Why should firms go dark?

A strategic approach to the Tor network
Applied Cybersecurity for Managers
François Courset - Margot Favennec - Candice Hamou

Introduction: For the Web is dark, and full of terrors?

The Dark Web has been fascinating and fueling the imagination of many Internet users for a few years now. The collective art group Mediengruppe Bitnik even created a Random Darknet Shoper, a bot which bought a random object from the darknet market place Agora and then sent it to the two artists in charge of the project¹. This artistic project, aiming at debunking consumerism, showed yet that drugs are not the only things you can find on the Dark Net. You can also find everything you buy in the “clean world”, and buy these with a refund service - the two artists received a refund for a bag that was no longer available.

The Dark Web, instead of being the place gathering the worst side of humanity (drugs, pedophilian contents…) could also thus be a place where a real economy grows and prospers.

That’s why the following question deserves to be asked: can the Dark Web be profitable for firms then? Could a reliable “dark” business model exists and could the dark web be used as a almost regular tool to increase a firm’s profit?

First things first, the Dark Web is often misperceived among the global population since the media hype mainly focuses on scandals such as Silk Road’s.

This tends to depict it as a place where you can find barely anything illegal, from drugs to hitmen. Yet the Dark Web is not only about illegal traffic. It is much more than that.

What’s more, a distinction has to be made, a distinction that is far to often forgotten or neglected.

As shown by the two pictures you will find below, there are different levels beneath the “Surface Web” we all know. First comes the “Deep Web”, where you can find many reports, sTorage datas, and again underneath this Deep Web comes the “Dark Web”, where all communications are encrypted.

Now let’s clarify what each term means:

- **Deep Web**: information not accessible with a regular search engine. It is a Web concept regarding search engine, invented by Mike Bergman in 2000 (*The Deep Web: Surfacing Hidden Value*)
- **DarkNet = Dark Web = Tor =** information not accessible with a regular search engine or a browser

The Deep Web has a far larger content that the Surface Web: 1GO of indexed page versus 550GO of deep web page and 19TB of indexed content versus 7500 TB of deep web content, to quote only but a few numbers from a recent study.

To be really thorough, Dark Nets are all the overlay networks on the Deepweb, and Dark Web is the content of some Darknets. Thus one DarkWeb may be considered as a small portion of Deep Web. Deep Web and DarkWeb are very often confond, yet they are not the same!

We chose to focus on Tor since this is what most people use to get into Darknets and to browse the Web anonomously. Tor enables you to protect your privacy while looking at any webcontent, and from our point of view, this is one crucial asset for a business model based on the use of Darknets.

In the wake of the growing yearn for privacy and of protest against wild data collection, Tor is definitely something firms should get interested in.

1. Going to the dark side: a business opportunity

Not everything on the Dark Web is bad. In an age where NSA-type surveillance is omnipresent and privacy seems like a thing of the past, the dark web offers an anonymity, by not tracking your online behaviour and using cryptocurrencies such as the bitcoin - but we'll get back to this later.

Some companies could benefit from a trip to the dark web.

Of course, companies that are making business from Dark Web-related activities could. The example of the porn industry is particularly relevant: a porn website could open a version in the Dark Web (using only very legal content of course) to make it more attractive to a whole new kind of clients.

But more traditional, classical companies could too: nowadays, the Tor network is being more and more used inside the firms.

- Using the Dark Web for a company

One way companies can use the Dark Web and make the most of it is by actually launching their own platform.

A paper written by researchers at the University of Luxembourg attempted to rank the most commonly accessed materials on the dark Web. What they found was that although sites trading in illegal activities and adult content are very popular, so too are those concerned with human rights and freedom of information.

So although the dark Web definitely has its ugly side, it has great potential, too.
Tor hidden services allow Tor users to offer various Internet services like web publishing or messaging while keeping the location of said services hidden.

The research from the University of Luxembourg showed hidden services in 17 different languages. Content was offered in the following languages besides English (each constituting less than 3%): German, Russian, Portuguese, Spanish, French, Polish, Japanese, Italian, Czech, Arabic, Dutch, Basque, Chinese, Hungarian, Bantu, Swedish.

![Figure 2: Tor Hidden services topics distribution](image)

**Figure 2: Tor Hidden services topics distribution**

*A graph extracted for the results of the work of researchers at the University of Luxembourg*

Not all websites on the Darkweb are like Silk Road - an online marketplace where users could buy drugs, guns and all sorts of other illegal items that was closed in October 2013.

Resources devoted to drugs, adult content, counterfeit (selling counterfeit products, stolen credit card numbers, hacked accounts, etc.), and weapons constitute 44%. The remaining 56% are devoted to a number of different topics: “Politics” and “Anonymity” are among the most popular (9% and 8% correspondingly). In the “Politics” category, one can find resources for reporting and discussing corruption, repressions, violations of human rights and freedom of speech, as well as leaked cables, and Wikileaks-like pages; the category “Anonymity” includes resources devoted to discussion of anonymity from both technical and

---

2 *Content and popularity analysis of Tor hidden services*
political points of views as well as services which provide different anonymous services like anonymous mail or anonymous hosting.

The category “Services” includes pages which offer money laundering, escrow services, hiring a killer or a thief, etc. In “Games” one can find a chess server, lotteries, and poker servers which accept bitcoins.

Tor hidden services are often criticized for being shelter for resources with illegal or controversial content. The arguments used are usually based on services such as “Silk Road” marketplace or child pornography.

On the contrary, Tor enthusiasts point out that many hidden services are in fact resources devoted to human rights, freedom of speech and information which is prohibited in countries with oppressive regimes. Obviously both types of services exist, but it is unclear which type prevails.

And this may not be the only opportunity the Dark Web offers.

- **The blockchain: making transactions faster**

A blockchain is a record, a ledger of all bitcoin transactions that has ever taken place.
It is similar to a ledger that a bank would maintain to record all transactions of their customers. But that's where the similarity ends. In a bank, the ledger is controlled by the bank itself. Only the bank can see the transactions. The bank has its own security and access system to secure the ledger and to enter transactions.

In the blockchain, a copy of the ledger file is shared between thousands of participants globally, also called miners. Even you can become a miner by simply downloading the open source bitcoin software. New bitcoin transactions are added in the blockchain by a consensus of a majority of the miners, explained below. People do mining because they receive new created bitcoins in return for their efforts. Once a transaction is entered in the blockchain, it can never be erased or modified.

Here is an illustration from the Financial Times to explain concretely what is the blockchain:

**Bitcoin** is basically an encrypted digital currency. Like regular cash, Bitcoin is good for transactions of all kinds, and notably, it also allows for anonymity; no one can trace a purchase, illegal or otherwise.

It is the most common currency employed in all Tor hidden-services trade.

Bitcoin may be the currency of the future - a decentralized and unregulated type of money free of the reins of any one government.

But because Bitcoin isn't backed by any government, its value fluctuates, often wildly. It's anything but a safe place to store your life savings. But when paired properly with Tor, it's perhaps the closest thing to a foolproof way to buy and sell on the Web.
Today, the bitcoin and the blockchain are becoming quite interesting to the fintechs, for it is accelerating transactions and protecting transactions from external interference.

In addition, developers have realized that it can help transfer not only money, but also any data. It makes it easy to obtain certificates from state agencies and makes the taxation system transparent: every taxpayer knows where his/her money goes.

The technology has been already used in practice: in Europe, there are applications that allow you to make purchases and take gadgets to maintenance service. IT-enthusiasts use it in the field of Internet of Things.

- **Securing data with the Dark Web**

A few days ago, a hacker was trying to sell over 10 million medical records from American health insurance clients, for 750 bitcoins (that is 508,671 dollars).

This also is one of the reasons companies should use the Dark Web for their business. McAfee estimates that the likely annual cost to the global economy from cybercrime is more than $400 billion. Therefore, knowing the Dark Web may help a business know the most current schemes and types of attacks they are likely to face one day, and that could damage their entire activity and credibility.

In fact, the 3Q 2015 IBM X-Force Threat Intelligence Quarterly Report, released last August, showed the growing dangers of cyber-attacks originating from the Dark Web through the use of the Tor network/browser. The report found that so far in 2015 more than 600,000 malicious events originated from Tor around the world. The United States lead with more than 150,000 malicious events, while countries including Romania, France, and
Luxembourg, have each seen more than 50,000 malicious events originating from Tor in 2015.

A great deal of these losses could be avoided, especially by having a notion of what the hackers are actively looking for and how they could access it.

What's more, knowing what is already out there in the Dark Web can be useful for businesses.

Data in the Dark Web is hard for search engines to see, but unseen doesn't equal unimportant. There is immense value in the information tucked away in the Dark Web.

The fact is that if you are looking for a newspaper article that published a long time ago on a newspaper that isn’t the New York Times or the Guardian – that is to say not a very very popular newspaper, you probably won’t find it with the search engines you usually use. But if you try on Tor, maybe you will.

The Dark Web – as well as the Deep Web – is an endless repository for a mind-reeling amount of information. There are engineering databases, financial information of all kinds, medical papers, pictures, illustrations... the list goes on, basically, forever.

Nonetheless, the use of the Dark Web and the Tor network should be carefully monitored. A firm should therefore develop a comprehensive corporate policy for the acceptable use of networks such as Tor. If an industry requires the use of Tor-like networks – journalists, law enforcement, cyber-security professionals – they should make sure that there is a complete corporate policy in place so employees understand how and when they can access these networks. Not every employee in the company need this access, so having a policy in place with limited approvals can lower the risk of threat and make it easier to track activity.

2. The dark side of the media: a way to free information?

Tor is a crucial asset for the media. Its very use indeed matches perfectly the core values of this area. Liberty of the press, liberty of information and information for all are actually three founding principles of the media that Tor could help implement. The growing yearn for free and transparent information - as shown by the Wikileaks, LuxLeaks, and other scandals and the regain of support for all whistle blowers - is moreover a trend the medias are trying to follow. The dark net is thus a topic they should tackle very seriously.

- Medias under censorship: Tor as a convenient and reliable tool to protect both readers and publishers
For people living in countries like China, Tor can be seen as a way to avoid censorship issues. Indeed, dictatorships watch very carefully their inhabitants’ browsing habits, making it almost impossible for the latest to visit censored or “subversive” - at least according to their very own definition - websites.

A person fearing to get caught while seeking unbiased information on the net can indeed be protected by the Tor network. Some news websites have thus developed a Tor version for those willing to stay anonymous while browsing through their website.

**ProPublica**[^3] is a good illustration of this trend: in 2015, this free information website decided to go dark in order to provide best information quality to everyone willing to have it no matter censorship. The users now have to download Tor and then use it to be able to browse on ProPublica anonymously.

In the same vein, **WikiLeaks**[^4] has some content on the Dark Web.

On its homepage for a traditional browser, you will see this:

![WikiLeaks homepage](https://www.wikileaks.org/)

“The following method requires some technical ability. If you are used to installing new software and configuring proxy servers you should have the required skills, otherwise you may wish to use one of our other submission methods. Don't let the technology defeat you!

[^3]: https://www.propublica.org/nerds/item/a-more-secure-and-anonymous-propublica-using-Tor-hidden-services
Tor, or The Onion Router, is a cryptographic technique first implemented by US Navy research to permit intelligence agents to use the internet without being traced, by encrypting and routing communications through many different internet servers. Subsequently, Tor has been developed by the US university MIT and by the California internet rights watchdog the Electronic Frontier Foundation and subsequently incorporated into Wikileaks.

Using our anonymous access package (see below) you can prevent internet spies knowing that your computer has connected to Wikileaks.

Most Wikileakers do not need this extra security, and there are simpler and possibly safer alternatives for once-off high-risk leaks (see Submissions). But for those who are at risk and want to access Wikileaks from the comfort of their homes or offices or need to bypass Internet censorship, Tor (Onion Routing) is an excellent solution.

**When you have installed** our Tor access package (see below), you may then connect to Wikileaks via our anonymous address (the ".onion" is short for "Onion Routing", but you do not need to be concerned with this detail). *NB: the original .onion link for browsing Wikileaks is currently unavailable; however, if you have installed Tor and are redirecting all of your browsing through the Tor network, you can still browse the normal WikiLeaks site with a high degree of anonymity (but not end-to-end encryption). The secure .onion address provided here and on the submissions page should still work, in any case."

We can see that Wikileaks, a website famous for the scandals with Julian Assange, its founder, relies a lot on Tor.

For committed newspaper, Tor is a huge opportunity.

Using Tor to publish satirical articles or caricatures would protect the artists and writers from being tracked down. For a new satirical newspaper, starting on the dark net first would probably be safer while the terrorist threat remains significative.

Outside the political area, Tor can be used by anyone who wishes to protect its privacy on the web while publishing articles. *The TorISt*⁵ is a good illustration of this trend. This literary newspaper has been launched this year on the Dark Web by Gehl and GMH, two persons advocating a casual use of the Tor network. They wanted to show that the dark side of the web is not only a place to buy drugs and porn but also - and especially - a place where you can browse any website and publish what you want to while protecting your privacy.

---

The TorIST has gained huge support among Dark Net users and a French complete version is soon to be developed\(^6\). This newspaper and its success show that Tor can be profitable for medias who decide to use it.

- **How to gain traffic and regild your image: recruiting customers through Tor**

From a more profit-centred point of view, Tor can be a massive promotional tool for newspapers accused to be too biased or too soft. By saying they are on the dark net, they would prove they really care to provide information to those who can’t have it on the “clean net”.

They also show, by going on the dark web, that the personal information of the user will be used by the very website of the newspaper only, which make the user feel safer and more likely to browse on this website than another. A recent survey showed that only 3.5% of people using Tor were using it to go on the dark web, most people only use it to preserve their privacy and browse through “regular” websites. We can thus assume that there is a large pool of Tor consumers (96.5%) would be interested in browsing the website of a firm.

that created a "onion" version. Those living under censorship represent a huge demand for free and unbiased information. If the media decided to advertise towards those people and to make them aware of the fact that they provide them with the same information as the uncensored part of the world on a "onion" website, they could gain traffic very fast and this would regild their image.

The media firms using Tor would indeed appear as real providers of information for all, and as firms really paying attention to the fact that some people do not have any access to unbiased information.

Regilding their image to the global population would motivate more people to visit their websites, and this would - best-case scenario of course - basically turn into a profitable virtuous circle, both on the reputation side and on the profit side.

Whether it is an ideological initiative or a promotional stunt, this could regild the firm’s image and make the traffic rise on the actual “traditional” website.

3. Facebook: a new business model?

Among all cases of media opening a "onion" version of their website on the Tor network, there is one that might have a way bigger impact on all the web ecosystem.

On October 31st 2014, Alec Muffet\(^7\) announced the launch of the "onion" version of Facebook\(^8\). The goal is to provide Facebook users already using the Tor browser to access Facebook, an end-to-end encrypted tool.

\(^7\) Muffet, A. (2014). Blogpost: Making Connections to Facebook More Secure
\(^8\) https://facebookcorewwi.onion/
This may seem paradoxical, regarding public opinion on Facebook privacy values, but as Runa Sandvik explains⁹:

“No, you’re not anonymous to Facebook when you log in, but this provides a huge benefit for users who want security and privacy […]. You get around the censorship and local adversarial surveillance, and it adds another layer of security on top of your connection.”.

To sum up, through the “.onion” address, Facebook guarantee its users that their personal data will only go into Facebook-owned servers.

This shift from such an Internet giant has huge consequences. As we mentioned before, the social network clearly hopes to draw more traffic to its website and to get rid of its bad reputation regarding privacy. Yet, it also brings along a new conception of security on the Internet.

Indeed, with this Tor-accessed version, Facebook becomes the first “.onion” website to have an SSL certificate. SSL certificates are used to establish a secure encrypted connection between a browser (user's computer) and a server (website). The SSL connection protects sensitive data, such as credit card information, exchanged during each visit (session)” (Digicert). It guarantees users that the websites they are browsing are owned by regular and trustworthy organizations. However, a SSL certificate alone does not guarantee users anonymity.

Accessing websites through the Tor browser adds this very layer of anonymity even if, until now, there was no guarantee that the website was an official one and not a phishing platform. With Facebook being the first company to get an SSL certificate for an “.onion” website, Tor can now be seen as a safe tool to surf on the dark web. Therefore coupling “.onion” and SSL allows an end-to-end security and privacy, SSL certificates even raised Tor’s quality of encryption from a 1024-bit to a 2048-bit encryption. Facebook has thus brought out a new way of considering user’s security on the Internet.

Runa Sandvik even considers that “Tor may be the next basic privacy protection Silicon Valley companies will be expected to offer their users”. Indeed, web users are facing the exponential growth of websites collecting their personal data to develop personalized recommendation systems, targeted advertising and so on.

“Big data” have become one of the main insight of companies, yet, legal frameworks are struggling to keep up with the pace. As a consequence, users are claiming for more data privacy. This trend explains the growth of Tor traffic as much as the success of a countless number of privacy-oriented apps. In the future and following Facebook, a lot a tech-giants might be interested in fulfilling this need for confidentiality by providing optional anonymity to its users. Adding the “.onion” address to the already widely used SSL certificate appears to be a convenient way for them to address this data-privacy concern.

---

⁹ Sandvik, R. (2014). Wired "Why Facebook Just Launched its own 'Dark Web' Site"
As for now, the traffic on the Tor network being a minority, it can be a tempting alternative to open discussions about data collection and analysis methods like Apple did.

However, as the dark web allows users to hide basically anything that is related to their identity but also cookies or ads, it might appear as the marketers’ worst nightmare. In fact, nearly everything that can be used to develop custom services or advertising is impossible on the Dark web.

This is particularly puzzling to see Facebook daring to dive into the Dark web. Its business model is mostly based on how well they know their users to develop targeted ads. So why did they choose to abandon a part of this knowledge?

In fact, as users still log into their personal Facebook account, the social network still has a clear vision of who they are. As we explained before, when using the dark web version of Facebook, it knows everything about you but others cannot. This is particularly relevant regarding data collection based on other websites. For example, companies such as Amazon are able to adapt their offer depending on what you have searched for on the web. This data comes from cookies that allow companies to track what a user has been doing on the web up to 30 days.

Currently cookies and external data are not crucial in the way Facebook work, even if their recent announcement to extend their advertising to external websites might be the beginning of a shift. However, a huge number of websites are using Facebook data to customize their offers. Through the launch of the “.onion” version, Facebook claims that its data can be auto-sufficient, but also makes emerge a new way of trading data. In the case of Tor users accounting for a majority of the traffic, websites which want to have Facebook information to target their offers will have to directly ask Facebook.

As Alec Muffet twitted:

Yet, for websites that own valuable information about their users, it can be a huge opportunity to increase the selling value of these data. It is the case for Facebook, but also for every kind of Social networks.

Nevertheless, these transformation of the economy of data will only occur if the Tor network traffic tends to be consequent or if a large number of widely used websites open their own “.onion” address. Yet, decision-makers still need to keep an eye on the dark web as it can entail opportunities for them.
What you should remember from what we covered

The dark web should be considered by companies for various reasons. It offers a large panel of useful tools that can be crucial for negotiation or security. Moreover, even if it can appear as a niche network, opening an onion version of the companies' websites might help them to boost their image. It can also bring new users to the website, users that usually cannot reach it because of censorship issues. Finally, we have seen new emerging trends related to the dark web. The Tor network might be seen in the future as a guarantee of security online but it can also deeply change the way data are used.

Taking into consideration the dark web, not only as a place of illegal activities, but also as a new channel with its own opportunities and constraints is thus essential for all decision-makers.