The Theory of Darknet

Philippe Davadie
Member of the Chair of Cybersecurity and Cyberdefense
June 2015, Article n°IV.7

Translated from French

What is a darknet?

An evolving definition

Using the term "darknet" in a conversation almost immediately sparks debate, as the term is controversial. For some, the darknet is the hidden face (dark) of the internet (net), for others it is a lawless area of cyberspace (net) where illegal activities are committed (dark). For others it is a mixture of both.

Before continuing, it is necessary to clarify the definitions of certain terms that are confused with the term "darknet": dark web, the deep web, invisible web, and the hidden web. These phrases are often used as synonyms of each other and cover the part of the internet that is available online but is not indexed by traditional generalist search engines (Google, Yahoo !, etc.). However, it is important to be cautious and to clarify that the invisible web is inaccessible to conventional search engines, as a result more and more specific search engines are developed. Thus the search engine Shodan [1], created in 2009, references all objects connected to the internet, regardless of their destination.

The darknet is fascinating and Google searches of this term have risen sharply in recent times:

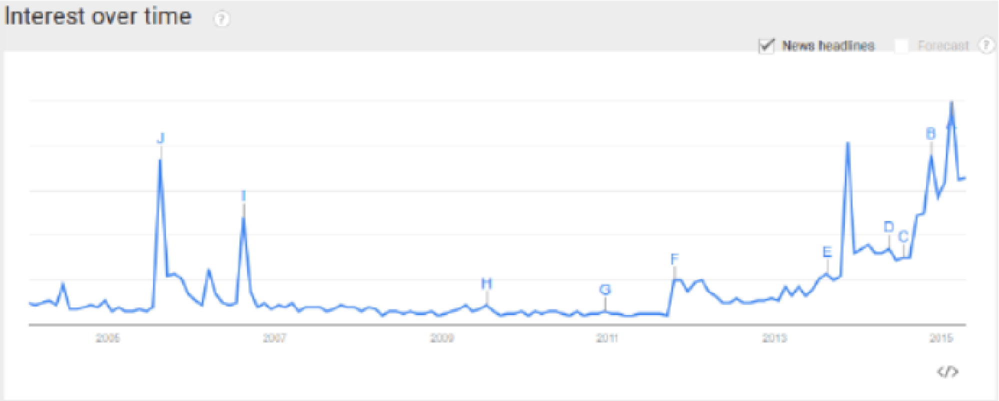


Figure 1: Queries of the term "darknet" since 2005 (Google Trends)

This incomplete graph (because it only includes Google queries) raises questions about the two peaks that appear in 2005 and 2006 before giving way to fewer queries and then increasing again in 2012. This may be explained by the publication of a book by Joseph Daniel Lasica in 2005 entitled, "*Darknet: Hollywood's War Against the Digital Generation*." Thereafter, interest fell before rising again in late 2011 when, notably, the Operation Darknet was carried out by Anonymous group, which we cover below.Disregarding the search peaks, we note that there is a trend of an increased number of queries of the term darknet.

What exactly is it?

If we consult the recent history of the internet, it appears that the term darknet was coined in the 1970s to identify networks where the users wished to disconnect voluntarily from the Arpanet.

According to Andrew Lewman in April 2015, Executive Director of the Tor Project (the Onion Router), "the term dark net actually comes from a Google or Alta Vista - if you remember that search engine from 15 years ago - from a presentation they did about here's all the data that is locked behind paywalls, locked behind log-in screens, in corporate networks. And if your goal is to crawl all the world's information, what is dark to you is the things you can't crawl"[Lew]. At that time what was hidden there from the public was not necessarily illegal. We note that here the term darknet for the authors of this presentation means what we now call the invisible web.

In 2002 the term was then used by Peter Biddle, Paul England, Marcus Peinado and Bryan Willman, all Microsoft employees, in an article [Bid] where they explain that such networks undermined copyright protection and that the development of DRM (digital rights management) could counter them. There they define the term darknet as follows: "a collection of networks and technologies used to share digital content. The darknet is not a separate physical network but an application and protocol layer riding on existing networks." If this definition does not suggest anything illegal, the context in which the term is used suggests the opposite, that the darknet promotes illegality. In 2011, Symon Aked defines a darknet as: "[d]arknets are encrypted data networks that ensure data transmitted cannot be intercepted, changed, observed or read by an unauthorised party. Darknets may also be designed to allow participants to be anonymous, or obtain pseudo-anonymity where desired"[Ake].

Given these differences of opinion, it seems difficult to find a definition that is accepted unanimously. Andrew Lewman also believes that "the term darknet is inappropriate; the network is often referred to as dark because search engines cannot see it"[1][Lew].

Whatever its relationship to legality suggested by these different definitions, we notice that in all these definitions of the term, the exclusion of the rest of the internet is the common denominator. This exclusion is highlighted by Anne Souvira, head of the investigative brigade of fraud in information technology (brigade d'enquêtes sur les fraudes aux technologies de l'information - BEFTI). For her the darknets are private networks, "often very secure to limit access" and protected by passwords, certificates, captchas, etc.[GSM] With restricted access, one can only access it with a referral, regardless of the form it is in. The darknets are therefore distinguished from the deepweb, the latter having been investigated elsewhere [Ber2].

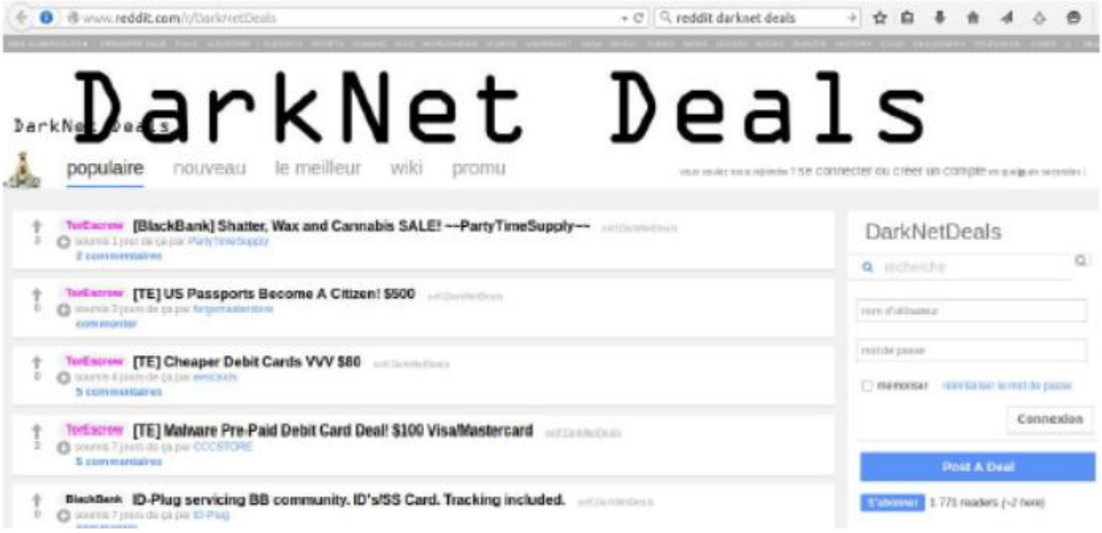
Is the darknet necessarily illegal?

[1] *Phrase translated into English, original phrase in French : "le terme darknet est inapproprié; le réseau est souvent qualifié de sombre (dark) parce que les moteurs de recherche ne peuvent le voir."*

This restriction of access feeds the belief that the darknets may be illegal trafficking havens. Thus the conspiracy theories in the real world echo the darknet theories in cyberspace. It is true, however, that such restrictions of network access is a necessary precondition for illegal activities to thrive (but not sufficient alone). Aked wrote: "Media sites, both technical and non-technical, make references to Darknets as havens for clandestine file sharing. They are often given an aura of mystique; where content of any type is just a mouse click away."[Ake]

In reality everything that comprises illegal and criminal activities is found on these networks: sale and exchange of confidential information, counterfeit items (cigarettes, false papers, etc.), collection of funds for organized criminal organizations, child pornography, "pirates for hire" (like killers for hire), websites that showcase malicious organizations, malware, weapons and drug trafficking, etc.

The figure below illustrates this.



[BlackBank] Shatter, Wax and Cannabis SALE! ~~PartyTimeSupply~~

[TE] US Passports Become A Citizen! $500

[TE] Cheaper Debit Cards VVV $80

[TE] Malware Pre-Paid Debit Card Deal! $100 Visa/Mastercard

ID-Plug servicing BB community. ID's/SS Card. Tracking included.

Figure 2: Possible sales on the darknets

The existence of these protected networks allows criminals to expand their business with a feeling of certain impunity, which has led them to develop specialized forums.[2] This development was highlighted in a report by RAND Corporation, “Markets for Cybercrime Tools and Stolen Data”[3] published in 2014. It appears that these marketplaces are organized and have become extensions of what is happening in the real criminal world. According to Michael Callahan, Vice President of Security Product Marketing at Juniper Networks, this could be a sign of maturity of this type of market, "the RAND study shows that if a market meets the following criteria: sophistication, specialization, reliability, accessibility and resilience, then it has reached maturity."[Rand]

The opportunities to engage in criminal activities on the darknets and the widespread generalization that anyone browsing the darknets is a criminal are separated by a thin line; however, it would be hasty to assume that everyone crosses it. Indeed criminals are not the only ones to visit these networks, as investigating pseudonyms[4] has allowed investigators to infiltrate the networks, and they are also the object of interest by some scientists and lastly, there is no denying the fact that some people visit out of curiosity.

[2] Cf. page http://www.informationweek.com/cybercrime-black-markets-grow-up/d/d-id/1127911

[3] Download at the site http://www.rand.org/pubs/research_reports/RR610.html

[4] Provided for by Article 706-87-1 of the Code de Procédure Pénale.

Symon Aked relativizes this negative view of the darnets by saying [Ake] "The Australian High Tech Crime Centre identified that ‘Darknets…could potentially be abused by cybercriminals to distribute propaganda, images of child abuse, or copyrighted digital files in a secure manner to avoid the scrutiny of law enforcement agencies.’"

Moreover, nothing prevents many honest people from creating a darknet to safely communicate amongst themselves about a legal project, such as the launch of a new product. For all the reasons stated above, the definition of a darknet on wikipedia seems relevant. According to wikipedia a darknet is a “virtual private network whose users are considered trust-worthy. Most of the time, these networks are small, often less than ten users each. A darknet can be created by any type of person and for any purpose, but the technique is most often used specifically to create anonymous peer-to-peer file sharing networks. The darknets are distinct from other distributed peer-to-peer networks because sharing within them is anonymous (that is to say that IP addresses are not publicly shared) and therefore users can communicate with little fear of government or business interference.”
We note, however, that the use of the word *confidence* seems ill-adapted, particularly in the case where the darknet is used by different types of criminals.

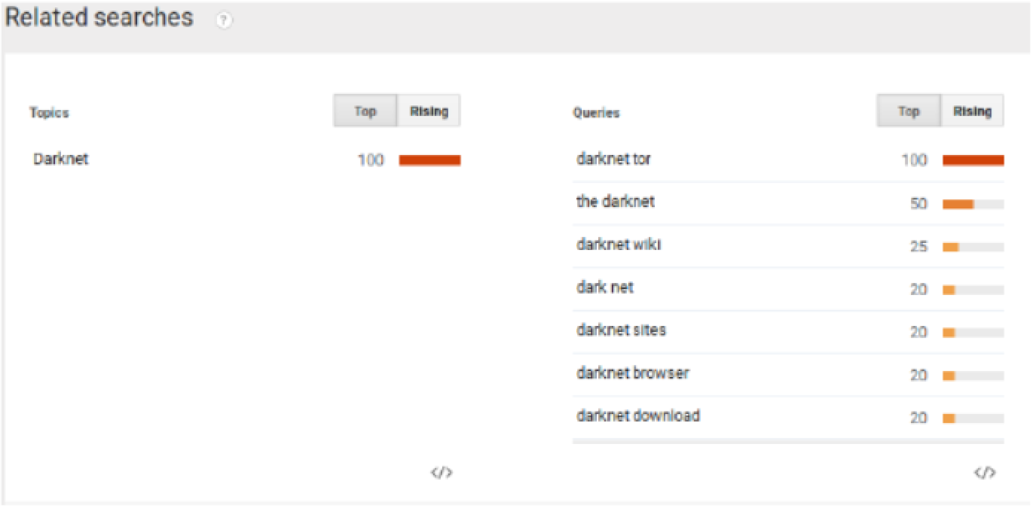
Tools and mechanisms

Entering the darknet

Based on the work already cited by Biddle, England, Peinado and Willman [Bid], some darknets used software designed for peer-to-peer file sharing such as Napster and Gnutella. The latter software had to be abandoned because, according to these authors, it did not allow one to preserve anonymity.

It seems that currently, Freenet (an anonymous and distributed computer network functioning as a space for shared storage and distribution) [Ake], I2P (an anonymous network with a simple overlay network software that applications can use to send, via end-to-end encrypted communication, information to each other) [Ake] and GNUnet (a peer-to-peer network ensuring anonymity) are the most used. Other software allows for the creation of such networks, such as Retroshare (free) and SafetyGate Invisible (commercial).

Bringing up the darknet requires bringing up Tor, a software strongly associated with the darknets that reinforces many negative critiques and efforts of reverse engineering to unlock its secrets. Moreover, a search of the term darknet shows (Google trends) that those looking for the term are strongly associated with Tor.



Related searches

Topics	Top / Rising
Darknet	100

Queries	Top / Rising
darknet tor	100
the darknet	50
darknet wiki	25
dark net	20
darknet sites	20
darknet browser	20
darknet download	20

Figure 3: Queries related to the term darknet (Google Trends)

While the protocol mainly used on the internet is HTTP (Hyper Text Transfer Protocol), Tor uses its own protocol and Andrew Lewman defines it as "an anonymous browser that puts you in control of your data." He also adds "Tor exists for all the reasons of internet freedom and putting users in control of their data. And that's what we'll continue to do and we'll continue to research going further."[Lew] According to the estimates of Andrew Lewman, Tor is used by about 2.5 million people daily, with users mainly located in the USA and Europe where protection of privacy is a concern [Lew].

Using only Tor does not guarantee complete privacy of exchanges and uses. Andrew Lewman explains, " I think that if your only adversary is the NSA or GCHQ you've probably already lost that battle, because they are multibillion-dollar agencies with fantastic capabilities, and a single tool... much like you cannot build a house with just a hammer, you need a whole toolbox and a whole set of practices to be able to defeat adversaries like that."[Lew]

To maximize the time during which privacy is maintained, it is advisable to use a VPN in addition to Tor. Two options are offered to the user:
- to connect to a VPN first, then Tor. The path followed is: the computer, the VPN, Tor and the Internet. The ISP ignores that you are connected to Tor, and your VPN can not track your activity.
- to connect to Tor first, then the VPN. The path followed is: the computer, Tor, the VPN, Internet. The VPN does not know your IP address, and any VPN logs are protected by Tor. This solution enhances anonymity.

Several players are positioned to use technology to create a darknet. Mozilla is committed to the Polaris Initiative with other internet companies concerned with privacy issues to "collaborate more effectively, more explicitly and directly" and thus integrate "more privacy features into our products."[Moz] This commitment was made following the results of a survey conducted in October 2014 on a sample of over 7,000 adult internet-users that showed that 74% of respondents felt that their personal information on the web was less private over the course of a year and that major internet companies had too much private information about them.

Navigating the darknets

Once the darknet was created and anonymity was protected, the question of navigation of the web was brought up. Indeed, alternating the navigation method in darknet wtih that of the open web is likely to eventually compromise anonymity. These techniques and software alone therefore do not suffice. Once a darknet is created, it must remain and find functions similar to those offered on the public Internet.

However, because the darknets are shrouded in secrecy, it cannot be accessed via public search engines. It is necessary to go through hidden wiki that include the address directories of sites on the darknet. One can also use specialized search engines such as Grams, which has an interface similar to that of Google.

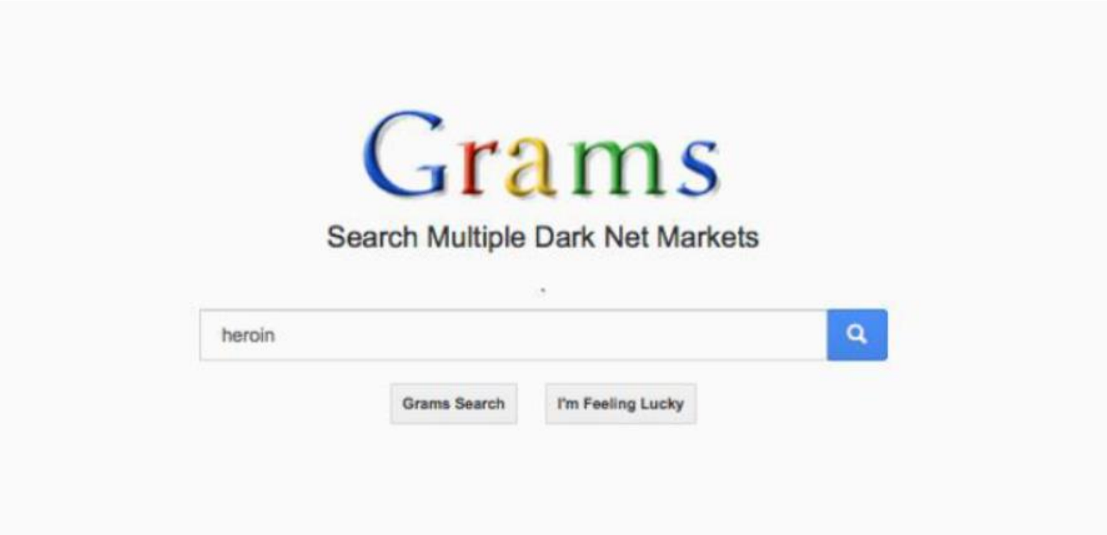


Figure 4: The Grams homepage

The Grams creator said: "I am working on the algorithm so it is a lot like Google's it will have a scoring system based how long the listing has been up, how many transactions, how many good reviews. That way you will see the best listing first. I am going to add a filter market this week so a user can search only the markets they have accounts for. I have the code for the price converter written just haven't implemented it yet. "[Red] The URL to access the browser is: URL-grams7enufi7jmdl.onion

One can also use Onion City, the search engine of Tor (http://onion.city/) that after one week of indexing had already indexed 350,000 pages.

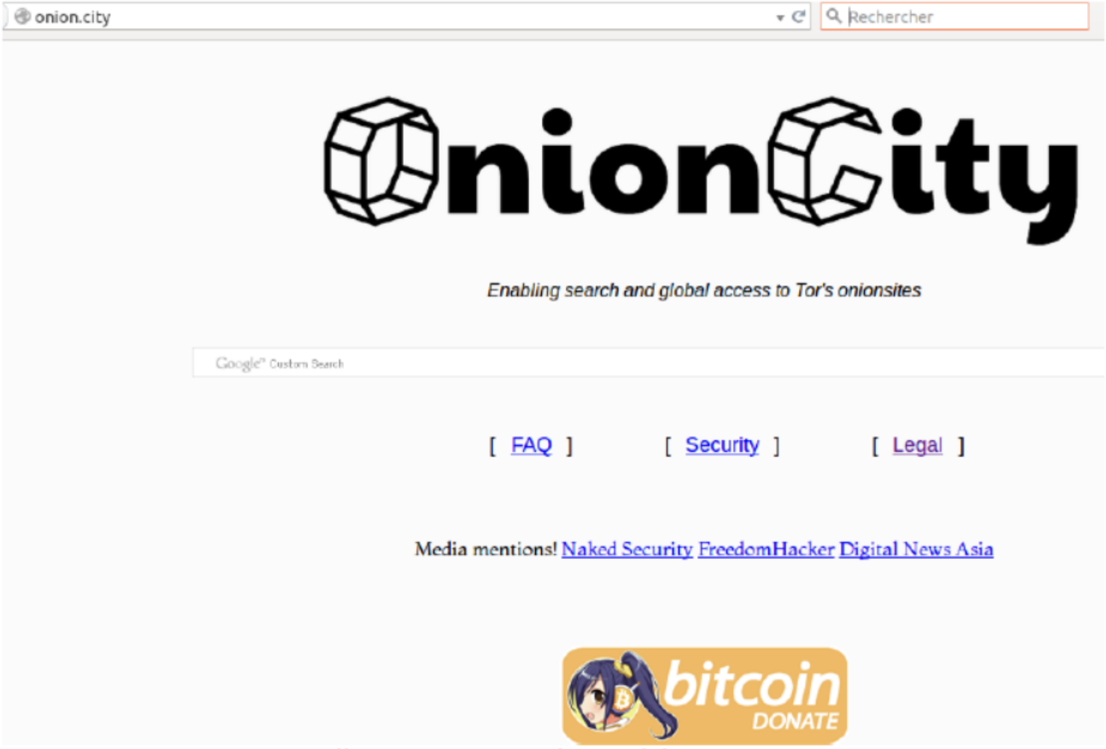

onion.city
Rechercher
OnionCity
Enabling search and global access to Tor's onionsites
Google™ Custom Search
[FAQ]
[Security]
[Legal]
Media mentions! Naked Security FreedomHacker Digital News Asia
bitcoin
DONATE

Figure 5: Onion City Homepage

Controversies

The darknets cannot help but stir up controversy at a time when there are increasingly frequently intrusions to privacy, which are the result of legislative changes that seem to follow the motto "it does not bother those who have nothing to hide." The most significant is not so much the existence of the darknet, which can be seen as evidence that any human group will seek to preserve its secrets, but the tools used to maintain anonymity on the internet. And Tor seems to be the flag bearer. Controversies surrounding the subject never cease, the fact that it is the result of a project by the US Navy launched in 2002, is significant because it is paradoxical. Andrew Lewman added to this paradox when he said: "The people in the US government who fund us really want privacy and anonymity to exist." [Lew]

According to a study by Gareth Owen of Portsmouth University shown during the meeting of the Chaos Computer Congress in 2014, 80% of visits via TOR can be linked to pedophilia [Wir2]. These results are controversial, because "law enforcement and anti-abuse groups patrol pedophilia Dark Web sites to measure and track them, for instance, which can count as a ‘visit’" [Wir2]. Besides this there were denial of service attempts to these sites and visits from botnets. Recognizing these limitations, the author of the study stated: "We do not know the cause of the high hit count [to child abuse sites] and cannot say with any certainty that it corresponds with humans "[Wir2]. These sites, however, represent only 2% of websites reachable via TOR.

Were means and objective confused in this controversy? Those seeking pedophile sites will most often do so anonymously. To conclude based on this study that TOR is bound up with crime, amounts to a campaign against anonymity and pseudonymity, regardless of the circumstances.

Aked, in his study cited above, lists the types of documents he could find using various software to enter the darknets [Ake]. On I2P BitTorrent, he found no child sexual abuse material, as was the case with the I2P networks Gnutella and eDonkey, Freenet and with Frost. However, he himself recognizes the limitations of his study and that it was not exhaustive.

Utility and the future

The Volatility of Darknet

It seems that much of what is found on the darknet is volatile. When browsing publications on the subject, we noted that the life of the sites indexed by Tor would be only a few days to weeks. However, this is not surprising, whether the activity protected in the darknet is legal or not. Illegal activity owes its longevity to its secrecy and stealth. If secrecy is provided by the mentioned software, stealth is the result of human action. In the real world, criminals change the locations of their operations often as a way to extend their existence. It is logical to observe the same thing in cyberspace.

As for legal activities, if creators consider it necessary to use the darknet it is because they fear being listened to or tracked. A frequent change of darknet settings allows them to circumvent the surveillance they want avoid.

Darknet Users

Over time, the darknets changed from sharing confidential files to sharing pirated files (mainly music in the late 90s) and then to sharing illegal products, and finally to the defense of privacy. Saying that darknet is the only means of protection for illegal activities is reductive. Besides, as Biddle, England, Peinado and Willman acknowledged, Gnutella does not allow illegal things [Bid].

Given the contradictory ideas circulating about the darknets, it is logical to ask whether these networks are actually used or if they are only a cybernetic urban legend. A study [Kad] conducted in 2014 and 2015 that was intended to calculate the share of network traffic attributed to hidden-services and count the number of unique addresses (in .onion), shows that "30,000 hidden-services on the Tor network represent about 3.4% of total traffic in the network, according to a study of the Tor project."

However, as we noted earlier, we do not only find sites or objects deemed illegal on the darknet. Thus, in 2014 Facebook launched a specific service via Tor: https: //facebookcorewwwi.onion/ [College].

Content repression by publishers

In 2002, Biddle, England, Peinado and Willman assessed that the fight against the darknets was difficult as "networks such as Gnutella are difficult to regulate because they are spread-out widely and they have hundreds of millions of nodes. Looking at them more closely, one finds multiple vulnerabilities."[5] [Bid]

Repression was nevertheless possible because of the absence of real user anonymity: "All attacks we have identified exploit the lack of endpoint anonymity and are aided by the effects of free riding. We have seen effective legal measures on all peer-to-peer technologies that are used to provide effectively global access to copyrighted material. Centralized web servers were effectively closed down. Napster was effectively closed down. Gnutella and Kazaa are under threat because of free rider weaknesses and lack of endpoint anonymity. Lack of endpoint anonymity is a direct result of the globally accessible global object database, and it is the existence of the global database that most distinguishes the newer darknets from the earlier small worlds. At this point, it is hard to judge whether the darknet will be able to retain this global database in the long term, but it seems seems clear that legal setbacks to global-index peer-to-peer will continue to be severe."[6] The same authors, however, felt that if Gnutella closed, other programs such as Freenet or Mnemosyne would take their place.

They deduced that the only solution was to limit the file entries in the darknet via the development of DRM, of “watermarking” (to insert an invisible mark in the file content) and “fingerprinting.” The difference between these two methods is that fingerprinting is more *a-posteriori* control and watermarking is *a-priori*. In the same document, they also talk about the future of the darknets. "The legal future of darknet-technologies is less certain, but we believe that, at least for some classes of user, and possibly for the population at large, efficient darknets will exist."[7] "There is evidence that the darknet will continue to exist and provide low cost, high-quality service to a large group of consumers. This means that in many markets, the darknet will be a competitor to legal commerce."[8]

This last argument suggests that the darknets are not a phenomenon at an end, but a technical means to continue to be developed to ensure their continuation. This hypothesis is confirmed by RAND that believes that there will be "…more activity in darknets, more use of crypto-currencies, greater anonymity capabilities in malware, and more attention to encrypting and protecting communications and transactions"[Rand].

[5] § 2.4.3

[6] § 2.4.4

[7] § 5

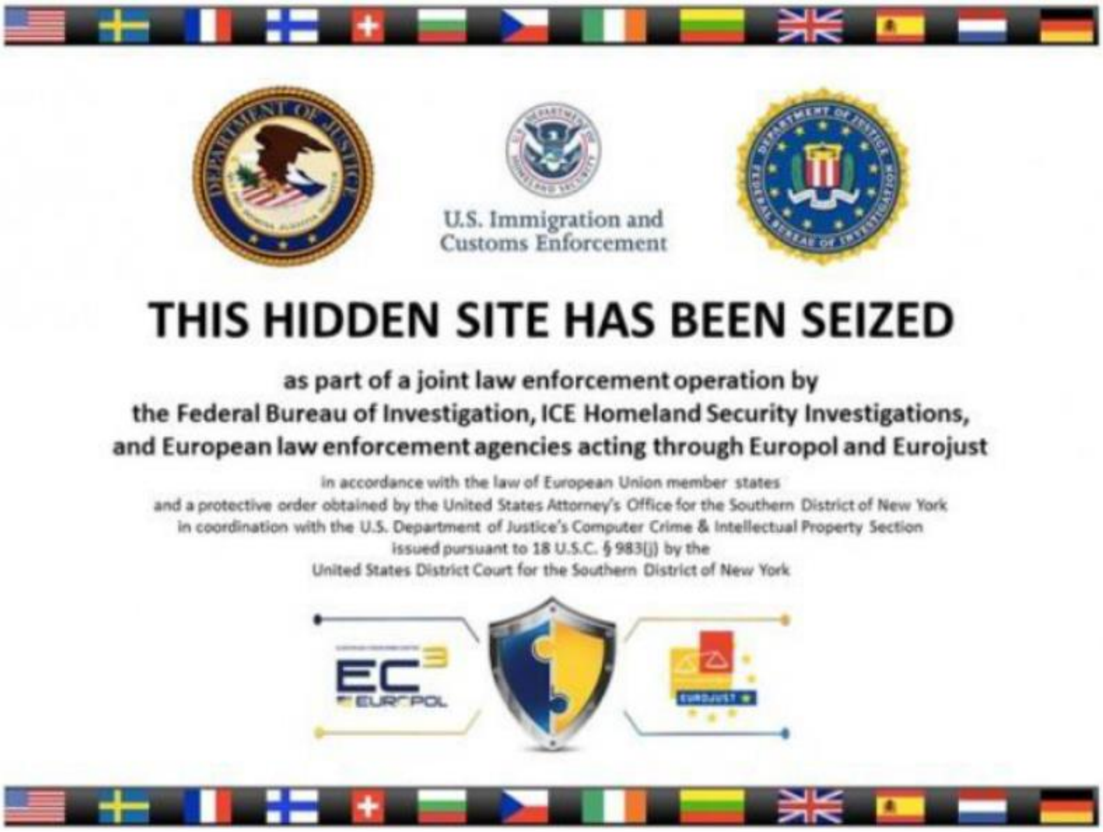
[8] § 5.2

Legal repression

Since darknets will continue to develop, at the cost of technical changes if necessary, it is logical that security forces invite them (to the extent possible) to monitor the activities carried out there. A recent piece by Thierry Berthier and Olivier Kempf [Ber] on cybercrime as a whole, shows that 10% of criminals are responsible for 90% of cyber nuisances. Applying a similar rate to the darknets (10% of their users are responsible for 90% of issues), then it is obvious that the efforts of the security forces will concentrate on certain darknets, in that they cannot close them all at once.

This is what the FBI did when it attacked Silkroad in October 2013 but then there was a resurgence after a while. In November 2014 the Onymous operation carried out by the FBI and Europol managed to close more than 400 sites that were selling drugs and weapons, which baffled Tor developers: was the anonymity of Tor compromised? A Europol spokesman deliberately remained quiet on this issue in order to be able to repeat this type of operation, while Andrew Lewman downplayed the likelihood of the corruption of Tor [WIR3]. A presentation on this subject by Alexander Volynkin and Michael McCord, researchers at Carnegie Mellon University, that was supposed to be given at the Black Hat Conference in 2014 was hastily canceled (the reason for the cancellation was not published) and the Tor team advised software users to use patches [Hil]. The resurgence of Silkroad, enhanced or not with technical changes, shows us a new type of struggle between the justice and the faith

On these occasions, U.S. law enforcement is not withholding when it comes to press releases on victories, as was the case in April 2015 during the dismantling of a network making counterfeit currency [NYT1]. As evidence of their victory, the American authorities do not hesitate to take over the closed site, adding a seizure banner as a well-established practice:



THIS HIDDEN SITE HAS BEEN SEIZED

as part of a joint law enforcement operation by
the Federal Bureau of Investigation, ICE Homeland Security Investigations,
and European law enforcement agencies acting through Europol and Eurojust

in accordance with the law of European Union member states
and a protective order obtained by the United States Attorney's Office for the Southern District of New York
in coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section
issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

Figure 6: Seizure Banner

This does not guarantee the prosecution of a case, even if Ross Ulbrecht, founder of Silkroad, has been sentenced to life imprisonment by a U.S. court. Given the paradox stated above, this struggle may seem strange because DARPA decided to help Tor improve the quality of its services: "DARPA is funding multiple projects focused on improving Tor's hidden services across '1-3 years,' Tor's director of communications Kate Krauss told the Daily Dot via email."[Dd1]. The links between DARPA and Tor are quite close, since Tor will be extensively used in the Memex program[9]: "Ultimately, Memex should provide crawling capabilities in the Dark Web integrating cryptographic functions of the Tor system. It is reasonable to imagine that these strategic functions were good part of the initial specifications of the Memex program whose budget is estimated to be between $15 and $20 million dollars"[Ber2].

We also note that the fight against illegal activities is not only the prerogative of law enforcement. Thus, on October 17th, 2011, the group Anonymous launched Operation Darknet against forty pedophile sites by blocking user accounts of some 1,589 users. It called for all child pornography to be taken off of these sites. As these operations are of course not coordinated with the police and they do not always see a good eye, as law enforcement seeks to gather evidence of crimes to bring perpetrators to justice. This is not cooperation.

Illustration: 7
Operation Darknet

Should we go on the darknets?
Why go on the darknets?

The idea of monitoring the darknets by companies or even infiltrating them is increasingly discussed. The argument to justify monitoring is that companies want to see what is being said about them (in terms of reputation), to detect early signs of an attack, to know whether some of its resources are used in a botnet, and finally to know the means that will be used to carry out a cyberattack. Clearly, the only darknets affected by this monitoring are those that harbor illegal activities. We make this clarification before continuing.

According Adrien Petit, a cybercrime consultant, it is necessary to monitor many communication channels [GSM]:

[9] Cf. http://www.darpa.mil/newsevents/releases/2014/02/09.aspx

- Social networks: for example, cybercriminals that specialize in blackmail from the Rex Mundi group have published documents of their recent victims (Domino's pizza and Labio) on their site .onion;
- The “pasties” databases (pastebin.com, JustePaste.it ...) have, among others things, DDoS instructions, copies of bank cards collected, etc.;
- Other tools are also observed: IRC channels, broadcasting sites, hacking advice forums, and any link to the Dark Web ... Indeed, cybercriminals extensively use these different channels to advertise, make their demands and recruit and also to resell contraband.

Even if this goal seems worthy, the major drawback lies in the fact that these measures are taken *a posteriori* or are beyond the resources of the companies (analysis of pasties databases). They are therefore not very advisable, particularly for SMEs.

However, while monitoring the darknets allows a company to be aware of what is being plotted against it, this monitoring raises several questions:

- how can a company be accepted into a darknet?
- is it sure of the veracity of the data exchanged?
- all illegal information is not transmitted exclusively in the darknets. YouTube is also a platform used for advertising by criminals [CEIS].

Can we trust what we find there?

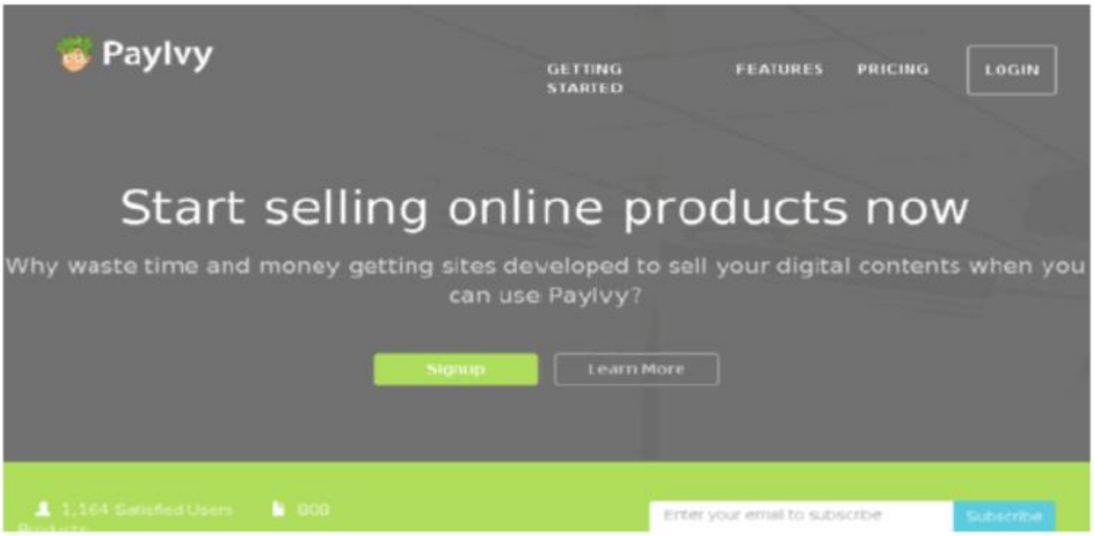
Once admitted to a darknet hosting illicit or illegal content, can we take the information we find there at face value? Before answering this question, we should study the conditions of admission to a darknet. No one can be admitted if he or she did not prove, one way or another, his or her membership to the user community of said network. This is apparent from the RAND study: "Vetting was rare in the early days; it was easy enough for an actor to just want to get involved, and be included. Today, vetting is more robust, and the cost to entry is higher, as takedowns increase and as law enforcement and security companies get more successful at infiltrating the black market"[Rand].

If common sense seems to bring the greatest skepticism, one can also take into account the results of a study conducted by researchers at the *Privacy Security and Automation Lab* of Drexel University (Pennsylvania, U.S.). They looked at cybercriminal forums to find out how criminal organizations function on the internet: "We have tried to answer the question: what does organized crime really mean in cyberspace?" explained Vaibhav Garg, member of the team. One of their findings is (as one would have suspected) that the issue of trust must be addressed. Rebekah Overdof stated "The main challenge to a cybercriminal organization is the lack of trust among peers [Ddig]. Besides "a newcomer is not necessarily free to whatever: he first has to prove his worth and establish confidence, allowing him to climb in the hierarchy"[Ddig]. Despite all these precautions, participants in these illegal activities are not immune to disappointment. In 2015, the Evolution marketplace disappeared after 42,000 bitcoins were stolen. It seems that the robbers were the owners of this marketplace and known by the pseudonyms Verto and Kimble [DD3].

Drexel University researchers have also found that organizations were operating in two different ways, gangs (with a single leader clearly identified) or mobs (with several leaders). In the first case, any profit opportunity is up for grabs, while the mobs are an interconnection of communities and seek to make profit from their activities. We realize then that, even if a company is accepted into one or more darknet it would be difficult to know whether the information collected is reliable, it would also need to know how the criminal organization works so it can predict its targets. There may not have enough time to predict the way they will be targeted. Finally, this study must be looked at in relative terms because the data it is based on came from piracy. It is partial and may not reflect entire criminal networks and their operations on the internet. To take these as entirely true guidelines would be unwise.

Since a high volume of documents of any kind on the internet can quickly overwhelm any human research capacity, one might question of the usefulness of monitoring the darknets. In addition, camouflage terms may add to the complexity of the search: searching without knowing what you are looking for is like trying to find a needle in a haystack.

One should bear in mind that it is not always necessary to visit darknets to get illegal information. The Payivy example (not long ago) reminds us of this, where internet users realized that it was possible to buy pirated PayPal account numbers, while paying by Paypal! "PayIvy has become a major conduit for hawking stolen accounts and credentials." [Kre]



Start selling online products now

Why waste time and money getting sites developed to sell your digital contents when you can use PayIvy?

Figure 8: PayIvy commercial website

Conclusion

The darknet is a neutral private network, in the sense that it is not necessarily malicious. This neutrality should not, however, encourage naivety. There, confidence does not prevail as *a priori*. It is advisable to only venture there only if one knows what one is doing, and there is no guarantee of the veracity of the information found there. The darknets can be compared, in a legal sense, to be a territory held by gangs and criminal organizations: where only guests enter and only because once there something is expected of them.

Simple precaution then would discourage one from venturing there, even in the name of a company: it is not sure that one will get the result they want, and there is a proven risk of compromising the equipment used.

Over time it will be interesting to see how the darknets will be dealt with by legal doctrine. Looking through the lens of the current debates, including theft of digital data and digital identity, it is not impossible that the question arises of whether or not the darknets should be considered a private space in the same way that a hotel room is.

References

[Ake] Aked Symon: “An Investigation into Darknets and the Content available via anonymous peer-to-peer file sharing,” School of Computer and Security Science , Edith Cowan University, Perth Western Australia. 2011

[Ber] Berthier Thierry and Kempf Olivier: “De la cyberveille à la prévision des agressions. Actes du C&ESAR 2014.”

[Ber2] http://www.huffingtonpost.fr/thierry-berthier/enjeux-et-defis-deep-web_b_7219384.html?utm_hp_ref=france

[Bid] Peter Biddle, Paul England, Marcus Peinado and Bryan Willman: “The Darknet and the Future of Content Distribution.” 2002

[CEIS] CEIS: Cybercriminalité et réseaux sociaux: liaisons dangereuses. Janvier 2015.

[Ddig] http://www.diplomatie-digitale.com/featured/surete/influence-reseaux-cybercriminels-1626

[Dd1] http://www.dailydot.com/politics/next-generation-tor-darpa/

[Dd2] http://www.dailydot.com/politics/facebook-tor-explained/

[Dd3] http://www.dailydot.com/crime/evolution-dark-net-black-market-bitcoin-scam/

[Fac] https://www.facebook.com/notes/protect-the-graph/making-connections-to-facebook-more-secure/1526085754298237

[GSM] Global Security Mag: http://www.globalsecuritymag.fr/Dark-Web-visite-guidee-de-la-face,20150420,52388.html

[Hil] Kashmir Hill, “How Did The FBI Break Tor?” http://www.forbes.com/sites/kashmirhill/2014/11/07/how-did-law-enforcement-break-tor/

[Kad] George Kadianakis and Karsten Loesing: “Extrapolating network totals from hidden-service statistics.” January 2015

[Kre] “PayIvy Sells Your Online Accounts Via PayPal,” Available on the site: http://krebsonsecurity.com/2015/05/payivy-sells-your-online-accounts-via-paypal/

[Lew] Andrew Lewman: interview on the site http://www.bbc.com/news/technology-28886465 August 2014

[Moz] https://blog.mozilla.org/privacy/2014/11/10/introducing-polaris-privacy-initiative-to-accelerate-user-focused-privacy-online/

[NYT1] http://www.nytimes.com/aponline/2015/04/02/us/ap-us-counterfeiting-uganda.html?_r=0

[Rand] RAND: “Markets for Cybercrime Tools and Stolen Data,” 2014.

[Red] http://www.reddit.com/r/DarkNetMarkets/comments/22jg6b/darknet_markets_search_engine/

[Wir1] http://www.wired.com/2014/04/grams-search-engine-dark-web/

[Wir2] http://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/

[Wir3] http://www.wired.com/2014/11/operation-onymous-dark-web-arrests/