THE DARKNET: AN ENORMOUS BLACK BOX OF CYBERSPACE

Ms. Paridhi Saxena [*]
Mr. Sudhanshu Lata [**]

Introduction

Searching on the internet today can be compared to dragging a net across the surface of the ocean. There is a treasure of information that is deep, and therefore unnoticed. The reason is simple that basic search methodology and technology have not evolved significantly since the inception of the internet.[1]

Traditional search engines often crawls around the surface web pages only. In order to discover a page, it must be static and linked to other pages. Traditional search engines are not able to retrieve content from the deep web. Because these crawlers cannot probe beneath the surface the deep web has therefore been hidden from plain sight.

The 'Deep Web' refers to all the web pages that search engines cannot find. It is a part of the Internet that isn't necessarily malevolent, but is simply too large or incomprehensible to be indexed due to the limitations of crawling and indexing software (like Google/Yahoo etc). What makes the discovery of the deep web so noteworthy is the quality of the content found within. There are literally hundreds of billions of highly valuable documents hidden in searchable databases that cannot be retrieved by regular search engines.[2]

The Dark Web is a part of the non-indexed part of the Internet which is used by those who are purposely trying to control access because they have a great desire for privacy, or because what they're doing is illegal. It contains content that has been deliberately cloaked. The Dark Web may be accessed both for lawful purposes and to cover up criminal or other malicious

[*] Legal Research Assistant(Temporary), Government of Chhattisgarh, Law & Legislative Affairs Department, Raipur (C.G.)

[**] Student, 3rd year, B.A. LL.B. (H), Hidayatullah National law University, Raipur (C.G.).

[1] Michael k. Bergman, The Deep Web: Surfacing Hidden Value, Brightplanet - Deep Content available at http://brightplanet.com/wp-content/uploads/2012/03/12550176481-deepwebwhitepaper1.pdf (September 24, 2001)

[2] *Ibid*.

Published in Articles section of www.manupatra.com

activities. It is this exploitation of the Dark Web for illegal practices that has acquired the interest of officials and policy makers.[3]

A good example will be that of the Silk Road— named after the ancient trading route and one of the most notorious sites formerly located on the Dark Web. The Silk Road was an online global bazaar for illicit services and contraband, mainly drugs. Vendors of these illegal substances were located in more than 10 countries around the world, and contraband goods and services were provided to more than 1,00,000 buyers.[4] It has been estimated that the Silk Road generated about $1.2 billion in sales between January 2011 and September 2013, after which it was seized by the federal agents.[5]

By hiding the identities of those involved in dealings and often conducting business via Bitcoin[6], Darknet markets inherently represent illegality and regulatory evasion. Even where otherwise legitimate goods and services are involved, Darknet transactions often represent a range of national crimes, from tax evasion to failure to observe duties and other limitations on imports and exports.

Cyber Crime in the Darknet

Virtual crime is not any different than crime in the real world — it is just executed in a new medium: "'Virtual criminality' is basically the same as the terrestrial crime with which we are familiar. To be sure, some of the manifestations are new. But a great deal of crime committed with or against computers differs only in terms of the medium. While the technology of implementation, and particularly its efficiency, may be without precedent, the crime is fundamentally familiar. It is less a question of something

[3] The Internet, the DeepWeb, and the Dark Web available on https://danielmiessler.com/study/internet-deep-dark-web/ (accessed on 5 February 2016)

[4] Department of Justice, United States Attorney's Office, "Ross Ulbricht, a/k/a "Dread Pirate Roberts," sentenced in manhattan federal court to life in prison," press release may 29, 2015 available at https://www.fbi.gov/newyork/press-releases/2015/ross-ulbricht-aka-dread-pirate-roberts-sentenced-in-manhattan-federal-court-to-life-in-prison (accessed on 5 february 2016).

[5] Department of Justice, United States Attorney's Office, "Manhattan US. Attorney announces seizure of additional $28 million worth of bitcoins belonging to Ross William Ulbricht, alleged owner and operator of "Silk Road" website," press release, October 25, 2013.

[6] A decentralized virtual currency created in 2008 which ensures a high degree of anonymity to users.

Published in Articles section of www.manupatra.com

completely different than a recognizable crime committed in a completely different way."[7]

I. Drugs, Weapons and Exotic animals

Websites such as Silk Road act as anonymous marketplaces selling everything from bland items such as books and clothes, to more illicit goods such as drugs and weapons. Aesthetically, these sites appear like any number of shopping websites, with a short description of the goods, and an accompanying photograph.[8]

II. Stolen goods and Information

It is correct to assume that dedicated sites facilitate users to trade in both physical and proprietary information, including passwords and access to passwords for surface web paid-pornography sites and PayPal passwords.[9] PayPal Store, Creditcards for All and Another Porn Exchange are active websites that offer such services.

III. Murder

The Assassination Market website is a prediction market where a party can place a bet on the date of death of a given individual, and collect a payoff if the date is "guessed" accurately. This motivates the assassination of individuals because the assassin, knowing when the action will take place, could profit by making an accurate bet on the time of the subject's death. Because the payoff is for knowing the date rather than performing the action of the assassination, it is substantially more difficult to assign criminal liability for the assassination.[10] There are also websites to hire an assassin — popular ones are White Wolves and C'thuthlu.[11]

IV. Terrorism

The dark web and terrorists seem to complement each other — the latter need an anonymous network that is readily available yet generally inaccessible. It would be hard for terrorists to keep up a

[7] Grabosky, Peter. 2001. "Virtual Criminality: Old Wine in New Bottles?" Social & Legal Studies 10: 243–49. Http:// sls.sagepub.com/content/10/2/243.full.pdf.

[8] Bartlett, Jamie. 2014. "Dark Net Markets: The Ebay of Drug Dealing," The Observer, October 5.

[9] Westin, Ken. 2014. "Stolen Credit Cards And The Black Market: How The Deep Web Underground Economy Works." Linkedin, August 22.

[10] Greenberg, Andy. 2013. "Meet the 'Assassination Market' Creator Who's Crowd Funding Murder with Bitcoins." Forbes, November 18.

[11] Pocock, Zane. 2014. "How to Navigate the Deep Web." Critic, Issue 03, March 19.

presence on the surface web because of the ease with which their sites could be shut down and tracked back to the original poster.[12]

V. Exploit Markets

Exploits are malware based on software's vulnerabilities — before they are patched. Zero-day exploits target zero day vulnerabilities — those for which no official patch has been released by the vendor.[13] Exploit markets serve as platforms for buying and selling zero-day exploits, and an exploit's price factors in how widely the target software is used as well as the difficulty of cracking it.[14]

VI. Illegal Financial Transactions

Websites such as Banker & Co. and InstaCard facilitate untraceable financial transactions through various methods. They either launder bitcoins by disguising the true origin of the transactions or give users an anonymous debit card issued by a bank. Users are also given virtual credit cards issued by trusted operators in the dark web.[15]

Buying stolen credit card information has never been easier. A website called Atlantic Carding offers this service, and the more you pay, the more you get. The user's details — name, address and so on — are available at an additional cost.[16]

VII. The Hidden Wiki

The main directory on the dark Web is the Hidden Wiki. It also promotes money laundering services, contract killing, cyber attacks and restricted chemicals, along with instructions to make

[12] Michael Chertoff And Tobby Simon, The Impact of the Dark Web on Internet Governance And Cyber Security, Global Commission on Internet Governance Available At Https://Www.Cigionline.Org/Sites/Default/Files/Gcig_Paper_No6.Pdf (February 2015)

[13] "Zero-Day" refers to the fact that the programmer has had Zero Days to fix the flaw.

[14] Miller, Charlie. 2007. "The Legitimate Vulnerability Market: Inside the Secretive World of 0-Day Exploit Sales." Http://Weis2007.Econinfosec.Org/Papers/29.Pdf.

[15] Dean, Matt. 2014. "Digital Currencies Fueling Crime on the Dark Side of the Internet." Fox Business, December 18.

[16] Dahl, Julia. 2014. "Identity Theft Ensnares Millions While the Law Plays Catch Up." Cbs News, July 14.

Published in Articles section of www.manupatra.com

explosives. As with other dark web sites, the links to these sites frequently change to evade detection.[17]

VIII. Human Experimentation

The Human Experiment was a website that detailed medical experiments claimed to have been performed on homeless people who were usually unregistered citizens. According to the website, they were picked up off the street, experimented on and then usually died. The website has been inactive since 2011.[18]

IX. Heist

There are many rob-to-order pages available in the dark Web, hosted by people who are good at stealing and will steal anything that you cannot afford or just do not want to pay for.[19]

X. Arms Trafficking

Euroarms is a website that sells all kinds of weapons that can be delivered to your doorstep anywhere in Europe. The ammunition for these weapons is sold separately — that website has to be tracked down separately on the dark Web.[20]

XI. Pedophilia

Pedophilia, or child pornography is enormously accessible. Pornography is accepted on the surface web with some regulation. The dark Web offers various types of sites and forums for those wishing to engage in pedophilia.[21]

Darknet Markets

In 1972, long before eBay or Amazon, students from Stanford University in California and MIT in Massachusetts conducted the first ever bit of e-commerce. Using the "Arpanet" account at their artificial intelligence lab, the Stanford students sold their

[17] Williams, Christopher. 2011. “The Hidden Wiki: An Internet Underworld of Child Abuse.” The Daily Telegraph, October 27.

[18] Falconer, Joel. 2012. “A Journey into the Dark Corners of The Deep Web.” The Next Web, October 8.

[19] Siddiqui, Sameer Iqbal. 2014. “Real Power of Deep Web and How to Harness It.”Real Hackers Point (Blog), June 19.

[20] Love, Dylan. 2013. “There’s A Secret Internet for Drug Dealers, Assassins, and And Pedophiles.” Business Insider, March 6.

[21] Greenberg, Andy. 2013. “Meet the ‘Assassination Market’ Creator Who’s Crowdfunding Murder with Bitcoins.” Forbes, November 18. 2014. “Over 80 Percent Of Dark-Web Visits Relate To Pedophilia, Study Finds.” Wired, December 30.

counterparts a small amount of marijuana. Ever since, the net has turned over a steady trade in narcotics.

Just like almost every other business, drugs are moving online. And, just like almost every other business, e-commerce is faster, easier and offers great value. Most internet users who wish to hide their identity take simple measures, such as using pseudonyms on social media sites or clearing the web browser history from their computer.[22] A small proportion use sophisticated complicated anonymity systems that offer stronger protection.

The dark net markets sit on an encrypted part of the internet called Tor Hidden Services, where URLs are a string of seemingly meaningless numbers and letters that end in ".onion", and are accessed using a special browser called Tor. The browser, which was originally built by the US Navy but is now an open-source project, allows people to browse the net without giving away their location.[23]

This little-known parallel internet is a natural home for an uncensored drugs marketplace, as it is for whistleblower websites and political dissidents who also rely on its powers of obfuscation.

Law Enforcement & Darknet

The use of the Internet, and in particular the Dark Web, for malicious activities has led policy makers to question whether law enforcement and other officials have adequate tools to combat the illegal activities that might flow through this underworld.[24]

For them, the emergence of the Deep Web in general and Darknet in particular offers a new economic, social, and political ecosystem that was designed to exist and operate beyond the reach of law, regulation, and government oversight. With the authorities struggling to catch up with the surface web issues of fraud, piracy etc, the insidious nature of dark net remains completely out of the scanner. If policymakers want to understand the Deep Web and Darknet, they will need to give it premeditated focus and move beyond usual Internet search methods.

[22] pew research center, 2013, http://goo.gl/59aycp

[23] Jamie Bartlett, Dark Net Markets: The Ebay of Drug Dealing (5 October 2014) available at http://www.theguardian.com/society/2014/oct/05/dark-net-markets-drugs-dealing-ebay

[24] U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies, 113th Cong., 1st Sess., November 18, 2013.

Published in Articles section of www.manupatra.com

Law enforcement responses to the Dark Net have configured around traditional strategies of surveillance, interdiction and prosecution, although from a low base of technical capacity, with limited transnational integration and within the constraints imposed by national legislative frameworks.[25]

Traditional law enforcement strategies and policing techniques are inadequate to deal with the full range of Dark Net and hidden services available, and that pose challenges in terms of locating servers and uncovering encrypted, anonymous identities dispersed internationally among individuals. The transnational nature of the hidden markets render national level policing strategies and evidence gathering largely ineffectual, while simultaneously posing complex questions in relation to prosecution.[26]

Till date, enforcement has relied on the use of informants, undercover surveillance, tracking, hacking, exploitation or creation of security breaches (for example through the use of malware) and high publicity 'take downs' intended to alarm and intimidate users, vendors and host service providers, including through the message that no interactions can ever be anonymous and there is always a risk of arrest and prosecution.

In the 2014 World Drug Report, the rise of hidden, Dark Net drug markets was belatedly acknowledged. The Report set out that the variety of drugs available on the Dark Net appeared to be 'diverse and growing' and this posed 'unique challenges for law enforcement.' As outlined by Interpol in the Internet Organized Crime Assessment (iOCTA), the relationship between customer and vendor in the hidden markets is purely transactional. Criminals in cyberspace do not need to be close to the crime scene, they might never even travel to the target country; their activities can be conducted on a transnational basis and with minimum effort and risk by hiding their identity. Unlike as in the off-line worlds, where criminals normally need to be physically present at the crime scene.'[27]

[25] Julia Buxton & Tim Bingham, The Rise and Challenge of Dark Net Drug Markets, Global Drug Policy Observatory available at http://www.swansea.ac.uk/media/the%20rise%20and%20challenge%20of%20dark%20net%20drug%20markets.pdf (January 2015)

[26] Discussing Drugs on the Dark Net, Central European University available at http://www.ceu.edu/article/2015-03-03/discussing-drugs-dark-net (March 3, 2015)

[27] Europol's 2014 Internet Organised Crime Assessment (iOCTA) can be found at https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta

International law consists of rules and principles governing the relations and dealings of nations with each other. This somewhat old-fashioned way of thinking is problematic when it comes to the Internet. The legal issues that typically arise around the Internet rarely involve disputes between nations and their dealings, but often do involve individuals of different nationalities. The problem is compounded when dealing with the Dark Web, where users route their address through multiple servers to stay anonymous. It is virtually impossible to tell in which country a user of Tor is located.[28]

The trans-nationality of these networks thwarts eradication, regulatory, and prosecution efforts of any one state, creating cooperation, collective action, and law harmonization problems for state actors attempting to work together to counter unlawful use of the Internet.

On the Internet, data can easily enter any sovereign territory undetected. There are no borders and no customs officers protecting entry. With no treaty and no regulation, the Internet has been left a world without borders and without regulations. It is a bountiful world filed with limitless information having its dark corners.[29]

Actions taken against Darknet Markets

Law enforcement and judicial agencies around the globe undertook a joint action against dark markets running as hidden services on Tor network. The action aimed to stop the sale, distribution and promotion of illegal and harmful items, including weapons and drugs, which were being sold on online 'dark' marketplaces. Operation "Onymous", coordinated by Europol's European Cybercrime Centre (EC3), the FBI, the U.S. Immigration and Customs Enforcement's (ICE), Homeland Security Investigations (HSI) and Eurojust, resulted in 17 arrests of vendors and administrators running these online marketplaces and more than 410 hidden services being taken down. In addition, bitcoins worth approximately USD 1 million, EUR 180 000 euro in cash, drugs, gold and silver were seized.[30]

[28] Terry M. Brown, Trolling the Deep: Emerging International Concerns on the Deep Web (February 4, 2015) available at http://campbelllawobserver.com/trolling-the-deep-emerging-international-concerns-on-the-deep-web/

[29] *Ibid*.

[30] pierluigi paganini, operation onymous, the joint attack against dark markets in tor, security affairs available at

Law enforcement agencies around the world have started to take a keen interest in what takes place in this strange encrypted internet, and are getting better at shutting down these sites. Periodically one market disappears following a police raid or some vendors are arrested. It's usually the result of infiltration by undercover cops, or, more often, human error. But it's an arms race, and it feels like the police are losing. Because they live on the periphery, dark net markets are remarkably adaptive, and learn from each mistake: always innovating ways to be more secure, more decentralized, and harder to combat.[31]

The problem lies in finding the real criminals of the Dark Web, given the level of protection and anonymity offered by Tor. For every website that is shut down[32] a new one pops up in its place. For every Ross Ulbricht[33] that is arrested there are hundreds more lurking in the bowels of the Dark Web. How can the legal system fight an enemy that it can't even find? One of the easiest ways to curtail illegal activity on the Dark Web can be through regulation. But as is seen by the failure of the proposed ITU treaty[34], regulation is not on the horizon any time soon.

Suggestions

Given an acknowledged lack of technical capacity, legal constraints and poor international enforcement coordination, Dark Net prohibition efforts should give priority to crimes such as child sexual exploitation, cyber terrorism and weapons trafficking, and work with self-regulating, 'ethical' drug sites to enhance understanding of high-level criminality on the Dark Net.

http://securityaffairs.co/wordpress/29952/cyber-crime/operation-onymous-vs-dark-markets.html (november 7, 2014)

[31] Claude Ghaoui, Encyclopedia of Human Computer Interaction, Idea Group Reference, 2006 pg 239

[32] As of November 2014 the Silk Road was on version four

[33] Ross William Ulbricht created a darknet market named Silk Road and ran it until his 2013 arrest, under the pseudonym dread pirate Roberts. He was convicted of money laundering, computer hacking and conspiracy to traffic narcotics in February 2015. He is serving a life sentence without the possibility of parole.

[34] The treaty proposed by the United Nations international telecoms union ("ITU") was aimed at giving national governments control of the internet. The proposed treaty sought to "de-fragment" the internet and help the internet run more effectively through the use of government oversight. The treaty sought to establish that governments have an international legal right to access international telecommunication services, something not previously part of international law on telecommunications. Ultimately the United States, along with a coalition of other nations voted against the treaty causing it to fail.

Published in Articles section of www.manupatra.com

Using policy that targets individuals and the illicit exchange of information alone will not provide an adequate solution. Requesting the closure of certain bandwidth providers does not correct the underlying problem, as many of the sites will disappear to avoid detection and quietly transfer to other providers. A more successful long-term strategy is therefore to make more transparent transactions and data flow trails across the internet.[35]

Sting operations can be set up where either hidden websites are created or an account is created on an existing one and illegal transaction can be conducted. If a buyer is purchasing a physical item, an address must be given and law enforcement can simply arrive at the buyer's doorstep once the package arrives. Timing correlation attacks can also be done where by looking at the time a request moves through the initial server and matching it with the time a request moves out the final server and towards the hidden site. If the times match up that a specific user was accessing a specific site.

It is the split nature of the internet that has a direct impact on policy development. Darknet activity is not a regional issue, but rather a global issue. Legislation will need to be coordinated to align national and regional policies with international policy.[36]

There are two priorities-

→ to ensure that existing cyber crime policies operate in a joined-up manner across national boundaries to tackle criminal activity.

→ to correct the current disconnection between legislation at the national, regional and international levels.

The United Nations Office for Drugs and Crime (UNODC) has therefore recommended a number of approaches that can be taken by policy makers to move away from the reliance on traditional law, towards forming overarching formal international co-operation on criminal matters. Co-operative policy controls that UNDOC has suggested that can be developed include:

→ Companies and organizations being required by law to disclose security breaches.

[35] Anita Greenhill, Responding to the 'Darknet', Manchester Policy Blogs: Science and Technology available at http://blog.policy.manchester.ac.uk/sci-tech/2014/06/responding-to-the-darknet/ (June 27, 2014)

[36] *Ibid*.

- → Banks being instructed to co-ordinate their security responses and ensure their security contractors share information.
- → National governments should co-ordinate their police focus on specific areas of cybercrime, such as botnets, dissident exchange, etc.
- → Cybercrime should be treated as an illegal industry and its activities such as money laundering targeted.[37]

The key to all of this was that only international collaboration would help bring cyber-criminals to justice. There is a need to pool resources together, that's the way forward. Also, there should be stronger relationships between the private sector, law enforcement and the courts to ensure that all the legal authorities that exist can be brought to bear against cyber attackers. Moreover, law enforcement alone is not equipped to outdo the ingenuity and dynamic nature of a market force like the Darknet. The private sector may offer advanced legal and technical solutions to disrupt transnational organized crime online that deters such activity more effectively than the arrest of a small number of hackers.[38]

It is important that transparency and openness relating to data transactions is encouraged at industry and governmental level. In addition, governments need to carefully consider and co- ordinate policy development to enable them to co-operate in overcoming the emerging challenges of the internet in the 21st century – the darknet and cybercrime.

Preventing criminal activity on Tor Hidden Services presents Law Enforcement Agencies (LEAs) with a major challenge. LEAs may seek information about a user’s online behaviour from Internet Service Providers (ISPs). However, Tor is designed so that no single entity (including ISPs and Tor Project Inc.) knows about a user’s online behaviour, such as which websites they visited. Therefore, such agencies need to pursue more complex methods to find out about the online behaviour of a Tor user.

Law enforcement should focus skills and resources on high level organized and voracious cyber-crime including child and female sexual exploitation, financial crime, weapons trafficking, cross

[37] Supra 37.

[38] Doug Depeppe, Deputizing the Cyber Posse: The Next Frontier of Public-Private Partnership available at http://www.forbes.com/sites/frontline/2014/08/26/deputizing-the-cyber-posse-the-next-frontier-of-public-private-partnership/#4ec6b8086e6e (August 26, 2014)

border cyber- attacks and cyber terrorism. As outlined in a 'Computers at Risk' report by the US National Research Council from 1991, 'Tomorrow's terrorist may be able to do more with a keyboard than with a bomb.'[39]

Also, the growth of hidden markets and the Dark Net more broadly evokes startling statements and publicity from politicians, the media and law enforcement. Public opinion and policy responses must not be framed by panic and fear of emerging technologies. A primacy must be placed on information, explanation and evidence, particularly to bridge generational divides over technology literacy and use.

What the government should be concentrating on is an effort to break the financial ties that hold the darknets together. Finding who holds the purse strings is a complex task, but it's a technique that's been proven to work time and time again. And perhaps it should also be noted that it's an approach that's well within the capabilities of the powerful surveillance tools that government security agencies have put in place to monitor social connections and financial traffic online as part of their efforts to combat terrorism.[40]

Conclusion

Silk Road and the Dark Web are so new that case law, scholarly articles, and even the legal system have not caught up yet. The best way to understand the problems presented by the Dark Web is through the lens of public policy. The Dark Web is not inherently bad, but it is a classic example of the "one rotten apple spoils the whole bunch" scenario where the negative aspects of the Dark Web have the potential to ruin the whole thing if they are not properly controlled.

As the law currently stands, the legal system cannot do much to combat the darker elements of the Dark Web. It is clear that some regulation must be put into place. There are aspects of the Dark Web that present real danger to our society and the law is not well equipped to handle them at the current point in time.

[39] D. Denning (2000) Cyberterrorism: The Logic Bomb versus the Truck Bomb', Global Dialogue. 2:4.

[40] Simon Bisson, The Key to Cleaning up the Internet is Tackling the Darknets, Not Letting Censorship in by the Back Door available at http://www.zdnet.com/article/the-key-to-cleaning-up-the-internet-is-tackling-the-darknets-not-letting-censorship-in-by-the-back-door/ (July 22, 2013)

Published in Articles section of www.manupatra.com

Recent revelations about wide scale nation-state monitoring of the Internet and recent arrests of cybercriminals behind sites hosted in the dark web are starting to lead us to other changes. It would not be surprising to see the criminal underbelly becoming more split into alternative dark nets or private networks, further complicating the job of investigators.

The markets for hacking programs, cybercrime tools, and stolen data, in particular, have continued to grow with no signs of slowing down. There is an urgent need for policymakers and the public to better understand the Deep Web and develop more comprehensive law enforcement, regulatory and national security response.

The dark web has the potential to host an increasingly large number of malicious services and activities and, unfortunately, it will not be long before new large marketplaces emerge. Security researchers have to remain cautious and find new ways to spot upcoming malicious services to deal with this new phenomenon as quickly as possible.

Published in Articles section of www.manupatra.com