

# 11

## Using the Dark Web for Your Business

In the previous chapter, I enumerated case studies and use cases of the Dark Web. As you've seen, there are many ways that people use the Dark Web.

One might say that you can use the Dark Web in the same way as you use the Surface Web, while the main difference is which browser you use to access the sites: searching for information, consuming content (music, audio, video, written content, and more), participating in social networks, posting content, and communicating.

Also, if you access to the Dark Web in the proper manner, you will be anonymous and able to protect your privacy, something that is much harder on the Surface Web, due to its design and architecture (and use—think about targeted ads, for example).

In this chapter, I'll be focusing on business uses of the Dark Web, and maybe provide readers with insights on how to utilize the Dark Web for their own organizations. My goal in this chapter is to provide ideas and use cases that can benefit businesses, based on common and personal experience.

The anonymity and privacy that is gained by using Tor or any other *Dark Web browser* allows businesses to perform actions that would otherwise expose them and the information they were looking for, thus even harming them financially or their good name.

In this chapter, we will be talking about the following types of users who access the Dark Web for different purposes:

- IT professionals
- Law enforcement agencies
- Business companies
- Military organizations
- Cybersecurity professionals

## IT professionals

I'll start with IT professionals. They are usually the closest to the Dark Web, and feel the most comfortable accessing it, either because of their vocation, or simply out of curiosity.

They know how to use the tools that allow safe access to the Dark Web, such as VPNs and Tor.

Many IT professionals need to access materials on the internet for their work, which may violate strict company procedures, such as not being allowed to access site X using organizational browsers. This is a tricky situation, since they can't perform their work without violating the procedure/policy.

This is a type of catch-22.

To resolve this, IT professionals can use the Tor Browser (or other *Dark Web browsers*), which won't alert the organizational security systems of this action, due to the way Tor works.

Additionally, if the IT professionals do this on a regular basis, they usually have a dedicated machine ready for Dark Web access, which also minimizes their risk of exposing the organization (monitoring search terms helps attackers' information-gathering, so if they can't monitor the searches, this minimizes the attack surface), which would naturally clash with the original intent—preventing organizational information from leaking while attempting to collect important information. These dedicated machines would have a secure OS installed on it, such as the ones we discussed in previous chapters, have a VPN installed, and all traffic would be configured to go through Tor.

They can also use Tor to verify their IP-based firewall rules, such as to test rules that allow or block specific IP addresses or ranges. The IT professionals can use Tor to verify that the rules are effective, since it doesn't use an IP from the organizational ranges. This can be done in a variety of scenarios—checking whether external IPs have access to internal resources, checking whether organizational **Network Access Control systems (NACs)** are working effectively by preventing access to organizational resources from IP ranges that aren't in the organizational pool, or even by preventing access from MAC addresses that aren't recognized by the organization.

Sometimes **Internet Service Providers (ISPs)** have network issues, such as problems with DNS resolution or routing issues, so if this happens, IT people can use Tor to access resources on the internet, providing business continuity.

In the same manner, an IT professional can connect to services without having to use an external machine or account. This depends on the nature of the network issue, of course. Not all of these issues can be overcome by using Tor, but many can, so be aware and always assess the situation.

Many business people access the Dark Web, using Tor, for many reasons, for example to view competitors' websites without being affected by any rules that are in place on the website, such as displaying misinformation to machines accessing it from specific IP ranges or sources. As you know already, Tor obfuscates the IP of the source machine, preventing detection, and allowing the user to access resources, both on the Dark Web and the Surface Web, with a very low chance of detection (if precautions are taken, of course).

The Dark Web is a treasure trove of hidden or raw data. So, companies research scientific and business topics there, providing valuable insights on their business, their customers, and their competition. The data there is usually unfiltered, and unbiased, which helps them to make more informed decisions.

## **Business companies**

Many organizations create security-breach information repositories (clearinghouses) to collect information about breaches and breach attempts. Then they correlate the information and try to detect patterns or definitive information, which will allow them to better protect themselves, mitigate risk, and alert internal security teams, or even similar companies, to these attacks.

Also, these repositories are prime targets for attackers, so managing them on the Dark Web provides protection from detection and exfiltration of the information and their source IPs.

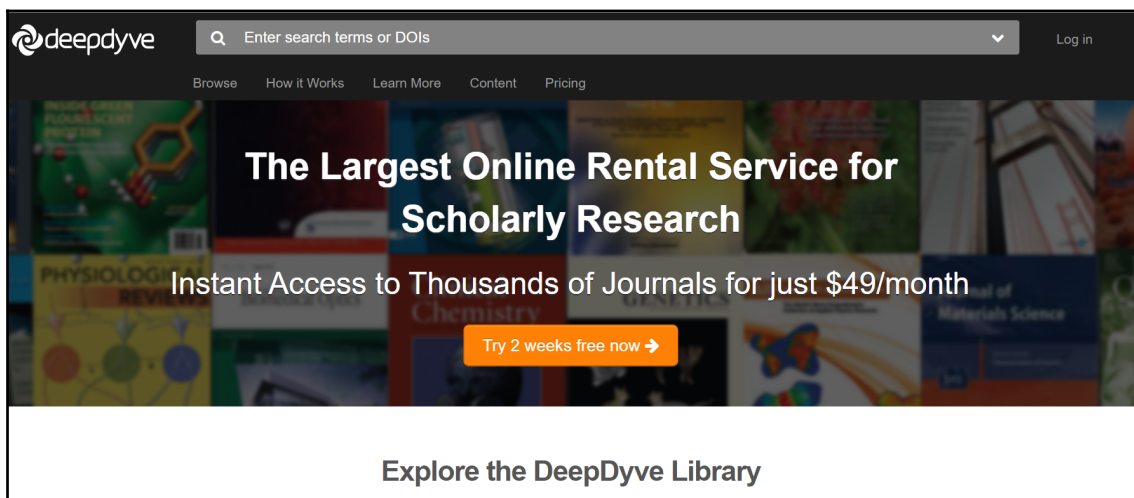
Organizations that are employee-focused use the Dark Web as a place in which employees can report to management on irresponsible or illegal activity performed inside the organization, without fear of repercussion.

Many companies also have analysts who monitor various websites for information that can help them. Naturally, they don't want their competitors to detect what they're watching (to prevent industrial espionage) and to compile patterns or information about them, so they use Tor for this.

We've been focusing on the Dark Web, but it's important to remember that there's a lot of information also on the Deep Web, located in organizational databases and systems, which are simply not indexed by search engines, and which can be accessed by either using a dedicated search system, or by signing up and logging into the organizational systems.

Several such examples are as follows:

- **DeepDyve:** A site that aggregates millions of scholarly articles, only accessible if you sign up:



- **Academic Index:** A site that provides access to Deep Web academic sites:

[About Us](#) [Contact Us](#) [Read our Blog](#) [Search Tips](#) [Citation](#) [Testimonials](#)



# academicIndex.net





### Search Additional Multidisciplinary Web Portals

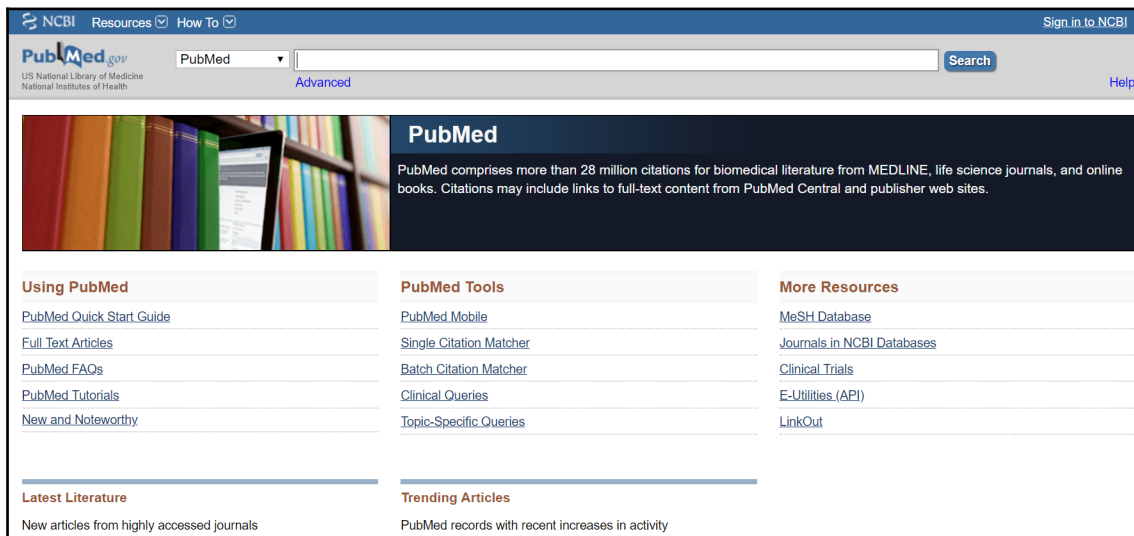
Note: Select/Deselect a portal to search.

<input type="checkbox"/> Bielefeld SE	<input type="checkbox"/> ERIC	<input type="checkbox"/> Archive Grid	<input type="checkbox"/> DOAJ	<input type="checkbox"/> RefSeek
<input type="checkbox"/> Chabot College	<input type="checkbox"/> GovInfo	<input type="checkbox"/> IntechOpen	<input type="checkbox"/> OAJSE	<input type="checkbox"/> Virtual LRC
<input type="checkbox"/> FOIA Data	<input type="checkbox"/> UK Statistics Authority	<input type="checkbox"/> JSTOR	<input type="checkbox"/> OpenDoar	<input type="checkbox"/> Science Advisor
<input type="checkbox"/> Jurn		<input type="checkbox"/> LibGuides	<input type="checkbox"/> Ref. Repository	


- **Sciencegov:** A site with scientific articles collected from US government agencies:



- **PubMed:** The US National Library of Medicine's database:




- **Law Library of Congress:** Claims to be the largest collection of legal materials in the world, with over 2,000,000 volumes available:




[ASK A LIBRARIAN](#)
[DIGITAL COLLECTIONS](#)
[LIBRARY CATALOGS](#)

[The Library of Congress > Law Library of Congress](#)


LAW.gov




- [Law Library Home](#)
- [About the Law Library](#)
- [Research & Reports](#)
- [Find Legal Resources](#)
- [Educational & Research Opportunities](#)
- [Visiting the Law Library](#)
- [News & Events](#)
- [Contact](#)




**Congress.gov**  
 A mobile-friendly, faceted search for U.S. legislative information.




**Congressional Record App**  
 The official record of the proceedings and debates of the U.S. Congress.




**Law Library Highlights**



Try the New Experimental Congress.gov Chrome Browser Extension



Hurricane Maria and Its Lessons on Preservation



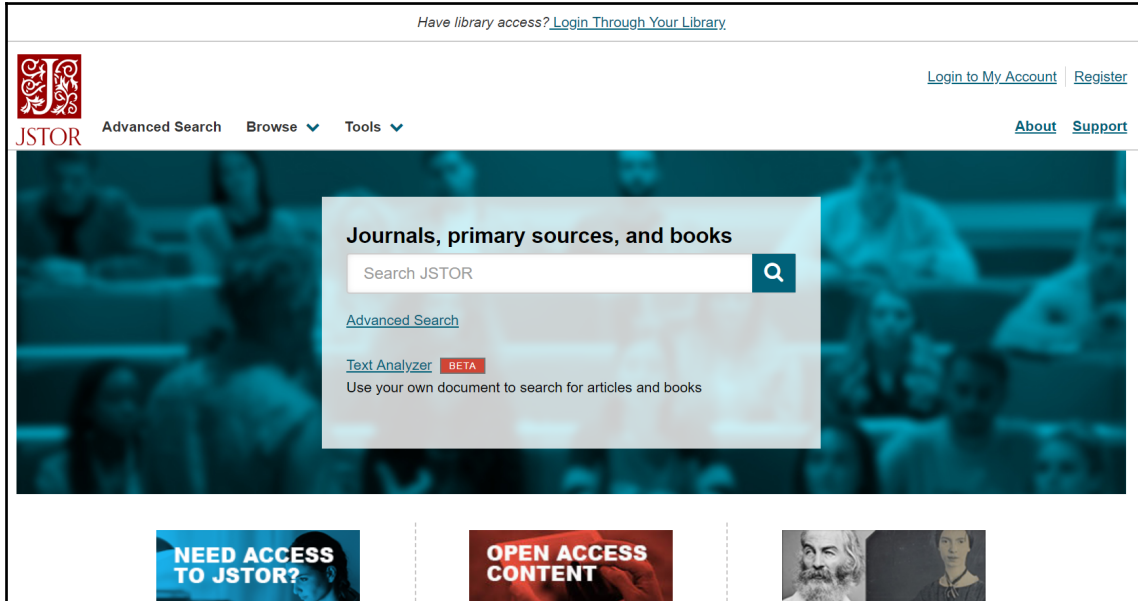
The Murder of Penowanyanquis and the Trial of Arthur Peach, Plymouth, 1638

**U.S. Legislative Information**

**Law Library Hours**  
**Public Hours**  
 M-F, 8:30 a.m. to 5:00 p.m.  
 Sat., 8:30 a.m. to 5:00 p.m.  
  
**Location**  
 101 Independence Ave, S.E.  
 Washington, D.C. 20540  
 James Madison Building (Room 242)  
  
**Phone**

[ 175 ]

- **JSTOR:** One of the oldest online libraries. Members receive access to more than 12,000,000 academic journal articles, books, and primary sources in 75 disciplines:



But there are many many more, of course.

## Law enforcement agencies

As I wrote before, law enforcement agencies have a strong presence on the Dark Web. The officers working for these agencies can engage in undercover sting operations to capture criminals and other people engaged in illegal activity. Using Tor provides anonymity and hides the source IPs of the officers' computers, which otherwise would have blown their cover.

In the same manner, law enforcement agencies perform discreet online surveillance of services and websites without revealing themselves, by using Tor.



In order to better explain how law enforcement can operate on the Dark Web, I'd like to tell you about Operation Bayonet, a Dutch-led sting operation, to take down Hansa, a Dark Web market site, numbering 3,600 dealers offering more than 24,000 drug product listings, as well as fraud tools and counterfeit documents. They were able to monitor Hansa's buyers and sellers, using various tools and methods, and discreetly altered Hansa's code to grab additional information, which helped identify those users, and even tricked many of Hansa's anonymous sellers into opening a file on their computers that revealed their location to the investigators. During the investigation, both Surface and Dark Web capabilities were exploited by the investigators, using the anonymity provided, to discover Hansa's development server, where new features were tested before deploying them to the live site, taking control of it, and through it, finding the live site servers.

They copied the server's drives, including records of every transaction performed, and every communication that took place through its anonymized messaging system. This led them to discover the founders' IRC chat logs, which surprisingly, included the administrators names and even their home addresses.

Even though you might think that the operation ends here, there's more. The Dutch investigators wanted to try to capture vendors selling illegal goods through Hansa, so rather than arresting the site administrators immediately, they waited. This caused a setback in the operation, as the Hansa servers they had found vanished, but the site kept on working. They understood that they'd been discovered by the site admins. Rather than admitting defeat, the investigators invested months in going over all the evidence they had collected so far, and in April 2017, got a lucky break—a bitcoin payment had been made from an address that had included in the IRC chat logs they had discovered. By using blockchain-analysis software, the bitcoin payment provider was found to have an office in the Netherlands.

The police contacted the bitcoin payment company and obtained information about the payment recipient—a company in Lithuania.

Again, as fate would have it, the investigators paused before closing down the site, following a meeting with the FBI, who told them that they would be shutting down AlphaBay, one of the most popular drug markets on the Dark Web at the time.

This would cause the vendors and buyers to look for a new marketplace, and it would probably be Hansa. The Dutch police understood that this would put them in a position to apprehend many more drug dealers and people selling illegal goods than if they'd just shut down Hansa. They'd also be able instill a feeling of distrust in the safety of Dark Web markets, and that the law would be able to get them anywhere, even on the Dark Web.

In a joint action, German police arrested the two people suspected of being Hansa's admins, and were able to seize their hard drives. Then the Dutch police migrated the Hansa server's data to their own servers, effectively taking control of the site.

They then proceeded to rewrite the site code, logged the user's passwords, and unencrypted the messages on the site, discovering many buyers' home addresses.

They also removed a feature that anonymized photos, causing user metadata to remain embedded in the files, providing geolocation information that led to locating more than 50 drug dealers.

Files that acted as homing beacons were sent to sellers, designed to look like a backup key for bitcoin received on the website. Opening the file connected the sellers' devices to a specific URL, uncovering the sellers' IP addresses.

After Alphabay was closed in July 2017, over 30,000 drug buyers registered on Hansa, falling under police surveillance. The amount of newly-registered users became so great that the police stopped registration for nearly two weeks.

After 27 days of collecting information about the people buying and selling on Hansa, the Dutch police shut down the site, leaving a notice to anyone who might try to access it:

*"We trace people who are active at Dark Markets and offer illicit goods or services," the site read. "Are you one of them? Then you have our attention."*

Dozens of arrests were performed, over \$12,000,000 in bitcoin was seized, in addition to the effect that it had on the Dark Web criminal element.

Also, in a massive sting operation in the US, law enforcement agents from a multiple state departments—including the Department of Justice, Homeland Security Investigations, the US Secret Service, the Postal Inspection Service, and the **Drug Enforcement Administration (DEA)**—apprehended and arrested over 35 dark web traders across the country, by posing as traders and vendors themselves.

Additionally, to ensure anonymous tips, posting them on the Dark Web, or even just using Tor, will keep the reporters anonymous.

## Military organizations

Military organizations use the Dark Web for covert communications, protecting military actions, operations, and adhering to military information security procedures (such as non-disclosure).

It also allows military, governmental, and civilian intelligence, and counter-intelligence units to collect information without revealing themselves to the subjects of their research.

As you now know, the internet was originally designed and launched by DARPA, to ensure continued communication in case of attacks on the US, and to hide the physical location of the communicating objects, Tor was developed, based on this, and further ensures the above.

In an attempt to combat the use of the Dark Web for sex trafficking, DARPA built a search engine called Memex to try to find information and leads from the Dark Web.

It cost DARPA \$67,000,000, and is in use by over 33 law enforcement agencies since 2014. It looks for online behavioral signals in ads and helps detect whether a person is being trafficked.

Even though it's extremely hard to collect information about a person on the Dark Web, signals exist in data, in online photos, and even in the text of ads.

Intelligence capabilities compare the information it collects to behaviors associated with trafficking, trying to understand the human trafficking footprint in online spaces.

*"Our goal is to understand the footprint of human trafficking in online spaces, whether that be the dark web or the open web." – Wade Shen, a program manager in DARPA's Information*

## Cybersecurity professionals

Cybersecurity professionals also use the Dark Web. They monitor sites, forums, and blogs, where hackers exchange information regarding new exploits and hacks, companies or individuals they've targeted, and more. This provides them with threat intelligence and insights into emerging threats, thus enabling them to better protect their organizations.

There are also many systems that collect threat intelligence, some collecting information from the Dark Web, such as Silobreaker, Webhose, RepKnight, Terbium labs, Massive, Recorded Future, Sixgill, Hold Security, and AlienVault, which provide information about new malware and exploits and also allow the user to detect whether there's jabber about a person or company, by searching for a credit card number or a social security number, among other capabilities. This allows them to detect new vulnerabilities and exploits, and also receive insights as to whether companies are being targeted or were hacked and had their information leaked.

If you remember, I mentioned that Facebook and other sites have a Dark Web presence. The business advantage is providing access to their services and business to citizens in countries where these types of sites are blocked, thus enlarging their customer base (and ultimately making more money).

## Summary

In this book, we discussed how to access the Dark Web, the who, and the why.

You've seen that it's used for the best of reasons, and the worst...

As with all technology, it's neither good nor evil; it's how the technology is used that makes the difference.

The Dark Web is very similar to the Surface Web. The main difference is the anonymity and privacy, which are more pronounced on the Dark Web.

In this chapter, I tried to show you that the Dark Web can be very beneficial, and that law enforcement is working diligently to protect us, both off and on the Dark Web.

I hope that you see, as I do, the advantages of the Dark Web, rather than its dangers or disadvantages.

Use it, but on your own terms. Use it safely, use it wisely, and ultimately, it should benefit you.

Maybe renaming it to something less ominous might change the perception most people have of it, but as Shakespeare wrote, What's in a name?

## Questions

1. What was the Dutch police's sting operation called?
  - A. Operation Saber
  - B. Operation Bayonet
  - C. Operation Switchblade
  - D. Operation Turnover
2. What do some tools look for on the Dark Web?
  - A. Artificial Intelligence
  - B. Business Intelligence
  - C. Threat Intelligence
  - D. Basic Intelligence
3. What advantages does the Dark Web offer to IT professionals?
  - A. Accessing information that is located on sites which are usually blocked
  - B. Testing security systems and firewall rules
  - C. Overcoming network issues such as routing or DNS resolving

## Further reading

The following resources might be of interest if you'd like to dive deeper into the subjects covered in this chapter:

- [https://en.wikipedia.org/wiki/Operation\\_Bayonet\\_\(darknet\)](https://en.wikipedia.org/wiki/Operation_Bayonet_(darknet))
- <https://darknetdiaries.com/episode/24/>
- <https://go.recordedfuture.com/dark-web>