INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

IJARIIT

ISSN: 2454-132X
Impact factor: 6.078
(Volume 6, Issue 3)
Available online at: www.ijariit.com

The freedom of dark web: A digital scrutiny of terrorism on the dark web

Shivam Pandey
shivam22pandey22@gmail.com
Dronacharya College of Engineering, Gurugram, Haryana

"How do you deter offenders from using such facilities while also respecting the privacy of lawful citizens?

The response to that is easy, you don't.

You can't limit anything which is supposed to be unrestrictive because it's very nature. That is the anonymity problem. Anyone can do something or say something so we have no choice but to take the good with the bad. Even if law enforcement agencies were able to completely shut down the entire network they would not. Because the US administration needs TOR just as much as anyone else."

"The United States government can't simply run an anonymity system for everybody and then use it themselves only because then every time a connection came from it people would say "Oh, it's another CIA agent looking at my website!" if those are the only people using this network. So, you need to have other people using the network so that they can blend together."

- Roger Dingledine, Co-founder and Director, the Tor Project

ABSTRACT

The terms Deep Web, Deep Net, Invisible Web, or Dark Web allude to the substance on the World Wide Web that isn't recorded by standard web indexes. One can depict the Internet as made out of layers: the "upper" layer, or the Surface Web, can without much of a stretch be gotten to by standard quests. Be that as it may, "further" layers, the substance of the Deep Web, have not been filed by customary web crawlers, for example, Google. Michael K. Bergman who composed the fundamental paper on the Deep Web, contrasted looking through the Internet with hauling a net over the outside of the sea: an extraordinary arrangement might be trapped in the net, however there is an abundance of data that is more profound and thusly missed [1]. Truth be told, a large portion of the Web's data is covered far down on locales, and standard web indexes can't get to it.

Keywords— *Deep web, Dark Web, Internet, Terrorism on the Internet*

1. INTRODUCTION

During the beginning of the Internet, online data was effortlessly listed and there was no trouble for clients to get to it without any problem. Anyway, as the utilization of the Internet extended, ordinary web crawlers had the option to recover static pages yet demonstrated wasteful for dynamic pages. A static page is one connected to different pages on the Internet while a unique page is connected to a specific site page and can be recovered uniquely through focused questions or projects. This made a hole between the static and dynamic site pages on the web and the gap began to enlarge as time passed. In this way, as of now in 1994, Jill Ellsworth authored the saying 'undetectable web' to allude to data that remaining parts 'imperceptible' to questions of regular web search tools utilized at that time.

In 2001, Bergman instituted another term, 'Profound Web', regularly characterized as instructive substance on the Internet which seems to be: (an) out of reach through direct questions by ordinary web indexes; (b) got to just through focused inquiries or catchphrases; (c) either not filed or incapable to be ordered by customary web crawlers; (d) ensured by security systems like login IDs, passwords, participation enlistments and codes.[2]

2. THE DEEP DARK WEB

It is practically difficult to gauge the size of the profound web in light of the fact that most of its data is covered up or blocked. While some early gauges put the size of the Deep Web at 400-500 times that of the surface web,[3] "the changing dynamic of how data is gotten to and introduced implies that the Deep Web is developing exponentially and at a rate that resists quantification."[4] According to an investigation distributed in Nature, Google records close to 16 percent of the surface Web and misses the entirety of the Deep Web. Some random inquiry turns up simply 0.03 percent of the data that exists on the web. As RAND Corporation master Lilian Ablon as you present this individual and utilize this forename, so should you do as such with Bergman prior noted, “Everything over the water is the thing that we would consider the surface web that can be recorded through Google or you can discover through a web index. Yet, underneath the water that tremendous chunk of ice is 80% greater than what is over the water, that is the profound web, that is the piece of the web that is not recorded. There is such a large amount of the web that we can’t simply Google for; it’s dim to us, it’s dim to Google.” [5] Somewhat redundant since icy mass relationship was at that point utilized.

The most profound layers of the Deep Web, a fragment known as the Dark Web, contain content that has been deliberately disguised. The ‘Dark Web’ can be characterized as the bit of the profound web which contains commonly unlawful and hostile to social data and must be gotten to through specific programs. Hence, for instance, the Dark Web is utilized for material, for example, youngster erotic entertainment, unapproved holes of delicate data, tax evasion, copyright encroachment, charge card extortion, fraud, unlawful deals of weapons, and so forth. A recent report by University of Portsmouth software engineering scientist Gareth Owen introduced the consequences of a six-month test of the web’s dark layers. Owen found that the most regularly mentioned sorts of substance on these dark web stages were kid erotic entertainment followed by illegal businesses, while the individual locales with the most elevated traffic were devoted to botnet operations.[6] In 2014, writer Jamie Bartlett in his book The Dark Net depicts a scope of underground and rising sub-societies, including internet based life racists, cam young ladies, self-hurt networks, sedate markets, crypto-revolutionaries and transhumanists. [7] As of late, the dark web has been moving towards progressively mysterious areas because of the crackdown of government organizations on it.

The Dark Web can be visited by any web client; however it is hard to work out who is behind the locales and the destinations are not found by utilizing web crawlers. People can get to the Dark Web by utilizing exceptional programming, for example, Tor (short for The Onion Router) or I2P (Invisible Internet Project). Tor was at first made by the U.S. Maritime Research Laboratory as a device for secretly conveying on the web.

Tor depends upon a system of volunteer PCs to course clients ‘web traffic through a progression of other clients’ PCs with the goal that the traffic can’t be followed to the first client. A few designers have made instruments, for example, Tor2web, that permit people to get to Tor facilitated content without downloading and introducing the Tor programming, in spite of the fact that getting to the Dark Web through these methods doesn’t anonymize movement. Not all Dark Web destinations use Tor, however the guideline continues as before. The guest needs to utilize a similar encryption device as the site and - critically - realize where to discover the site, so as to type in the URL and visit. Once on the Dark Web, clients regularly explore it through indexes, for example, the “Covered up Wiki,” which sorts out destinations by classification, like Wikipedia.

In the Dark Web, people may convey through methods, for example, secure email, web visits, or individual informing facilitated on Tor.[8] The Dark Web stood out as truly newsworthy in 2015 with the hacking of the Ashley Madison database. Ashley Madison is a web-based dating administration for wedded individuals, under the motto “Life is short. Have an unsanctioned romance.” The organization got consideration on July 15, 2015, after programmers broke into its database, taking the individual information of somewhere in the range of 37 million clients. Afterward, the gathering dumped 9.7 GB worth of information onto the Dark Web including the messages, names, street numbers, sexual dreams and Visa data of the customers. The Ashley Madison hack isn’t the first occasion when that the Dark Web has made it into the news. Maybe the most prominent story is the situation of the online underground market Silk Road, the illicit medication commercial center which worked on the Dark Web for a long time before the FBI shut down this site in 2013 and captured webpage organizer Ross Ulbricht. He was therefore condemned to life in jail. The Dark Web has been related with the scandalous WikiLeaks, the characterized media website, just as bitcoins, said to be the money of the Dark Web. Over its two-year run at the top, Silk Road made over US$1.2 Billion in bitcoin.[9]

3. TERRORIST MIGRATION ON DARK WEB

Fear mongers have been dynamic on different online stages since the late 1990s. [10] Incomprehensibly, the exceptionally decentralized system of correspondence that the U.S. knowledge and resistance organizations made out of dread of the Soviet Union presently serves the interests of the best enemy of the West’s security administrations since the finish of the Cold War: worldwide fear. Fear based oppressor associations and their supporters keep up a huge number of sites and interpersonal interaction stages, abusing the unregulated, mysterious, and effectively available nature of the Internet to pass on a variety of messages to an assortment of focused crowds. Various examinations have distinguished no less than eight unique manners by which psychological militants are utilizing the Internet to propel their motivation. These range from mental fighting and purposeful publicity to profoundly instrumental uses, for example, gathering pledges, enlistment, information mining, and coordination of activities.

In any case, the surface web was found to be unreasonably hazardous for secrecy looking for psychological militants: they could be checked, followed and found. The Dark Web and psychological warfare appear to be made for one another – fear mongers need an unknown, concealed system that is promptly accessible yet for the most part out of reach and imperceptible. The Dark Web is extremely gainful for fear-based oppressor gatherings: While they may lose a wide crowd that is accessible on the Surface Web, they can abuse the haziness of the Dark Web to encourage their objectives. A considerable lot of the fear monger sites and web-based social networking on the Surface Web are checked by counter-psychological oppression offices and are frequently closed down or hacked. Interestingly, on the Dark Web, decentralized and mysterious systems help in dodging capture and the conclusion of these fear-based oppressor stages. Along these lines, the Dark Web resembles a ‘treasure trove’ which gives psychological oppressors preferably mysterious correspondence, empowering the sharing of information and directions, posting instructional booklets, online enlistment, arranging and coordination of actions.[11] According to the London-based Quilliam Foundation, this pattern ought not shock anybody: “Endeavours to square fanatic material online will consistently come up short”. The position paper by Quiliam about the British government’s endeavors to square radical action on the web, expresses: “The psychological oppressor material returns on the Internet as fast as it is ousted and this arrangement dangers driving aficionados on to the “dark web” where they are much harder to track.”[12] Moreover, “Islamist gatherings what's more, talk rooms in English and French are still broadly accessible, however an enormous part of progressively fanatic Islamic talk currently happens inside the dark web".[13]

Before, fear mongers rushed to embrace and apply each developing on the web stage. In the late 1990s, it was the utilization of sites. At that point they included the more intelligent gatherings, chatrooms and the video-sharing and picture-sharing foundation of YouTube, Instagram and such. The presentation and quick spread of online networking, for example, Twitter or Facebook were immediately noted by various psychological oppressor bunches who began posting messages, recordings, manuals and purposeful publicity material on the famous web-based life. Along these lines, the thought of the Dark Web with its novel focal points of obscurity, mystery and communicator-controlled access is unquestionably more than engaging for them. In July 2015, The FBI reported that Islamic State, or ISIS (or ISIL), is utilizing the Dark Web to move fear assaults over the globe. FBI Director James Comey cautioned that ISIS is utilizing new types of correspondence and encryption, and his administration's present legitimate and mechanical capacities may not be adequate to keep up. "ISIL's exercises on the Surface Web are currently being checked intently, and the choice by various governments to bring down or channel fanatic substance has constrained the jihadists to search for new online places of refuge," Beatrice Berton writes in another report on ISIS' utilization of the dark net. "The Dark Web is an ideal elective as it is blocked off to most however traversable for the started not many – and it is totally mysterious," Berton noted.[14] Tor program email administrations, for example, Torbox and Sigaint are mainstream among the Jihadists since they shroud both their personalities and their area.

In March 2015, Jihadists posted online a digital book titled "How to Survive in the West: A Mujahid Guide." This is the most recent in a progression of digital books gathered by supporters of and selection representatives for the Islamic State. This digital book's part titles include: "Concealing the Extremist Identity", "Procuring Money", "Web Privacy", "Preparing", "Bomb-Making", "Moving Weapons", and "What Happens When You Are Spied On And Get Raided". One of the methods examined in the manual is the utilization of TOR while scanning for and inquiring about jihadi points on the web. [15] On June 11, 2015, Virginia occupant Ali Shukri Amin, who had been captured on March 4, 2015, conceded in court that he had worked a few productive star ISIS accounts. On his destinations, he gave protection data to his devotees, and alluded to TOR over and over. For instance, when asked on July 13, 2014 "Why are individuals getting some information about how to utilize TOR?" he answered, "To be unknown on the web, they don't need the administration seeing what they do and getting them in a difficult situation." He additionally prompted his crowd "Don't offer these expressions inside US except if you're working through TOR and Ghost VPN."

Terrorists are continually searching for more current and better applications and stages so as to keep up their online nearness on however many outlets as would be prudent. Our multi year-long research venture on observing fear monger utilization of online stages has yielded a database containing all psychological oppressor gatherings' utilization of sites, visit rooms, web based life, etc.[16] An examination of the database uncovers new patterns in psychological militant utilization of the Web, including, the most current one – the utilization of the Dark Web.

4. THE WIKI TERROR - GOES DARKER

For more than two decades, psychological militants have utilized the Internet to give data to individual fear based oppressors, including maps, photos, bearings, codes and specialized subtleties of how to utilize explosives, harms, weapons, synthetics, etc.[17] The Surface Web is home to many locales that give online manuals on the best way to construct compound and hazardous weapons. A significant number of these locales post the Fear monger's Handbook and The Anarchist Cookbook, two notable manuals that offer nitty gritty directions of how to develop a wide scope of bombs. Another manual, The Mujahadeen Poisons Handbook, composed by Abdel-Aziz in 1996 and 'distributed' on the official Hamas site, subtleties in twenty-three pages how to get ready different natively constructed harms, noxious gases, and other savage materials for use in psychological militant assaults. Notwithstanding propelling their own sites, fear based oppressors can outfit the intelligent capacities of online stages utilizing chatrooms, moment delivery people, sites, video sharing-sites, and web based life, for example, Facebook, MySpace, Twitter, Instagram and YouTube.[18] These famous stages have been likewise utilized for web based preparing and intuitive guidance.

The significance of these online libraries of psychological oppressor down to earth know-how driven jihadists to recommend a Wikipedia for fear mongers. As per a SITE report, in January 2014, a jihadist transferred on Wikipedia Arabic material for bunches incorporating al-Qaeda in the Islamic Maghreb (AQIM) and the Haqqani Network, and people, for example, Attiya Allah and Abu Musab al-Suri. A similar jihadist even proposed that jihadists make a "Jihadwiki." [19] indeed, the collecting psychological oppressor postings of directions, messages, addresses, manuals, and so forth – made in certainty a "Wikipedia of Terror". Be that as it may, this database is on a superficial level web, open additionally to counter-fear mongering offices, police and security administrations. Not exclusively would they be able to screen the material posted, yet additionally endeavor to recognize the surfers downloading material from these destinations and even "poison the well" by changing and altering the substance. This is the point at which the Dark Web turned into the new, elective Wiki-Terror.

The transition to the Dark Web requires fundamental information on the Tor programming and comparative projects, yet for the individuals who are curious about these strategies, there are online manuals. The Hackers Handbook, for instance, presents the accompanying presentation. This instructional exercise will assist you with getting to the Deep Web. What is the Deep Web? It's basically the entirety of the sites you can't discover on the web through a typical program or web search tool. It's all the unlawful things that aren't permitted on the web, for example, street pharmacist indexes, bootleg market exchanges, programmers, assassins, pedophiles, and whatever else you wouldn't hope to discover typically. It is strongly suggested you peruse the Deep Web with firewalls on, and your webcam detached. Be careful about what you download, and peruse at your own risk![20]

Perusing on the Dark Web isn't as straightforward as on the Surface Web, yet psychological oppressors and their devotees are getting a charge out of the free administrations of the Hidden Wiki. The Hidden Wiki is the name of a few control safe Tor concealed administrations. The primary page fills in as a registry of connections to different destinations. As a help, The Hidden Wiki works through the Onion pseudo top-level area which can be gotten to just by utilizing Tor or a Tor entryway. Its primary page gives connects to other concealed administrations, including connections to illegal tax avoidance, contract murdering, digital assaults for recruit, medications, and bomb making. The remainder of the wiki is basically uncensored too and furthermore offers connects to destinations facilitating kid sex entertainment and misuse pictures. The first Hidden Wiki was changed commonly and copied to numerous mirrors destinations since it was regularly hacked.

Psychological oppressors post on the Dark Web material specifying activities and tasks. For instance, in July 2014 five sites of different Austria-based organizations have been ruined by the master AL-Qaeda hacking bunch "Al-Qaeda Electronic". The gathering's media arm, "al-Maarek Media," posted the case for the assault on its web-based life accounts and for its on the Deep Web. The posting incorporated the URLs of the focused-on sites and reflections of the ruinations. The content in the ruined site pages were all indistinguishable, and have been recently utilized by "Al-Qaeda Electronic" in assaults on various French, British, Norwegian, Russian, and Vietnamese sites. Afterward, in August 2015, a Turkish language Dark Web gathering "Turkish DarkWeb" circled manuals for building explosives and weapons and talked about the gadgets' productivity, sway, and proposed use.

On August 27, 2014, Al-Aan TV detailed that a PC having a place with a Tunisian individual from ISIS was caught by "moderate radicals in Syria." According to the report, the PC contained, notwithstanding numerous jihadi talks, a huge number of jihadi records that its proprietor had distributed, for the most part on the Dark Web. One of them was an itemized 19-page record about creation organic weapons and about spreading "substance or natural specialists in an approach to affect the greatest number of individuals." A British report, entitled "ISIS Encyclopaedia of Terror: The privileged insights behind Islamic State's 'data Jihad' on the West" uncovered that a full-scale psychological oppression 'how-to' control, assembled by ISIS, is covered up on the Dark Web. It closes: "English ISIS initiates are instructed how utilize the 'dark web' to speak with a worldwide system of terrorists".[21]

5. FUNDING AND BUYING IN THE DARK WEB

At the point when programming designer Satoshi Nakamoto presented bitcoin in 2008 as an elective money autonomous of a focal authority,[22] the subsidizing of universal psychological militant associations was positively not part of the first idea. Be that as it may, that is actually what is at present occurring. Utilizing the Dark Web, fear mongers can raise assets for their association and their motivation by tolerating bitcoin gifts which they, thus, use for buying weapons in the Dark Web bootleg trades. For example, "Store the Islamic Struggle suddenly and completely" is a website page in the Deep Web which welcomes gifts for Jihad through bitcoin exchanges to a specific bitcoin address. A PDF archive posted online under the pen name Amreeki Witness titled Bitcoin wa Sadaqat alJihad which means "Bitcoin and the Charity of Violent Physical Struggle" is actually a guide for utilizing the Dark Web for online cryptic exchange of cash.[23] The report makes unequivocal reference to dark markets like Silk Road and other Dark Net markets clarifying how it is conceivable to purchase weapons for the Mujahideen utilizing Bitcoin and the Dark Wallet application to "send a large number of dollars of Bitcoin in a split second from the United States, United Kingdom, South Africa, Ghana, Malaysia, Sri Lanka, or any place else right to the pockets of the Mujahideen". An ongoing US Treasury Department study reports that bitcoin might be utilized to

support psychological oppression: The National Terrorist Financing Risk Assessment, distributed twelfth June, 2015, remembers virtual monetary forms for a rundown of "potential developing" hazards as an apparatus for subsidizing fear mongering, expressing that bitcoin "might be helpless against maltreatment by fear-based oppressor lenders".[24]

In reality, there is developing proof of psychological oppressor utilization of Dark Web channels for raising money. The Combating Terrorism Technical Support Office (CTTSO), a division of the US Department of defence that recognizes and creates counterterrorism capacities and explores sporadic fighting and advancing dangers has just noticed the developing danger. A CTTSO notice from January 2, 2014 cautioned that "The presentation of virtual money will probably shape danger account by expanding the obscurity, value-based speed, and in general efficiencies of psychological oppressor assaults".[25] In January 2015, S2T, a Singapore-based digital insight organization revealed solid proof that a dread cell, indicating to be identified with Islamic State and working in the Americas, is requesting Bitcoins as a major aspect of its raising money efforts.[26] The online message from the gathering's pledge drive, a man later recognized distinctly as Abu-Mustafa pronounced:

> One can't send a bank move to a mujahid or suspected mujahid without the kafir governments managing today quickly staying alert. A proposed answer for this is something known as Bitcoin. To set up an absolutely unknown gift framework that could send a great many dollars of Bitcoin in a split-second right to the pockets of the mujahideen, almost no future done.

As per Ido Wulkan, a senior web-knowledge investigator at S2T who has uncovered this ISIS' movement, "Because of the expanding endeavors of online life sites to close ISIS-related records it was evaluated that worldwide jihad activists would look for shelter in obscurity web".[27] Jimmy Gurule, the previous undersecretary of the Treasury Department, noticed that ISIS contrasts from other fear based oppressor bunches in that it is a self-financing association by methods for cash got from the offer of oil on the bootleg market. ISIS additionally utilizes payment and coercion to help its fear monger exercises. These assets from bootleg market oil deals, payoff and coercion must be washed all together for ISIS supporters to stay unknown and free from apprehension.[28]

The Dark Web additionally furnishes psychological oppressors with a perfect commercial center for buying weapons and explosives. EuroGuns, for instance, is an online dark stage which handles deals of different weapons. For instance, AK-47s – the sort of ambush rifle utilized by the Kouachi siblings in the Charlie Hebdo assaults – are sold for $550 each on EuroArms. In addition, a few messages, for example, the Terrorist's Handbook and the Explosives Guide can be bought on AlphaBay. Other Dark Web administrations for psychological militants incorporate the gracefully of phony archives and travel papers: Fake Documents Service, for example, offers customers 'unique great phony international IDs, driver's licenses, ID cards, stamps and other items' for use in the UK, US, Australia and Belgium, among other countries.[29]

In April 2015 a 16-year-old kid who requested a fatal poison from the Dark Web was condemned in Manchester, England. This followed an examination by the North West Counter Terrorism Unit (NWCTU), who had been educated that the adolescent was endeavoring to acquire an exceptionally poisonous toxic substance called Abrin, which is viewed as multiple times more harmful than ricin.

6. COMMUNICATING IN THE DARK

Psychological oppressors utilize online stages to convey – among themselves, with their devotees, with the broad communications and the general population on the loose. Nonetheless, their correspondences may lead, as it did, to distinguishing proof and capture. In this manner, they see the Dark Web and other dark channels as the most secure outlets. As of late, ISIS and other jihadist bunches have utilized new online applications which permit clients to communicate their messages to a boundless number of individuals through encoded cell phone applications, for example, Telegram.

ISIS has not had an official nearness on Twitter since July 2014, when its last records were closed down. In spite of the weight on its media activity, ISIS has consistently demonstrated exceptionally flexible and versatile: it began exploring different avenues regarding a progression of less wellknown web based life stages, for example, the protection centered Diaspora just as VKontakte, Russia’s biggest interpersonal organization, whose prime supporters the Durov siblings proceeded to set up Telegram in 2013. Telegram is an application for sending content and mixed media messages on Android, iOS, and Windows gadgets. Telegram is so sure of its security that it twice offered a $300,000 prize to the main individual who could break its encryption. Worked by autonomous engineers, the Berlin-based Telegram Messenger application was first propelled for iPhone in August 2013 and for Android two months after the fact.

On 26 September 2015, only four days after Telegram declared the dispatch of its new “Stations” device, ISIS media agents on Twitter began promoting the gathering’s own station named Nashir, which deciphers as “Wholesaler” in English. Jihadists were pulled in by Telegram’s gloat to give a “mystery visit” office, which vigorously scrambles messages client to user with a one of a kind key to dodge interference by programmers or government offices. Al-Qaeda’s Yemen branch (AQAP) propelled its own Telegram “station” on 25 September 2015 and the Libyan Ansar al-Shari’ah group made its channel the next day. On September 26, 2015, a Twitter account announced that Al-Qaeda in the Arabian Peninsula (AQAP) presently has a station on the safe interchanges application Telegram. The channel, as indicated by the tweet, will be utilized to spread the gathering’s news and discharges.

Jihadists enlivened by ISIS, including a British young person indicted in October 2015, have utilized the application’s safe scrambled informing to lead the arranging of assault. The 14-year-old spoke with individual Islamic State supporters over Telegram and traded messages about a plot to assault the Anzac Day march in Melbourne, Australia. Persuaded his messages would stay mystery from the security administrations, he examined the coordination of the abomination and the conceivable murdering strategies. It was uniquely by some coincidence, when the police captured the student over another issue and held onto his telephone, that the Melbourne fear plot came to light.[30] When gotten some information about it, Telegram’s CEO Pavel Durov surrendered that ISIS in reality utilizes Telegram to guarantee the security of its correspondences, yet included: “I imagine that protection, at last, and our privilege for security is a higher priority than our dread of awful things occurring, as terrorism”.[31]

7. CONCLUSIONS

In spite of the fact that the Internet has been accessible to people in general since the 1990s, the Dark Web has just risen as of late. The clandestine idea of this piece of the web joined with an absence of valuable strategy intended for Dark Web information assortment and investigation has constrained the ability to study and battle Dark Web psychological warfare. At the point when IBM’s security division distributed its security dangers report for the second from last quarter of 2015, it featured the danger of digital assaults originating from the Dark Web, utilizing TOR systems. Giving clear proof which shows that the Dark Web has transformed into a significant stage for worldwide fear mongering and crimes is totally vital so as to give the catalyst to the vital apparatuses to be created to counter it. To be sure, there has been expanded enthusiasm for creating strategies material to this end. As of now in 2008, a philosophy for examining the Dark Web was proposed and even tested.[32] That review consolidated different information and Web mining advances to deliver the methods for both extensive Dark Web information assortment and examination.

The University of Arizona-Dark Web venture is a drawn out logical research program that intends to contemplate and comprehend the wonder of worldwide fear mongering by means of a computational, information driven approach.[33] Over the long time this undertaking created one of the world’s most broad files of fanatic sites, discussions, sight and sound records (pictures and recordings) just as online networking postings.

In any case, with the developing refinement of psychological militant’s utilization of the Dark Web, there is a need to grow new techniques and measures for following and dissecting fear monger utilization of the Dark Web. This is the new and testing undertaking of counter-psychological oppression organizations. Along these lines, for instance, DARPA, the defence Advanced Research Projects Agency, accepts the appropriate response can be found in MEMEX, a product that takes into account better inventorying of Deep Web destinations.

In mid-2014, DARPA discharged an announcement on their site sketching out the starter subtleties of the “MEMEX program”, which focuses on the improvement of new inquiry innovations defeating a few confinements of content-based pursuits. DARPA trusts that the MEMEX innovation created through this examination will empower web indexes to enter and mine the Deep and the Dark Web. Imagined as a simple PC to enhance human memory, the MEMEX (a blend of “memory” and “file”) would look around the Dark Web and furthermore tune its information to explicit spaces of intrigue.

As revealed in a 2015 Wired article, the hunt innovation being created by the MEMEX program “plans to sparkle a light on the dark web and uncover examples and connections in online information to help law authorization and others track unlawful activity”.[34] MEMEX was initially produced for checking human dealing on the Deep Web, yet similar standards can be applied to practically any illegal Deep Web action.

In 2014, an examination of the source code in one NSA program called XKeyscore, (uncovered by the Edward

Snowden's breaks), demonstrated that any client just endeavouring to download Tor was naturally fingerprinted, basically empowering the NSA to know the character of a large number of Tor clients. As per a report from the German news source Tagesschau, there are nine servers running TOR, including one at the MIT Computer Science and Artificial Intelligence Laboratory. All are under steady NSA observation. The NSA source code moreover uncovered a portion of the conduct which clients display can promptly be labeled or "fingerprinted" for alleged profound parcel examination, an examination concerning the substance of information bundles sent over the Internet, for example, messages, web searches and perusing history.[35]

In February 2015, an extraordinary report entitled "The Impact of the Dark Web on Internet Governance and Cyber Security", wrote by Michael Chertoff (previous US Homeland Security Secretary) and Tobby Simon (leader of the India-based Synergia Foundation), introduced a few proposals in regards to the Dark Web.[36] In their report, Chertoff and Simon state "so as to plan far reaching techniques and strategies for overseeing the Internet, it is imperative to think about bits of knowledge on its farthest reaches—the profound Web and, all the more significantly, the Dark Web."

They likewise note that "While the Dark Web may do not have the expansive intrigue that is accessible on a superficial level Web, the concealed biological system is helpful for promulgation, enrollment, financing and arranging, which identifies with our unique comprehension of the Dark Web as an unregulated space".

They prescribe the accompanying endeavors to screen the Dark Web:

- Mapping the concealed administrations catalog by conveying hubs in the DHT[37];
- Customer information checking by searching for associations with non-standard spaces;
- Social webpage checking to spot message trades containing new Dark Web areas;
- Hidden assistance checking of new locales for continuous or later investigation;
- Semantic examination to follow future criminal operations and pernicious on-screen characters;
- Marketplace profiling to accumulate data about merchants, clients and the sorts of good traded.

At last, there is another side to examining the Dark Web which likewise has favourable employments. While it can disguise fear-based oppressor interchanges and exercises, it likewise serves columnists, social liberties and majority rule government activists which may all be under danger of control or detainment. In nations like China, Iran and Saudi Arabia where the system is blue-pencilled or controlled, the Dark Web gives a significant outlet and stage. Hence, the disturbing invasion of Internet sagacious fear mongers to the "virtual caverns" of the Dark Web should trigger a worldwide quest for an answer, yet one that ought not impede genuine, legitimate opportunity of articulation.

8. REFERENCES

[1] Michael Bergman, "White Paper: The Deep Web: Surfacing Hidden Value", *Journal of Electronic Publishing*, vol. 7, issue 1, August 2001. Accessed October 13, 2015.

[2] Bergman, "White Paper: The Deep Web: Surfacing Hidden Value".

[3] Donald Barker and Melissa Barker. *Internet Research Illustrated*. Independence, KY: Cengage Learning, 2013, 4.

[4] Bright Planet, *Deep Web: A Primer*. Accessed October 15, 2015.

[5] Cited in CNN report "Pentagon hunts for ISIS on the secret Internet", May 12, 2015. Accessed October 10, 2015.

[6] Gareth Owen, "Tor: Hidden Services and Deanonymisation".Accessed September 20, 2015.

[7] Jamie Bartlett, *The Dark Net*. New York: Random House, 2014.

[8] Kristin Finklea, 2015. *Dark Web*, special report for Congressional Research Service, 2015.

[9] Evander, Smart. "The Dark Web: A Closer Look at one of the World's Largest Bitcoin Economies", *The Cointelegraph*, September 29, 2015.

[10] Gabriel Weimann, *Terror on the Internet*. Washington, DC: United States Institute of Peace, 2006; Gabriel Weimann: *Terrorism in Cyberspace: The Next Generation*. New York: Columbia University Press, 2015.

[11] Dilipraj, E. "Terror in the Deep and Dark Web", *Air Power Journal* 9, 120-140, 2014.

[12] Reported by *The Telegraph*, December 24, 2014. http://www. telegraph.co.uk/news/uknews/terrorism-in-the-uk/11300881/ Terrorist-materialreappears-online-as-quickly-as-it-is-banished-warns-thinktank.html

[13] Ghaffar Hussain and Erin Marie Saltman, "Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter it". A special report by Quilliam, May 2014. http://www. quilliamfoundation.org/wp/wpcontent/uploads/publications/free/ jihad-trending-quilliam

[14] Beatrice Berton, "The dark side of the web: ISIL's one-stop shop?". Report of the European Union Institute for Security Studies, June 2015.

[15] See MEMRI JTTM report "The 'Dark Web' And Jihad: A Preliminary Review Of Jihadis' Perspective On The Underside Of The World Wide Web", May 21, 2014. Accessed October 1, 2015.

[16] Reported in numerous publications, reports, books and papers. See for example, Weimann, *Terrorism in Cyberspace: The Next Generation*; Weimann, *Terror on the Internet*; Weimann, "The Psychology of Mass-mediated Terrorism," *American Behavioral Scientist* 52(1), 69-86, 2008; Gabriel Weimann and Abraham Kaplan, *Freedom and Terror: Reason and Unreason in Politics*, London: Routledge, 2011.

[17] Gabriel Weimann, "Virtual training camps: terrorists "use of the Internet." *Teaching terror: Strategic and tactical learning in the terrorist world*, 110-32, 2006.

[18] Jonathan Kennedy, and Gabriel Weimann. "The strength of weak terrorist ties." *Terrorism and Political Violence* 23.2, 201-212, 2011.

[19] Gabriel Weimann, "Terror on Facebook, Twitter, and YouTube." *Brown Journal of World Affairs*, 16, 45-54, 2009; Gabriel Weimann, "New Terrorism and New Media", Woodrow Wilson Center Research Report, May 2014.

[20] SITE Intelligence Group Report, "Jihadist Suggests Creating "Jihadwiki"", January 14, 2014.

[21] *Hackers Handbook*. September 1, 2015. http://www. hackershandbook.org/tutorials/deepweb

[22] Jasper Hamill, ISIS Encyclopedia of Terror: The secrets behind Islamic State's 'information Jihad' on the West revealed", Mirror Online, April 27, 2015.

[23] Joshua Davis, "The Crypto-Currency: Bitcoin and its mysterious inventor.". *The New Yorker*, October 10, 2011.

[24] http://www.scribd.com/doc/240561686/Bitcoin-wa-Sadaqat-alJihad

[25] The full report "National Terrorist Financing Risk Assessment 06-12-2015" can be found at: http://de.scribd.com/doc/268508302/ National-Terrorist-FinancingRisk-Assessment-06-12-2015

[26] Mark Rees, "Bitcoin for Bad Guys: Virtual Currency as an Anti-Terrorism Tool", *Bitcoin Magazine*, May 14, 2014.

[27] The Israeli Daily *Hareetz*. January 29, 2015. http://www.haaretz. com/news/middle-east/.premium-1.639542

[28] Ibid.

[29] Quoted in Josh Fischer, "The Bitcoin ISIS connection", *Virtual Currency Today*, February 6, 2015. Accessed October 14, 2015. http://www.virtualcurrencytoday.com/articles/the-bitcoinisisconnection/

[30] Beatrice Berton, "The dark side of the web: ISIL's one-stop shop?", *Alert*, 30, June 26, 2015.

[31] Stephen Wright, "Fears over secret text apps used by terrorists: Encrypted application exposed by the Mail was used by schoolboy terrorist", *Daily Mail*. July 23, 2015.

[32] John Devon, "Telegram reaches 12bn messages a day, acknowledges terrorists use the encrypted servic", *Neowin*, September 23, 2015.

[33] Hsinchun Chen, Wingyan Chung, Jialun Qin, Edna Reid, Marc Sageman and Gabriel Weimann, "Uncovering the Dark Web: A Case Study of Jihad on the Web", *Journal of the American Society for Information Science and Technology*, 59(8), 1347–1359, 2008.

[34] Hsinchun Chen, Dark Web : *exploring and data mining the dark side of the web*, New York: Springer, 2012.

[35] Kim Zetter, "Darpa Is Developing a Search Engine for the Dark Web". *Wired*, February 2, 2015.

[36] Patrick Tucker, "If You Do This, the NSA Will Spy on You", Defense One, July 7, 2014.

[37] The report is available online at: www.cigionline.org/sites/default/ files/gcig_paper_no6.pdf

[38] A Distributed Hash Table (DHT) is a type of a distributed decentralized network that provides contact information sharing, so people downloading the same file can discover each other. Tor and I2P both use DHT: Due to the distributed nature of the hidden domain resolution of the services, DHT nodes can be deployed to monitor requests from a given domain.