MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

The Dark Web and Regulatory Challenges

Debopama Bhattacharya

July 23, 2021

Summary

The anonymous chat rooms and communication services on the dark web have made it an ideal platform for planning and coordinating dangerous criminal and terrorist activities. Greater international cooperation and steps like automatic deletion of personal data after a stipulated time period by mobile applications which collect account information for digital wallets, for instance, could increase the efficiency of cyber systems and prevent repeated incidents of data breaches.

The World Wide Web (WWW) hosts the enormous connection of web pages on the network of computers connected through the internet. The WWW, or simply the web, consists of the 'surface' web and the 'deep' web. The surface web is that portion which can be accessed by the ordinary internet users using standard search engines like Google, Yahoo, etc. But it can retrieve only an approximate 4 percent of the search results, while the majority of the results are hidden.

The other portion, known as the deep web, constitutes 96 percent of the web. The password-protected or paywall-protected websites, including online banking services, for instance, are considered a part of the deep web. Such websites hold the information relating to accounts of millions of individuals that is not accessible to the entire web population. The content of personal databases like email accounts, social media accounts, scientific and academic databases, legal documents, etc. that are accessible to only a closed group also form part of the deep web.

Within the deep web, there are some parts which are completely concealed, and are accessible by using specific software browsers, like Tor. These parts form the 'dark' web, also known as the invisible or the hidden web. The browser software used to access the dark web offer anonymising and encrypting facilities to the users so as to intentionally hide their browsing patterns, location and actual identities.

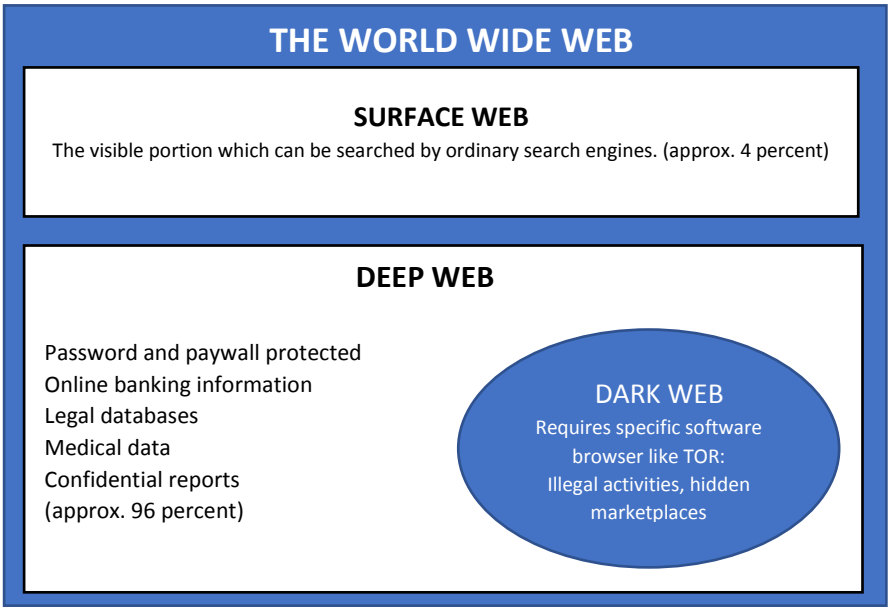

Figure I: Different layers of the World Wide Web (proportion not to scale)

The dark web has turned into a hot bed of illegal transactions, posing a threat to the cyberspace across multiple dimensions. Since anonymisers on the dark web make it difficult to track web patterns such as browsing history, location, etc., they are misused by criminals to hide their identities and carry out nefarious activities.

The infamous dark web market, 'Silk Road', was the first modern dark net market, best known as a platform for selling illegal drugs. This was taken down in 2013.[1] Since then, users across the world have searched the online dark market to anonymously access weapons, credit card data, malware, Distributed Denial of Service (DDoS) and stolen data, among others.

Accessing the Dark Web

In order to access the dark web, specific browser software are needed. Software like the Onion Router (Tor) browser, FreeNet, Invisible Internet Project (I2P), TAILS (The Amnesic Incognito Live System), Whonix and many others have made it convenient to navigate the dark web.[2] These software allow anonymity and confidentiality on the web by use of techniques like Proxy (an intermediate between sender and receiver for bypassing internet censorship), Tunneling/Virtual Private Networks (network providing inter-connectivity between various entities to provide secure communication), and by translating domain names to IP addresses in order to make it easier to access Internet resources.[3]

The Tor software among these is the most popular with more than 2 million daily users.[4] The Tor network (a number of computers running the server application) is different from the Tor browser (which is an application that enables users to access the internet by concealing their identity). Tor uses the onion routing method which is a layered technology that routes traffic through the established layers to conceal the identities of the users, thus making the Tor browser slower than any normal connection.

This technology was developed by the U.S. Naval Research lab in the 1990s to carry out secure intelligence communications. The lab released the code for Tor under a free license in 2004, following which the 'Tor Project', a non-profit organisation, was founded by computer scientists Roger Dingledine, Nick Mathewson and five others advocating right to free speech, privacy and anonymity.[5]

Tor is also used for legitimate activities like secure and sensitive communications relating to medical ailments, helping law enforcement officials track down criminals, and in assisting cybersecurity professionals to conduct security testing on their own networks securely. It also provides access to social media websites in countries where they are banned. Using the Tor browser is not a criminal activity, although intelligence units keep a track of Tor downloads to predict any possible criminal activity.

[1] UlbrichtCriminalComplaint, Sealed Complaint 13 MAG 2328, September 27, 2014.
[2] Subhdeep Kaur and Sukhchandan Randhawa, "Dark Web: A Web of Crimes", Springer Science+Business Media, January 28, 2020.
[3] Ibid.
[4] Tor Metrics, April 19, 2021.
[5] Tor Project People, The Tor Project.

Whistle blowers like Edward Snowden also reportedly used TAILS software browser in order to communicate with journalists and leak classified information on U.S. mass surveillance programs.[6] Apart from Tor and similar software, dark web pages can also be accessed by using bridges such as Tor2web from a standard browser without downloading and installing the Tor software.[7]

Exploitation of the Dark Web

Criminal and terrorist activities

The anonymous chat rooms and communication services on the dark web make it an ideal platform for planning and coordinating dangerous criminal and terrorist activities. Dark web, for instance, hosts hackers and hitmen for hire. In April 2021, an Italian man was arrested for allegedly hiring a hitman on the dark web to attack his ex-girlfriend by throwing acid on her and forcing her into a wheelchair. Europol issued a press release stating that the Italian national paid 10,000 Euros to hire the hitman from an "internet assassination website" hosted on a Tor network.[8]

Earlier in 2020, a website called Azerbaijani Eagles offered commissioning of a murder for $5,000 providing options such as beating, death by torture, etc. Experts and law enforcers have stated that these websites are mostly scams but people hiring hitmen through such websites are real.[9] A nurse from Illinois was sentenced to 12 years in prison after she spent $12,000 in Bitcoins on a dark web company to hire a hitman to get the wife of her boyfriend killed.[10]

Terrorist organisations like the ISIS extensively used the dark web to carry out their nefarious activities like spreading propaganda, recruiting and radicalising, or raising funds more secretly. ISIS's media outlet, Al-Hayat Media Center, posted a link on their forum explaining details of how to access their website on the dark web. It also shared the same message on their Telegram channel that had links to a Tor service with an ".onion" address.[11]

In March 2021, the World Health Organisation (WHO) warned people against the sale of counterfeit Covid-19 vaccines, particularly on the dark web. Fraud services like fake vaccines have the potential to exploit the huge unmet global demand for Covid-19 vaccines criminally. Therefore, the WHO urged people to only rely upon government-run vaccination programmes.[12] Nefarious activities like money

[6] Klint Finley, "Out in the Open: Inside the Operating System Edward Snowden Used to Evade the NSA", *Wired*, April 14, 2014.
[7] Tor2web, browse the Tor onion services, Tor2web.
[8] Dark Web Hitman Identified Through Crypto-Analysis, Europol, April 7, 2021.
[9] Nathaniel Popper, "Can you really hire hitman online?" The New York Times, March 4, 2020.
[10] Former Des Plaines Woman Pleads Guilty In Murder For Hire Plot, Press Release, August 27, 2019.
[11] Gabriel Weimann, "Terrorist Migration to the Dark Web", JSTOR, June 2016
[12] WHO warns against sale of counterfeit Covid-19 vaccines on dark web, Business Standard, March 27, 2021.

laundering, drug trafficking, terrorism financing, ransomware, cryptocurrencies on the dark web are all strongly linked to one another.

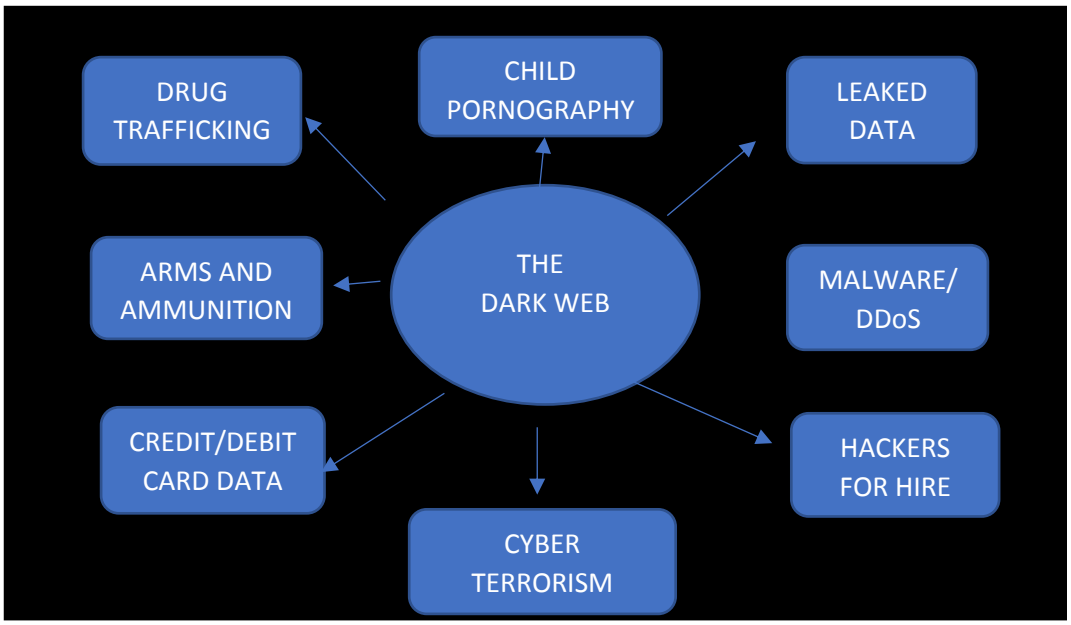

Figure II: Exploitation of the Dark Web (proportion not to scale)

Instances of Data breaches in India

- Juspay data was breached in January 2021 wherein data of around 10 crore cardholders was sold on the dark web for an undisclosed amount. It involved sensitive information of customers like email ids and mobile numbers and card transaction.[13]
- Mobikwik data that included sensitive information of 3.5 million users were put up for sale on the dark web in March 2021. The information contained the KYC details, addresses, phone numbers, Aadhar card details, etc. of Mobikwik users in India. The Reserve Bank of India (RBI) asked the digital wallet firm to get a forensic audit done with the help of CERT-IN-(Indian Computer Emergency Response Team)-empanelled auditor.[14]
- Domino's India data breach in April 2021 involved sensitive information of around 18 crore orders' released on the dark web for sale as a searchable database. Alon Gal, the CTO of Hudson Rock, a cybersecurity firm, posted on Twitter that this data was sold for around Rs 4.5 crore in bitcoins.[15]
- BigBasket data (from a November 2020 data breach confirmed by the company) was allegedly leaked on the dark web in April 2021. The data contained details of over 20 million customers such as their email addresses, names, birth dates, hashed passwords and phone numbers. The size of the

[13] Ashwin Manikandan and Anandi Chandrashekhar, "Juspay Data Leak fallout: RBI swings into action to curb cyberattacks", *The Economic Times*, January 6, 2021.
[14] RBI orders forensic audit of Mobikwik systems after data breach allegations, *Mint*, March 31, 2021.
[15] Jagmeet Singh, "Domino's India Data Allegedly Breached by Hacker Selling It on the Dark Web", *Gadgets360*, April 19, 2021.

database leaked was around 3.25 GB. A hacker group known as ShinyHunters, put the data on the dark web for download.[16]

Regulatory Challenges

The biggest hurdle that law enforcement agencies and policymakers face with respect to regulation of the dark web is its encryption technique and anonymity. The environment of the dark web is completely anonymous, therefore making it difficult to attain sufficient information that could help combat cybercrimes and track criminals who exploit this space. As of now, there is no universal definition of cyber terrorism which makes it even more difficult for the intelligence agencies to decide the jurisdiction of the crime. The dangers of cyberspace are multi-dimensional and most of the threats are linked to one another.

Apart from the strong encryption techniques, most financial transactions on the dark web are performed in cryptocurrencies which provide further anonymity. The underlying technology of cryptocurrency, called the block chain, is essentially a digital ledger of transactions distributed across the network in which the blocks are cryptographically secured. It records information in a way that makes it difficult or impossible to modify or hack the system. The Darkside group of hackers responsible for the Colonial Pipeline ransomware attack, for instance, demanded ransomware amount of $5 million in cryptocurrency.[17] The REvil ransomware gang that targeted IT firm Kaseya and hundreds of other businesses worldwide in early July 2021 had also demanded ransom to be paid in cryptocurrency bitcoin.[18]

Bitcoin transactions have facilitated all kinds of illegitimate activities by cyber criminals and terrorists on the dark web. Use of cryptocurrencies for financing illegitimate activities on the dark web has made it extremely difficult for law enforcement agencies to follow the trail of money in order to gather evidence of a crime. Regulation of cryptocurrencies is possible only with respect to their legitimate use while a large portion of them can still be used for illegitimate purposes.

Monitoring cryptocurrency chain would require a well-defined categorisation of centralised and decentralised roles in financial transactions. Block chain, the underlying technology of cryptocurrencies, is still an emerging technology with a demand of more expertise in the field. Another challenge with respect to the dark web is that most dark web sites are active for a period of 200 days to a maximum period of 300 days. Some also last for a period of less than two months, making it even more tedious to track them.[19]

---

[16] Sudhanshu Singh, "Big Basket data breach: email IDs, phone numbers, home addresses of two crore Indians allegedly leaked on the web", *Business Insider*, April 26, 2021.
[17] William Turton, Michael Riley, and Jennifer Jacobs, "Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom", *Bloomberg*, May 14, 2021.
[18] Gang behind huge cyber-attack demands $70m in Bitcoin, *BBC*, July 5, 2021.
[19] The Dark Web: Myths, Mysteries and Misconceptions, Kaspersky, 2018

Successful Takedowns of Dark Web Sites

- As part of the Operation Paris (OpParis) campaign launched by the amorphous hacker collective, Anonymous, after the 2015 Paris attacks, hundreds of websites on the dark web associated with ISIS were taken down.[20]
- A Russian citizen named Kirill Victorovich Firsov was imprisoned for 30 months for his role in selling stolen credit card information and other data on the dark web that was in turn used to execute other criminal activities, as per a US Department of Justice (DoJ) release on May 24 2021.[21] Firsov was the administrator of a website that provided stolen personal information and other services.
- On June 11, 2021, the Tor-based market on the Dark Web called 'Slilpp' was shut down.[22] Slilpp was responsible for dealing in stolen credentials on the dark web and offered its users access to as many as 1,400 websites, 80 million accounts and services worldwide.
- A Ukrainian national (extradited to the US in June 2019 after arrest in Spain a year earlier) linked to the cybercrime group FIN7 was sentenced to seven years imprisonment and ordered to pay $2.5 million.[23] The group is responsible for stealing more than $1 billion from US citizens and organisations and selling them on the dark web.
- Ukranian police announced on June 28, 2021 that advanced data analytics used by the Binance cryptocurrency exchange helped track down a group of money launderers called FANCYCAT, involved with numerous criminal scams, including laundering money for dark web operators and also the 'Clop ransomware' scam.[24]
- A suspect involved in a series of cyber-frauds related to banks, telecom and multinational corporations was arrested by the Moroccan police on July 6, 2021, as part of Operation Lyrebird.[25] The suspect attacked thousands of victims through phishing, credit card fraud and launched malware campaigns against the corporate networks of French-speaking communications companies.
- Data sites on the dark web associated with REvil gang became unreachable on July 13, 2021. It was speculated that this could be the result of prohibitions imposed by law enforcement agencies or the gang could have

[20] Abby Ohlheiser, "What you need to know about Anonymous's 'war' on the Islamic State", *The Washington Post*, November 17, 2015.
[21] Russian Hacker Sentenced to 30 Months for Running a Website Selling Stolen, Counterfeit and Hacked Accounts, Department of Justice, U.S. Attorney's Office, Southern District of California, May 24, 2021.
[22] Slilpp Marketplace Disrupted in International Cyber Operation, Department of Justice, Office of Public Affairs, June 10, 2021.
[23] High-Level Member of Hacking Group Sentenced to Prison for Scheme that Compromised Tens of Millions of Debit and Credit Cards, Department of Justice, Office of Public Affairs, June 24, 2021.
[24] John Leyden, "Binance reveals how data analytics led to ransomware-linked money laundering bust', PortSwigger, June 28, 2021.
[25] Moroccan police arrest suspected cybercriminal after INTERPOL probe, Interpol, July 6, 2021.

disbanded by itself. The REvil gang is the cybercriminal group that took credit for the massive international ransomware outbreak that happened on July 2 on the Kaseya IT management software.[26]

Way Forward

The dark web is a complicated environment providing both benefits and disadvantages based on whether it is utilised or exploited by the user. Darknet helps to protect the right to freedom of information and online privacy of individuals and is therefore often used by journalists and other activists across the world to carry out communication in a safe and secure manner. At the same time, it is misused by miscreants giving rise to a series of crimes.

A nuanced approach, therefore, by the law enforcement agencies is required to both protect the benefits of this space as well as eliminate the illegal activities thriving in it. A close cooperation between public and private organisations can help in dealing with the new and emerging technological challenges of the dark web, by providing solutions such as new encrypting tools, etc. Law enforcement agencies should actively take the help of sophisticated technologies like artificial intelligence, machine learning, among others.

With respect to the repeated data breach incidents, a specified regulation on the amount of personal data collection by various companies and their automatic deletion after a stipulated time period could increase the efficiency of cyber systems and secure the data and prevent such incidents in the future to a large extent. The challenges of the trans-border nature of the dark web can be dealt by sharing intelligence data across different sectors, agencies and organisations. International co-operation in the form of multilateral exchanges through seminars, forums and joint capacity building exercises is highly beneficial in this regard.

[26] Cameron Camp and Aryeh Goretsky, "Kaseya supply-chain attack: What we know so far", *WeLiveSecurity*, July 3, 2021; Latest ransomware attack appears to hit hundreds of American businesses, *The Guardian*, July 3, 2021.

About the Authors

Debopama Bhattacharya is Project Assistant at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
contact.idsa@nic.in www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses