addition to this, terrorist literature and other types of anti-social literature which is appealing to like-minded readers is also found here. Besides that, sports betting, illegal gambling and lottery are also a part of the dark web financial services. Furthermore, there are also more gruesome web pages which provide their readers the results of banned and cruel medical tests conducted on people, offer human organs for sale, and much more.[24]

IMPLICATIONS OF DEEP AND DARK WEB ON GLOBAL SECURITY

From the above description about the deep and dark web, it is obvious that it poses a serious threat to security in the cyber/ virtual world, but it should

[23] http://assmkedzgorodn7o.onion/, accessed on March 23, 2014.

[24] https://torlinkbgs6aabns.onion.to/, accessed on March 24, 2014.

also be noted that in the longer run, the services provided in the deep web, especially in the space of dark web, pose a greater threat to global security on the whole.

How Does the Deep and Dark Web Affect Global Security?

First, the hidden services which offer easy access to encrypted e-mails, forums, chats and other forms of file sharing services provide a safe haven for the terrorists and other non-state actors to communicate among themselves without any oversight of the government intelligence agencies. While the contents of the internet/surface net are being heavily monitored by the intelligence agencies of the world to spot the presence of any suspected terrorists, the deep web with its hidden services provides the hiding ground for them. Moreover, since the location of the user is masked while using the hidden services with proper precautions, this facility enables the terrorists to be active on the deep web with no fear being caught. Therefore, the deep web acts like a 'treasure trove' which provides them with anything and everything from encrypted means of communication, file sharing, training grounds, knowledge sharing, recruitment, to planning and coordination. They also attract funds for their organisation and their cause, using these hidden services of the deep web, by accepting bitcoin donations which they, in turn, use for purchasing weapons in the dark web black markets and use these against the society. For instance, "Fund the Islamic Struggle without Leaving a Trace" is a web page in the deep web which invites donations for *jihad* through bitcoin transactions to a particular bitcoin address.[25]

Secondly, the services and resources of the deep web and dark web are already a lucrative target for the black hat hackers, cyber thieves and other anti-social elements who concentrate their efforts in robbing the economy of the deep web for their personal financial gains. As most of the transactions in the deep web are through virtual currencies like bitcoins and through online money transactions like PayPal, these services are under heavy cyber attack by the hackers and cyber thieves to steal the wealth available on various web pages and from various virtual currency miners, stock holders

[25] http://teir4baj5mpvkg5n.onion/, accessed on March 25, 2014.

While the international community is fighting over governance of the internet, the existence of the deep web and its resources and services comprise a bigger concern for the parties that would govern the internet in the future.

and account holders. Also the virtual economy poses a grave threat to the economy of the real world as it is very unstable and also because of the fact that it does not have any accountability to it. Therefore, the deep web services act as a lucrative safe house for the anti-social elements to carry out their cyber laundering (online money laundering), through gambling, betting, lottery and even through direct encrypted transactions in the dark web. Furthermore, the issue of cloned and skimmed credit/debit cards details and other financial details being sold in the deep web creates chaos in the real world banking system. If this situation continues, it can also be stated that the theft of bank details and credit/ debit card details will increase in the future.

Thirdly, the dark web in particular is a great threat to the future generation users. Human psychology is such that the mind gets easily attracted to all the wrong things first, and the future generation, comprising children today, would be attracted towards the dark web easily, thereby changing the mindset of a whole generation. This will result in the internet being used in the future as a hub for illegal activities as the user has no fear of being caught. As a result, more and more cyber terrorists will come up who will pose a great danger to the cyber security of the world. Moreover, the uninterrupted sale of drugs and weapons, arms and ammunitions, fake IDs, etc in the dark web would result in the increase of drug addicts and juvenile criminals in the future. Also, the huge amounts of adult content material like pornography which can be easily accessed in the dark web would also result in creating warped mindsets and criminal thoughts in the minds of children who may end up becoming criminals in the future.

Finally, internet security and, on the whole, cyber security is at stake due to the hazardous effects of the deep and dark web. While the international community is fighting over governance of the internet, the existence of the deep web and its resources and services comprise a bigger concern for the parties that would govern the internet in the future. Also, it intensifies the debate between open source and restricted access, censorship, monitoring, surveillance and other forms of supervisory mechanisms imposed on the internet.

How is it Being Tackled?

Although action by the security agencies against the deep web may seem impossible because of the way it has made deep inroads into the lives of netizens around the world, the security agencies are trying their best to bring order in this chaotic deep space. While they have had success in some instances, they are still struggling on many fronts.

> For instance, in August 2013, almost 50 percent of the known .onion deep web pages completely vanished off the deep web network due to the crack-down on a hosting operation in Ireland. The hosting operation named as 'Freedom Hosting' was hacked using the 'javascript exploit' in the Firefox browser version 17 which was embedded in the Tor Browser bundle then and was taken down by the Federal Bureau of Investigation (FBI) of the US. Also, the owner of the Freedom Hosting infrastructure, Eric Eoin Marques was arrested and extradited from Ireland to the US. His infrastructure which hosted many of the .onion sites utilised 550 servers around Europe and offered space to anyone who wanted it, with a promise to never look at the contents personally. The hosting service was targeted by FBI because it was diagnosed that this infrastructure was the major hub in distributing child porn in the dark web.[26]

Later, in another instance, the black market giant in the deep web, 'Silk Road' was taken down on October 2, 2013 by the FBI in an operation conducted after years of painstaking process of piecing together the cyber footprints of the operator of the website and it also resulted in the arrest of the main operator Ross William Ulbricht aka Dread Pirate Roberts (DPR).

[26] "The Ultimate Guide to the Deep Web", in http://www.sickchirpse.com/deep-web-guide/, accessed on March 24, 2014.

It is impossible for any one country's government agencies to tackle all the problems of the global internet—the issue is too big for any one country to handle alone.

The FBI seized more than 26,000 bitcoins worth $3.6 million from accounts on Silk Road and 144,000 bitcoins worth $28 million that belonged to Ulbricht.[27] Subsequently on December 2, 2013, three more administrators of the site were also arrested. [28] Thus, bringing the whole dark net black market giant to a standstill, the FBI proved to the world that even the deep web can be traced, tracked, monitored and controlled by the law enforcing agencies.

Nevertheless, 'Silk Road 2.0' was resurrected by former associates of Ulbricht and it started functioning and with more security mechanisms from early November 2013. Many of the dark net sites which were brought down due the shutdown of the Freedom Hosting service, changed their hosting space and resurfaced again in the dark web. It is impossible for any one country's government agencies to tackle all the problems of the global internet—the issue is too big for any one country to handle alone. Also, many legal issues surface between various countries during the various phases of the investigation into any particular case. Also, the level of technicalities involved in the process make the issue more complex. Therefore, till the time some sort of proper governance is evolved for the internet, the law enforcing agencies of various countries and the criminals dwelling in the deep and dark net will keep on playing their cat and mouse game.

[27] Dave Lee, "Silk Road: How FBI Closed in on Suspect Ross Ulbricht", *BBC*, October 2, 2013, in http://www.bbc.com/news/technology-24371894, accessed on March 26, 2014.

[28] Andy Greenberg, "Feds Indict Three More Alleged Employees of Silk Road's Dread Pirate Roberts", *Forbes*, December 12, 2013, in http://www.forbes.com/sites/andygreenberg/2013/12/20/feds-indict-three-more-alleged-employees-of-the-silk-roads-dread-pirate-roberts/, accessed on March 27, 2014.