8

An Evolving Threat

The Deep Web

Learning Objectives

1. Explain the differences between the deep web and darknets.
2. Understand how the darknets are accessed.
3. Discuss the hidden wiki and how it is useful to criminals.
4. Understand the anonymity offered by the deep web.
5. Discuss the legal issues associated with use of the deep web and the darknets.

> 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 (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 in cash, drugs, gold and silver were seized.
>
> **—Europol, 2014**[1]

THINK ABOUT IT 8.1

Surface Web and Deep Web

Google, Facebook, and any website you can find via traditional search engines (Internet Explorer, Chrome, Firefox, etc.) are all located on the surface web. It is likely that when you use the Internet for research and/or social purposes you are using the surface web. The surface web only accounts for about 4% of all the Internet—the rest is found on the deep web, sometimes also referred to as the deep net. The deep web is not accessible through traditional search engines. In order to access the deep web, special considerations are needed, including private URL addresses or, for some areas, darknets (specialized software).

What Would You Do?

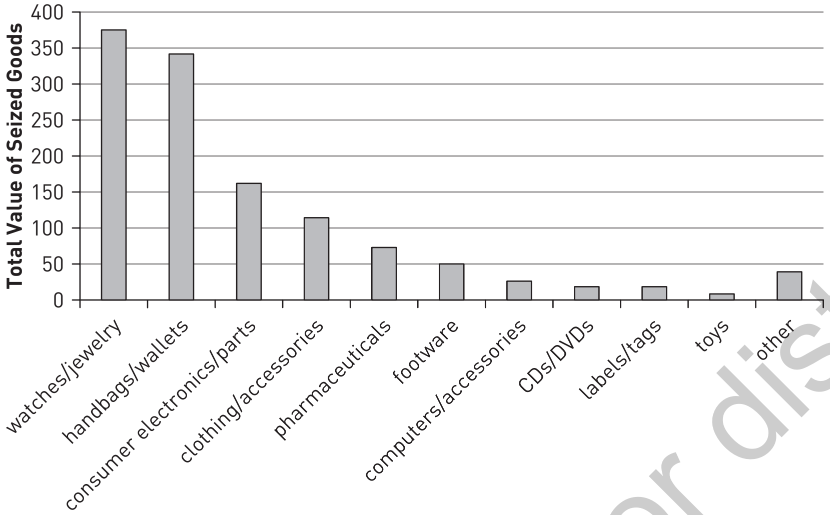
1. The deep web offers users an anonymity that the surface web cannot provide. What would you do if you knew that your electronic footprints could not be traced?
2. Why would this be appealing to criminals?
3. What problems does anonymity create for law enforcement and other criminal justice professionals?

The Surface Web

Before discussing a seemingly unknown aspect of the Internet, it is necessary to define what the majority of users consider to be the Internet: the surface web, or the public web. Like its name, the surface web contains any and all websites accessible via traditional search engines, such as Google. The surface web is accessible to anyone with Internet connection and is hosted by browsers such as Internet Explorer, Firefox, and Google Chrome. According to some sources, there are over 4 billion indexed web pages on the surface web; however, many search engines do not have the capacity to access all pages.[2] On average, Google accesses 16% of the surface web, while other search engines are able to access even less.[3]

Criminals do operate on the surface web but are more vulnerable to being discovered than if they operate on the deep web. Examples of crime on the surface web include the stealing of personal information and data for financial gain. However, even more deceptive are surface websites that operate as legitimate businesses but are marketing counterfeit goods. As illustrated in Chart 8.1, millions of dollars in counterfeit goods are seized every year by the U.S. government. Much of this is sold online via websites that are constantly changing their Internet protocol (IP) addresses. Unknown to the buyer, the goods are counterfeit and are being sold illegally, taking advantage of the easy access online shopping provides.

CHART 8.1 ● Counterfeit Goods Seized by the United States: 2014



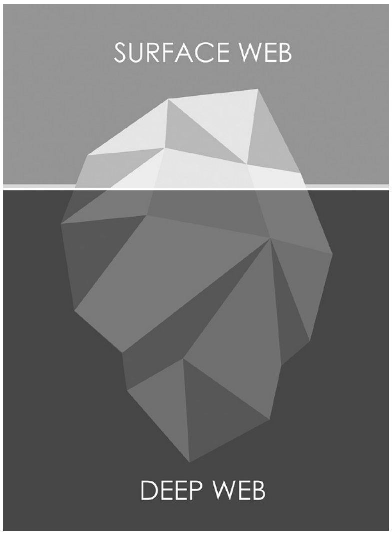
Source: Based on data from Bain, M. (2015). *Counterfeit watches and jewelry are the new counterfeit handbags*. Retrieved from http://qz.com/376249/counterfeit-watches-and-jewelry-are-the-new-counterfeit-handbags/.

The Deep Web and Darknets

Although the surface web seems vast and infinite, it is only a small piece of the Internet compared to the deep web. The surface web is often compared to the tip of the iceberg (see Figure 8.1) of the Internet, as the deep web is 400 to 500 times bigger than the surface web.[4] Moreover, there is an anonymity associated with parts of the deep web, specifically on the dark web. There is much confusion between the deep web and the dark web. These terms are often used interchangeably, but these two areas are not the same. The dark web is just a small portion of the deep web. Both are inaccessible from the surface web, and many general Internet users are unaware of their existence.

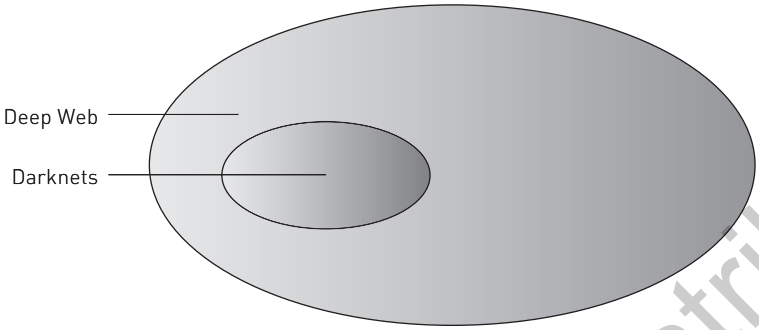
The deep web consists of all data behind firewalls. Surface websites use “crawlers” to browse the web in a systematic and automated manner. Deep websites cannot be found via these crawlers. Deep websites can include passcode protected websites, websites that are not searchable, sites that are not linked to other programs (in which the URL must be typed in), medical databases, business Intranets, and darknets (dark web).[5]

FIGURE 8.1 ● Surface Web Versus the Deep Web



© iStockphoto.com/traffic_analyzer

FIGURE 8.2 ● Deep Versus Darknets (Dark Web)



Darknets (also referred to as dark web) make up a small part of the massive deep web (see Figure 8.2), and this is where the majority of criminal activities on the deep web occur. There are two main forms of darknets: peer-to-peer networks (used for file sharing) and large anonymous networks.[6] We concentrate on the large anonymous networks in this chapter.

Due to the anonymity provided, many criminals may feel more comfortable operating in the darknet market than on the surface web or even in the physical world. One reason for this is the lack of law enforcement presence on the deep web. It is extremely difficult to track the digital footprints of criminals on the deep web (see Chapter 9 and the discussion of guardianship for more). Another reason for the high prevalence of criminal activity on the deep web is the ease of accessibility.

Accessibility

Accessing darknets is relatively easy, although it cannot be done via surface web search engines (i.e., Google). There are multiple portals for the darknet, including Freenet, I2P, and The Onion Router. To access the darknet, one must first download one of these platforms. Freenet describes itself as "a peer-to-peer platform for censorship-resistant communication and publishing. Browse websites, post on forums, and publish files within Freenet with strong privacy protections."[7]

The Invisible Internet Project (I2P) advertises that "The I2P network provides strong privacy protections for communication over the Internet. Many activities that would risk your privacy on the public Internet can be conducted anonymously inside I2P" and that it is "an anonymous overlay network—a network within a network. It is intended to protect communication from dragnet surveillance and monitoring by third parties such as ISPs."[8]

Although both of these provide sufficient access to darknets, the most popular portal for access is The Onion Router.

The Onion Router

The Onion Router (aka ToR) was originally developed by the U.S. Naval Research Laboratory as a method of anonymous communication. It can be downloaded for free, and the website asserts:

> Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.[9]

In regard to security, ToR

> protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.[10]

The number of ToR users around the world is increasing (see Chart 8.2), as many find benefit to the anonymity provided by the server. Once hidden within the layers of ToR, individuals can browse the darknets while their privacy is protected. Sites on the ToR network end in .onion, but if you were to type the web address into Google, the website would not be found. According to the ToR website, people use this platform for multiple *noncriminal* reasons, as outlined in Table 8.1.

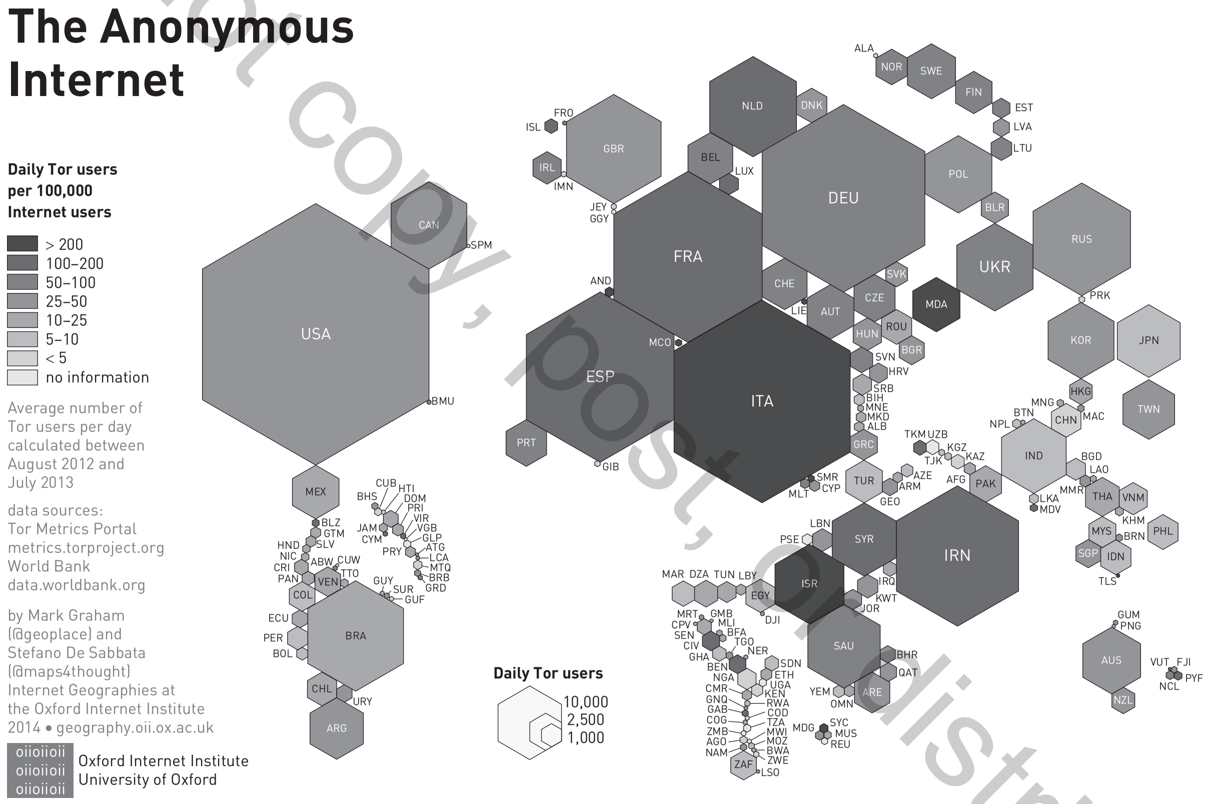
TABLE 8.1 ● Benefits of ToR Use

Who Is Using ToR?	Why? (Activity)
People Without Malicious Intent	Surf the net in privacy, protect themselves and their families
Businesses	Research competitions, keep strategies secret, internal accountability
Activists	Report abuses and violations from dangerous locations; whistleblowing
Media	Protect sources, resources, and report from areas where it is dangerous
Military/Law Enforcement	Protect communications, investigations, and intelligence

Source: Based on information from torproject.org.

Although many use ToR for legitimate purposes, darknets are known to attract criminals due to the anonymity they provide. Criminals can sell their illicit goods under the protection provided by the deep web.

CHART 8.2 ● Worldwide Onion Router (ToR) Users



Source: The Anonymous Internet by Mark Graham and Stefano De Sabbata, https://commons.wikimedia.org/wiki/File:Geographies_of_Tor.png. Licensed under CC BY-SA 4.0, https://creativecommons.org/licenses/by-sa/4.0/legalcode.

Products Available

As previously mentioned, both legal and illegal products and services are available on the deep web. Social media sites such as Facebook are accessible on the deep web. Research tools and databases are also located on the deep web. Some of these include JSTOR (an academic search engine), the National Oceanic and Atmospheric Administration, and NASA.[11] In countries where access to social media and/or academic materials/news is restricted or all together prohibited, the deep web offers a place where oppressed populations can retrieve and share information.

Other blogs and chatrooms are available on the deep web. Although not criminal, they may be groups that enjoy certain fetishes or activities and do not feel comfortable sharing that information on the surface web. Fan fiction, from sci-fi to Harry Potter, also finds a home on the deep web. Although some of these groups may not be viewed as mainstream, they are not illegal. The majority of illegal products on the deep web are found in black market darknets.

Via ToR or other specialized browsers, deep web users can access darknet marketplaces. Virtually every type of illegal goods, services, and information is available in darknet markets. Drugs, guns, credit card information, specialty items (Ebola-tainted blood, nuclear materials), and banned books/guides are all available for sale. Moreover, contract killings, human trafficking sales, and videos of human experiments are also products found via darknets. Sites with counterfeit products, as mentioned in the section on the surface web, have also found security on darknets. Once an individual accesses the darknet, they need only go to the hidden wiki in order to find links to any and/or all of these products.

THINK ABOUT IT 8.2

Black Market Blood

In the height of the West African Ebola crisis in 2014–2015, many hospitals could not keep up with the number of individuals being admitted. Resources were scarce, and many were left without proper health care. Due to this, some turned to black markets to buy the blood of survivors. This blood, known as convalescent serum, was believed to have antibodies that could prevent or possibly treat individuals with Ebola, much like modern vaccines.[12]

However, the blood of survivors is not the only blood for sale on the black market. One darknet site was offering Ebola-infected blood for sale by the gallon. Based on what we know about the Ebola virus, there is a 72-hour incubation period before symptoms begin to appear, and once they do, the disease can spread very rapidly.

What Would You Do?

1. Why would someone sell Ebola-infected blood?
2. What damages could occur if someone with malicious intent purchased the blood?
3. What issues does this pose to national and international security?

The Hidden Wiki

The hidden wiki is a popular way to search the darknets. It acts as a search engine for illicit goods, products, and services. The hidden wiki, just like traditional wikis, can be edited by anyone. This means that criminals can anonymously post links to their black market pages, and anyone on the darknet can access them.

Links on the hidden wiki may include websites that feature instructions for illegal activities such as bomb making or the production of methamphetamines. There are recruitment sites for jihadi organizations, assassins for hire, and sites that allow shoppers to purchase stolen credit card information. Darker aspects of some darknets may include violent pornography, snuff films, child pornography, and sadistic videos. Sites that show torture and human experimentation are also operating in the dark arena. Unfortunately, when there is a demand for a product, there is usually someone willing to supply it, and the anonymity provided on darknets can be very appealing to some suppliers.

Some of the most popular products advertised on the hidden wiki are drugs. Drug marketplaces run rampant on darknets. Silk Road (and the subsequent Silk Road 2.0) is arguably the most well-known .onion site for the drug market. As shown in Image 8.1, any and all drug products and paraphernalia are available via Silk Road.

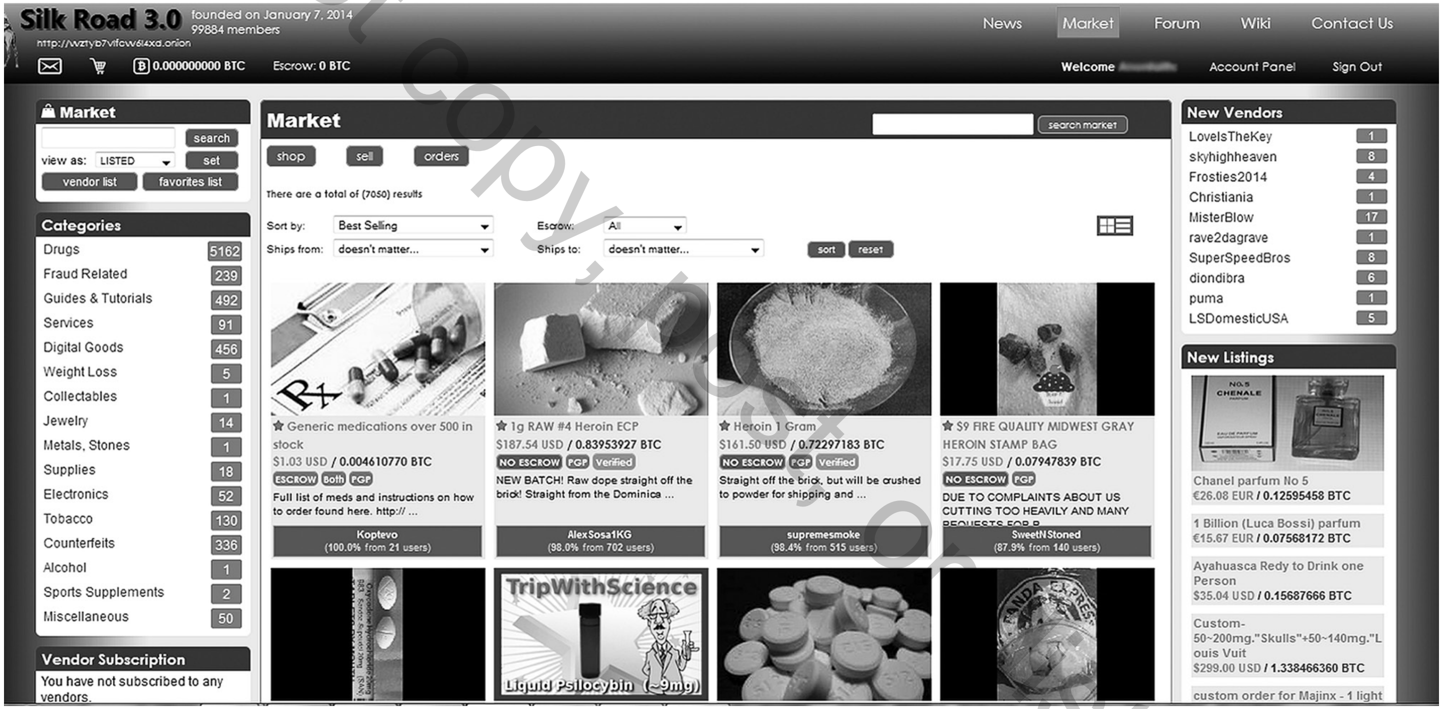
The Silk Road

The darknet Silk Road takes its name from the historical Silk Road, which, during the 19th century, was a trade route from China to Central Asia and then later into Europe. The road was traveled well by merchants selling silk, iron, gold, fruits, spices, and exotic animals. Although the road was a popular trade route, there are still many secrets to the original Silk Road that have yet to be uncovered.[13] The secretiveness of the historical Silk Road is one reason why using the name for the darknet marketplace is so applicable.

The darknet Silk Road runs like a black market eBay-type site for drugs, drug paraphernalia, and other goods and services. Potential buyers can read reviews on the products, the shipping, the seller's reputation, and more. Prices are listed in bitcoins and are shipped to remote addresses or post office boxes. During its prime operating period, Silk Road advertised more than 13,000 listings for controlled substances from vendors in the United States, Germany, the Netherlands, Canada, the United Kingdom, Spain, Ireland, Italy, Austria, and France.[14]

Vendors on Silk Road reportedly made over $1.2 million per month in 2011–2012 and more than doubled that in 2013. The ease of setting up a shop via Silk Road is another reason the site is so appealing. Potential sellers need only to fill out an online form and click a link to pay 150 bitcoin in order to become a vendor on Silk Road. According to one seller, "The opportunity to make money online is far greater than selling locally; even without moving lots of weight."[15] And as much as the vendors make, the operators who ran Silk Road profited with close to $92,000 per month in commissions alone.

IMAGE 8.1 ● Silk Road Marketplace Screenshot



Silk Road 3.0 founded on January 7, 2014
99884 members
http://wztyb7vifcw6l4xd.onion

0.000000000 BTC Escrow: 0 BTC

Welcome [redacted]

Market

view as: LISTED

Categories

Drugs	5162
Fraud Related	239
Guides & Tutorials	492
Services	91
Digital Goods	456
Weight Loss	5
Collectables	1
Jewelry	14
Metals, Stones	1
Supplies	18
Electronics	52
Tobacco	130
Counterfeits	336
Alcohol	1
Sports Supplements	2
Miscellaneous	50

Vendor Subscription

You have not subscribed to any vendors.

Market

There are a total of (7050) results

Sort by: Best Selling
Ships from: doesn't matter...
Escrow: All
Ships to: doesn't matter...

★ Generic medications over 500 in stock
$1.03 USD / 0.004610770 BTC
ESCROW Both PGP
Full list of meds and instructions on how to order found here. http:// ...
Koptevo
(100.0% from 21 users)

★ 1g RAW #4 Heroin ECP
$187.54 USD / 0.83953927 BTC
NO ESCROW PGP Verified
NEW BATCH! Raw dope straight off the brick! Straight from the Dominica ...
AlexSosa1KG
(98.0% from 702 users)

★ Heroin 1 Gram
$161.50 USD / 0.72297183 BTC
NO ESCROW PGP Verified
Straight off the brick, but will be crushed to powder for shipping and ...
supremesmoke
(98.4% from 515 users)

★ $9 FIRE QUALITY MIDWEST GRAY HEROIN STAMP BAG
$17.75 USD / 0.07947839 BTC
NO ESCROW PGP
DUE TO COMPLAINTS ABOUT US CUTTING TOO HEAVILY AND MANY REQUESTS FOR R
SweetNStoned
(87.9% from 140 users)

TripWithScience
Liquid Psilocybin (~9mg)

New Vendors

LoveIsTheKey	1
skyhighheaven	8
Frosties2014	4
Christiania	1
MisterBlow	17
rave2dagrave	1
SuperSpeedBros	8
diondibra	6
puma	1
LSDomesticUSA	5

New Listings

Chanel parfum No 5
€26.08 EUR / 0.12595458 BTC

1 Billion (Luca Bossi) parfum
€15.67 EUR / 0.07568172 BTC

Ayahuasca Redy to Drink one Person
$35.04 USD / 0.15687666 BTC

Custom-50~200mg."Skulls"+50~140mg."Louis Vuit
$299.00 USD / 1.338466360 BTC

custom order for Majinx - 1 light

Silkroad3.0 by Nialldawson, https://upload.wikimedia.org/wikipedia/commons/2/28/Silkroad30.png. Licensed under CC BY-SA 4.0, https://creativecommons.org/licenses/by-sa/4.0/legalcode

The success of Silk Road vendors is due mostly to the reputation they built for themselves based on product quality and customer reviews. As stated by one seller in research conducted by Van Hout and Bingham in 2014,

> reputation on Silk Road is what keeps the vendors in business. Your reputation is open to all. The seller who wants good business on Silk Road has to try and make every customer happy. Customer service has never been this good on the street market.[16]

One of the main issues with the quality of the product is ensuring that bad and/or tainted products are not sold. Although customers rate the quality of the drugs purchased, at least six overdose deaths have been tied to products purchased on Silk Road. Three victims overdosed on heroin, two from a synthetic form of LSD, and one from health issues triggered by drug use.[17]

Federal agencies have shut Silk Road down multiple times, but as hundreds of .onion addresses lead to the Silk Road, new links pop up once the site has been compromised. Law enforcement actions are discussed in detail later in the chapter.

THINK ABOUT IT 8.3

Dread Pirate Roberts and the Silk Road

The name Dread Pirate Roberts is usually associated with the movie *The Princess Bride*. However, it is also the pseudonym adopted by Ross Ulbricht, the creator of Silk Road. Ulbricht earned a master's degree in material science and engineering, and was also an Eagle Scout. As the creator of Silk Road, he earned over $13 million in commissions off the sale of illegal goods and services.

In 2013, after a multijurisdictional interagency operation, Ulbricht was arrested and charged with multiple offenses. In 2015, he was found guilty of seven offenses: distributing narcotics, distributing narcotics by means of the Internet, conspiracy to distribute narcotics, engaging in a continuing criminal enterprise, conspiring to commit computer hacking, conspiring to traffic in false identity documents, and conspiring to commit money laundering.[18]

Ulbricht was sentenced to life in prison and had to forfeit $183,961,921. Although Ulbricht received an extremely harsh sentence, online darknet drug markets, including Silk Road 2.0, still continue to flourish.

What Would You Do?

1. What does this tell criminal justice professionals about the role deterrence plays in crime in cyberspace?
2. How does this case affect the perception of the applicability of traditional criminal justice methods and theory to crime conducted online?
3. As a criminal justice professional, what would you do to ensure that the actions of Ulbricht were not replicated?

Payment: Cryptocurrency

Since bank accounts and credit cards contain personal information and are easily traceable, a different form of monetary transaction is necessary for darknet purchases. Cryptocurrency, or currency that exists only in the digital arena (you cannot physically hold digital money), is one way that purchases on the deep web can be made in anonymity. Used for both legitimate purchases and illegal ones, cryptocurrency has been evolving since 2009. Two of the most popular forms of cryptocurrency are bitcoins and dash.

Bitcoins (BTC or ฿)

Bitcoins, abbreviated BTC or with the symbol ฿, is a digital currency created in 2009 by an individual using the pseudonym Satoshi Nakamoto. Bitcoins can be used for online, seemingly anonymous, transactions; however, they are not issued by a bank. Bitcoins are also popular with hackers because this currency only exists online and is not controlled by a central authority nor subject to regulation, and therefore untraceable. This makes it very useful for criminals such as drug traffickers and hackers who are extorting money via malware infections (ransomware).

Bitcoins can be obtained in many ways, the simplest being through purchase. Bitcoin exchanges allow for the transfer and purchase of the online currency. Bitcoins can also be obtained via “mining.” Mining involves solving complex mathematical puzzles every 10 minutes. The person who solves the puzzle first receives approximately 25 bitcoins, although the amount can vary. Bitcoins are held in a virtual wallet associated with an encrypted IP address. Bitcoin transactions are recorded to ensure users can only spend their Bitcoins once. Although this may seem like a security issue, the blockchain that stores the transaction information has protections so the identities of those involved in the transactions are not identifiable.[19]

One issue with bitcoins is that this currency is not nearly as stable or predictable as real currency, such as the dollar or euro. The exchange rate of bitcoins is highly volatile. When first created, one U.S. dollar could purchase 1,309 bitcoins. In 2010, a programmer in Florida, experimenting with bitcoins, sent 10,000 BTC overseas to an individual in London to purchase pizza (valued around $25). Today, that pizza would be worth £1,961,034 ($2,443,945.39).[20] When the FBI shut down Silk Road as discussed previously, the value of bitcoins changed substantially. Since then, the bitcoin has fluctuated but consistently increased in value. As of February 1, 2017, the exchange rate for one bitcoin was 967.40 U.S. dollars.[21]

IMAGE 8.2 ● Bitcoins (BTC or ฿)

© iStockphoto.com/skodonnell

Many legal businesses do not accept bitcoins; however, this is starting to change. In the illegal marketplace, especially on darknets, it is a preferred payment method because it is completely anonymous and bitcoins can be transferred anywhere in the world safely and quickly.

Dash

Dash is another form of online digital currency. Modeled off of bitcoins, dash claims to improve on bitcoins by offering an enhanced level of security. According to dash's official webpage, with bitcoins it is possible to trace a transaction back to see the parties involved. Furthermore, because the bitcoin transactions are one-on-one, with miners being used to confirm validity of payment, a permanent record of all transactions is established.[22]

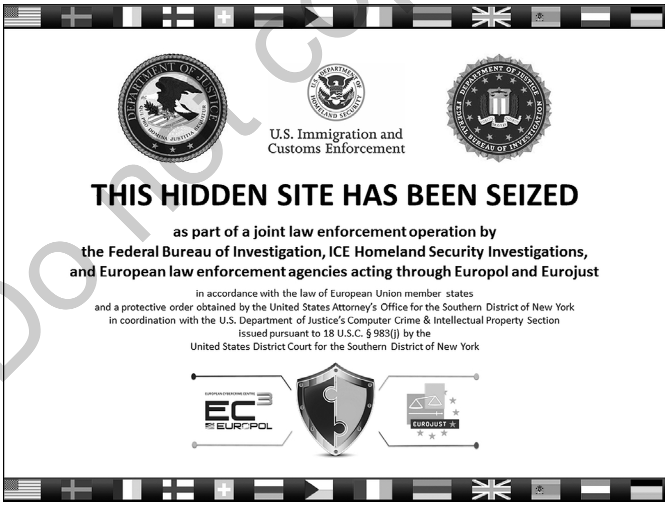
Dash eliminates this security issue by implementing a two-tier security network. With dash, a third party is not necessary to protect identities, as it uses masternodes (decentralized networks) to scramble data. Due to this, the wait to be approved for a transaction (a wait commonplace in transactions using bitcoins) is eliminated and transactions are almost instantly confirmed.[23] Many online sites, both on the deep and surface webs, have not yet implemented the use of dash as it is new and subsequently less well known than bitcoins. However, if the use of decentralized masternodes proves to be effective, dash may become the safer and faster option for online cryptocurrency.

Law Enforcement Response

Due to its popularity, Silk Road garnered the attention of the Drug Enforcement Agency. When the founder of Silk Road was arrested in October 2013, Silk Road was shut down (Image 8.3) and $25 million worth of bitcoins were seized. However, not long afterward, a copycat site known as Silk Road 2.0 emerged. When federal agents attempted to close it down, a backdoor was established by Silk Road administrators, allowing people with the password to enter the site.

An ongoing battle between federal law enforcement and dark web administrators has emerged, with law enforcement shutting down the site and administrators reopening Silk Road on a new .onion page. However, due to the attention received from federal agencies, other darknet drug markets have emerged. Some of the more popular alternative sites include Agora, Evolution, and Andromeda.

IMAGE 8.3 ● Silk Road Seizures



U.S. Immigration and Customs Enforcement

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

Federal Bureau of Investigation

As federal law enforcement became more aware of the darknet drug markets, they began cracking down on the sites. In 2014, agencies from around the world got together to shut down deep web black markets in an action known as Operation Onymous.

Operation Onymous

On November 6, 2014, law enforcement, collaborating together and coordinated via Europol, took down multiple darknet drug marketplaces, including Silk Road 2.0. Seventeen countries—the United States, Bulgaria, Czech Republic, Finland, France, Germany, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Netherlands, Romania, Spain, Sweden, Switzerland, and the United Kingdom—were involved in this collaborative effort. According to reports, over 400 .onion domain names associated with at least 27 darknet sites were seized and shut down.[24] In one of the biggest moves of law enforcement against darknet sites, the FBI arrested the alleged operator of Silk Road 2.0, Blake Benthall, and filed a civil complaint in New York.[25]

The civil complaint against the 27 darknet sites includes allegations of (1) selling illegal narcotics, (2) selling fake or stolen credit cards, (3) selling counterfeit currency, and (4) selling fake IDs, including passports.[26] An undisclosed number of bitcoins was also seized. Besides Benthall, 17 others were also arrested, although their identities were not revealed. Benthall, charged with multiple counts including narcotics trafficking, confessed to being involved with Silk Road 2.0. He is currently incarcerated at an unidentified location.

Anonymous and "Vigilante Justice"

As law enforcement is attempting to infiltrate darknet websites, the group Anonymous (see Chapter 5) is taking down darknet sites as well. In acts that could be considered hacktivism, or in some cases vigilante justice, Anonymous is able to penetrate parts of the deep web that law enforcement may not.

In February 2017, Anonymous shut down the over 16,000 .onion sites, including the darknet page Freedom Hosting II. Anonymous left the following message, defacing the site's access page:

> Hello, Freedom Hosting II, you have been hacked
>
> We are disappointed . . . This is an excerpt from your front page 'We have zero tolerance policy to child pornography.'-but what we found while searching through your server is more than 50% child porn . . .
>
> Moreover you host many scam sites, some of which are evidently run by yourself to cover hosting expenses.
>
> All your files have been copied and your databases have been dumped. (74GB of files and 2.3GB of database)
>
> Up until January 31st you were hosting 10613 sites. Private keys are included in the dump. Show full list (hyperlink)
>
> We are Anonymous. We do not forgive. We do not forget. You should have expected us.

> Thank you for your patience, you don't have to buy data ;) we made a torrent of the database dump download here (hyperlink)
>
> Here another torrent with all system files (excluding user data) download (hyperlink)
>
> You may still donate to BTC (bitcoins) to 14iCDyeCSp12AmhVfJGxtrzX-DabFop4QtU and support us.
>
> If you need to get in contact with us, our mail is fhosting@sigaint.org
>
> We repeatedly get how we got into the system. It was surprisingly easy. Here is how we did it: HOW TO HACK FH2 (hyperlink)
>
> Edit: couldn't reply to Clearnet – new mail
>
> Edit2; database dump added
>
> Edit3: added instructions on how we got into the system
>
> Edit4: system files added[27]

Anonymous is well known for their activism against ideas they do not support. They are not against the use of the web for criminal activities, but it is the type of activity (in this case, child pornography) that they act against. This is not the first time Anonymous has acted against darknet sites. In 2011, the predecessor of Freedom Hosting II (the original Freedom Hosting) hosted over 50% of darknet sites, including sites containing child pornography. Anonymous hit the site with denial-of-service attacks and the site was eventually removed by the FBI.[28]

THINK ABOUT IT 8.4

Online Vigilante Justice

Freedom Hosting II broke the law by posting child pornography links on its website. Before law enforcement could respond, the hacktivist group Anonymous hacked into the site, and in an act that could be described as vigilante justice, closed the forum down.

The term *vigilante* refers to "a member of a volunteer committee organized to suppress and punish crime summarily (as when the processes of law are viewed as inadequate),"[29] or someone who punishes certain behavior without the authority to do so.

What Freedom Hosting II was doing (allowing links to child pornography to be posted on their site after explicitly saying they would not do so) is against the law; however, so is hacking.

Should the actions of Anonymous be ignored by law enforcement, as their actions shut down more serious criminal activity, or should they be prosecuted as well, regardless of the good that came out of their criminal behavior?

What Would You Do?

1. Should the actions of Anonymous be protected?
2. Is there past precedent for such actions?
3. How would this affect other cases of vigilante justice, especially those cases that are not so nonviolent?

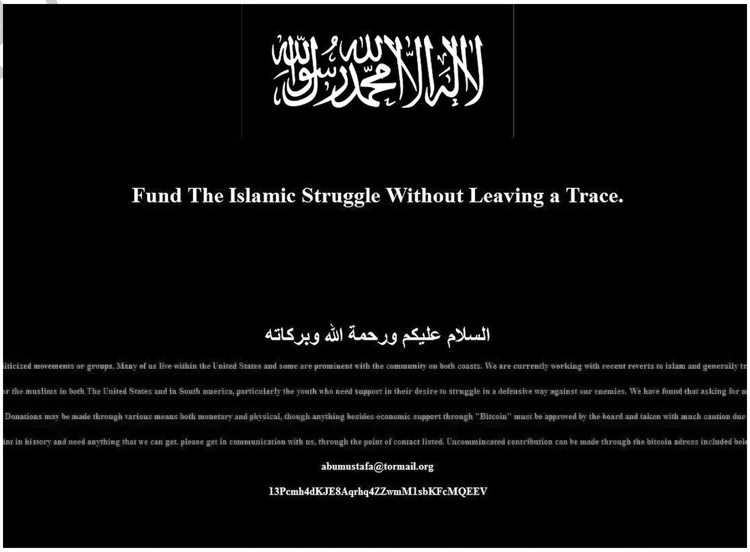
Terrorist Presence on the Deep and Dark Web

> The government does things like insisting that all encryption programs have a back door. But surely no one is stupid enough to think the terrorists are going to use encryption systems with a back door. The terrorists will simply hire a programmer to come up with secure encryption scheme.
>
> **—Kevin Mitnick**[30]

Cybercriminals are not the only criminal entity who have a presence on and can benefit from the anonymity provided by the deep web. Terrorist organizations can use the deep web as a place to hide their activities. Once anonymous, terrorist organizations can distribute propaganda, train and exchange information with hackers, post training videos, detail how to make nuclear bombs, buy and sell weapons, purchase false identification, and communicate without detection.[31]

Some examples of known terrorist presence on the dark web include an al-Qaeda online forum (ek-Is.org), a weapons marketplace (vlp4uw547agp52is.onion), and an identity marketplace (Web.g6lfrbqd3krju3ek.onion). Chin and his colleagues uncovered a deep web page, "Encyclopedia of Training and Preparedness," which included a set of lessons titled "The Nuclear Tutorial for the Mujahedeen." This tutorial contains over 450 pages of instructions for future jihadists and includes discussion of both nuclear and electromagnetic bombs.[32] Other training manuals and instructions for waging jihad against Western countries have also been discovered. Terrorist organizations use the dark web to reach out to followers, supporters, donators, sympathizers, and others who may contribute to the success of their organizations, as pictured in screenshot Image 8.4.

IMAGE 8.4 ● Screenshot of a Darknet Site for Funding Islamic Extremism



Fund The Islamic Struggle Without Leaving a Trace.

السلام عليكم ورحمة الله وبركاته

liticized movements or groups. Many of us live within the United States and some are prominent with the community on both coasts. We are currently working with recent reverts to islam and generally tr

or the muslims in both The United States and in South america, particularly the youth who need support in their desire to struggle in a defensive way against our enemies. We have found that asking for m

Donations may be made through various means both monetary and physical, though anything besides economic support through "Bitcoin" must be approved by the board and taken with much caution due

int in history and need anything that we can get. please get in communication with us, through the point of contact listed. Uncommincated contribution can be made through the bitcoin adress included bel

abumustafa@tormail.org

13Pcmh4dKJE8Aqrhq4ZZwmM1sbKFcMQEEV

CASE STUDY 8.1

ISIS and the Threat of the Darknet

It is well known that the Islamic State in Iraq and Syria (ISIS; also referred to as ISIL, the Islamic State, and Daesh) has an established presence on the surface web. ISIS has used online chatrooms, forums, and social media in an unprecedented fashion to distribute propaganda, recruit supporters, and to fundraise. However, there is rising concern that ISIS may also have a viable presence on the darknet.

It has been reported that ISIS hosts a "help desk" on the darknet to assist supporters in carrying out attacks. According to the report, the helpdesk operates 24 hours a day, with six operators to answer questions via a series of forums that ISIS supporters can go to for information on how they can support the extremist movement.[33] These chatrooms are not the only way that ISIS could exploit darknet resources for their cause. As previously mentioned, there are mercenaries and assassins for hire. ISIS has ample money to be able to hire these individuals to act on behalf of the organization. Furthermore, hackers for hire can be used to commit cyberattacks that steal data, and ISIS can turn around and sell the data for a profit.[34]

ISIS could use the darknet to coordinate attacks, make plans, and discuss potential targets. Training in cyberskills (hacking, staying hidden, encryption) is also available via darknets.

What Do You Think?

1. How could ISIS use such information to further their goals?

Legal Issues

The Constitution has long established the right to freedom of speech (First Amendment) and the protection against unwarranted search and seizure (Fourth Amendment). However, these issues are often questioned in regard to the Internet in general and especially the deep web. Moreover, due to the borderless arena that is the Internet, users of the deep web and its darknets should be aware of the legality associated with the country in which they are residing and that from which the website is hosted. What is legal in some countries may not be legal in others. The founding fathers were not anticipating the borderless, limitless jurisdiction of the web when they wrote the Constitution, so the U.S. Supreme Court has had to reexamine these issues to evaluate their applicability in cyberspace.

In regard to freedom of speech, the First Amendment reads:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.[35]

The U.S. Supreme Court elaborated on this by saying that these rights do not include situations that pose a "clear and present danger":

> A situation created which someone deems to require a governmental limitation on Constitutional First Amendment freedoms of speech, press or

> assembly, such as shouting "fire" in a crowded theater (speech), printing a list of the names and addresses of CIA agents (press) or gathering together a lynch mob (assembly).[36]

However, it is unknown as to what would cause a clear and present danger in cyberspace. Much of the information contained on darknets may be legal; however, what someone chooses to do with that information may not be. The Electronic Frontier Foundation (EFF) is an advocacy group that works to protect the right to free speech online, including the freedom to exchange ideas and opinions without the fear of prosecution. They also work to protect the right to anonymity on the Internet, especially on the deep web.

Anonymity is not guaranteed within the First Amendment, but it has been interpreted by the U.S. Supreme Court. Individuals can speak and write anonymously, as long as it does not violate the law. In the 1995 case of *McIntyre v. Ohio Elections Commission* 514 U.S. 334, the court ruled:

> Protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical minority views . . . Anonymity is a shield from the tyranny of the majority. . . . It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society.[37]

Since this 1995 decision, opportunities for anonymous speech and writing have increased substantially. See Legal Issue 8.1 to discuss how this interpretation may or may not apply to cyberspace.

The Fourth Amendment has also come under question in regard to online criminal activity, specifically in regard to search and seizure. The Fourth Amendment reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[38]

The Fourth Amendment was interpreted in 1914 in *Weeks v. United States* 232 U.S. 383, to include that any evidence seized during an illegal search was considered "fruits of the poisonous tree" and was not admissible in federal court (the Exclusionary Rule). The Exclusionary Rule was extended to apply to the states in 1961, *Mapp v. Ohio* 367 U.S. 643.[39]

The main Fourth Amendment/Exclusionary Rule issues in regard to the deep web are (1) how is probable cause established in cyberspace, (2) must warrants be issued to search cyberspace, and (3) if a search is found to be illegal, what online evidence should be excluded, or considered "fruits of the poisonous tree"?

In 2009, the U.S. Supreme Court examined search and seizure in cyberspace in the case of *U.S. v Wellman* 716 F. Supp. 2d 447. Wellman was accused of obtaining child pornography via peer-to-peer Internet sites. An online search revealed that the IP address attached to the pornography was associated with Wellman's computer. Based on this, a judge issued a warrant to search Wellman's home. The search of the home revealed more child pornography, both on the computer's hard drive and on DVDs, and Wellman was subsequently arrested.[40] This case presents an interesting perspective: Should evidence obtained in cyberspace be admissible to show probable cause and obtain a search warrant for a physical location?

LEGAL ISSUE 8.1

ANONYMITY AND THE FIRST AMENDMENT

In 1995, with the case of *McIntyre v. Ohio Elections Commission*, the U.S. Supreme Court interpreted how the First Amendment applied to anonymity. By holding that "protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical minority views . . . Anonymity is a shield from the tyranny of the majority. . . . It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society," the court protected anonymous speech and writing as long as it did not break the law.

On the deep web and its darknets, anonymity is a given—that is, established once an individual signs in to the ToR network or another deep web browser. The EFF works to protect the rights of online anonymity. However, this is increasingly difficult when many of the darknet sites contain information that may lead to illegal behavior. Review what EFF has published on their webpage about anonymity (https://www.eff.org/search/site/anonymity) and then discuss the following questions:

1. How has the deep web changed the way that First Amendment rights may be interpreted?
2. Should darknet sites be able to publish information that is not criminal in and of itself, and if so, should they be held responsible if a darknet user decides to use the information in an illegal or malicious way?
3. What role does EFF play in defending the right to anonymity, both on the surface and on the deep web?

Summary

The evolution of the deep web and its subsequent darknets has expanded at an unprecedented pace. The deep web is not criminal in and of itself; however, the anonymity provided, especially on darknets, makes it an attractive tool for criminals. Furthermore, the use of hidden IP addresses and cryptocurrency allow for increased anonymity when operating on the deep web. These benefits also make darknets extremely attractive to terrorists for use in propaganda distribution, recruitment, and fundraising. As the deep web and darknets continue to expand and evolve, the criminal justice system must be able to adapt to the legal issues that may arise from this cyber jurisdiction. It remains to be seen how the Supreme Court will interpret free speech and search and seizure in cyberspace, especially as it pertains to the deep web.

Key Terms

Bitcoins	153
Blockchain	153
Cryptocurrency	153
Dark Web/Darknet	145
Dash	153
Deep Web	145
Electronic Frontier Foundation	159
Exclusionary Rule	159
Hidden Wiki	150
Intranet	145
Operation Onymous	155
Ross Ulbricht	152
Satoshi Nakamoto	153
Silk Road	150
Surface Web	144
ToR (The Onion Router)	146

Discussion Questions

1. What is the difference between the surface web, the deep web, and darknets?
2. What is cryptocurrency, and how does it work?
3. Discuss the evolution of darknet marketplaces and products that are available.
4. How does the deep web, and subsequently darknets, make investigating and prosecuting cybercrime difficult?
5. Discuss the changing role of the First and Fourth Amendments in regard to actions on the deep web.

Internet Resources

The Onion Router (ToR)
https://www.torproject.org/

The Official Webpage for Dash
https://www.dash.org

The Electronic Frontier Foundation
https://www.eff.org

Court Cases

United States of America v. Any and All Assets of the Following Dark Market Websites Operating on the TOR Network, Including But Not Limited To The ".Onion" Addresses of the Websites, the Servers Hosting the Websites, and Any BitCoins or Other Digital Currency Residing on Those Servers: Silk Road 2.0; Alpaca; Black Market; Blue Sky; Bungee 54; Cannabis UK; Cloud Nine; CStore; DeDope; Executive Outcomes; Fake ID; Fake Real Plastic; Farmer1; Fast Cash!; Hackintosh; Hydra; Pablo Escobar Drugstore; Pandora; Pay Pal Center; Real Cards Team; REPAAA'S Hidden Empire; Smokeables; Sol's Unified USD Counterfeit's; Super Notes Counter; The Green Machine; TOR Bazaar; and Zero Squad, And all property traceable there to, Defendants-in-rem. (14 Civ. 8812 [JPO])

McIntyre v. Ohio Elections Commission 514 U.S. 334

Weeks v. United States 232 U.S. 383

Mapp v. Ohio 367 U.S. 643

U.S. v Wellman 716 F. Supp. 2d 447

Digital Resources

Want a better grade?

Get the tools you need to sharpen your study skills. Access practice quizzes and eFlashcards, at **study.sagepub.com/kremling**.