Congressional Research Service
Informing the legislative debate since 1914

Dark Web

Kristin Finklea
Specialist in Domestic Security

July 7, 2015

Congressional Research Service
7-5700
www.crs.gov
R44101

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

The layers of the Internet go far beyond the surface content that many can easily access in their daily searches. The other content is that of the *Deep Web*, content that has not been indexed by traditional search engines such as Google. The furthest corners of the Deep Web, segments known as the *Dark Web*, contain content that has been *intentionally* concealed. The Dark Web may be used for legitimate purposes as well as to conceal criminal or otherwise malicious activities. It is the exploitation of the Dark Web for illegal practices that has garnered the interest of officials and policy makers.

Individuals can access the Dark Web by using special software such as Tor (short for The Onion Router). Tor relies upon a network of volunteer computers to route users' web traffic through a series of other users' computers such that the traffic cannot be traced to the original user. Some developers have created tools—such as Tor2web—that may allow individuals access to Tor-hosted content without downloading and installing the Tor software, though accessing the Dark Web through these means does not anonymize activity. Once on the Dark Web, users often navigate it through directories such as the "Hidden Wiki," which organizes sites by category, similar to Wikipedia. Individuals can also search the Dark Web with search engines, which may be broad, searching across the Deep Web, or more specific, searching for contraband like illicit drugs, guns, or counterfeit money. While on the Dark Web, individuals may communicate through means such as secure email, web chats, or personal messaging hosted on Tor. Though tools such as Tor aim to anonymize content and activity, researchers and security experts are constantly developing means by which certain hidden services or individuals could be identified or "deanonymized."

Anonymizing services such as Tor have been used for legal and illegal activities ranging from maintaining privacy to selling illegal goods—mainly purchased with Bitcoin or other digital currencies. They may be used to circumvent censorship, access blocked content, or maintain the privacy of sensitive communications or business plans. However, a range of malicious actors, from criminals to terrorists to state-sponsored spies, can also leverage cyberspace and the Dark Web can serve as a forum for conversation, coordination, and action. It is unclear how much of the Dark Web is dedicated to serving a particular illicit market at any one time, and, because of the anonymity of services such as Tor, it is even further unclear how much traffic is actually flowing to any given site.

Just as criminals can rely upon the anonymity of the Dark Web, so too can the law enforcement, military, and intelligence communities. They may, for example, use it to conduct online surveillance and sting operations and to maintain anonymous tip lines. Anonymity in the Dark Web can be used to shield officials from identification and hacking by adversaries. It can also be used to conduct a clandestine or covert computer network operation such as taking down a website or a denial of service attack, or to intercept communications. Reportedly, officials are continuously working on expanding techniques to deanonymize activity on the Dark Web and identify malicious actors online.

Contents

Figures

Contacts

Beyond the Internet content that many can easily access online lies another layer—indeed a much larger layer—of material that is not accessed through a traditional online search. As experts have noted, "[s]earching on the Internet today can be compared to dragging a net across the surface of the ocean. While a great deal may be caught in the net, there is still a wealth of information that is deep, and therefore, missed."[1] This deep area of the Internet, or the Deep Web, is characterized by the unknown—unknown breadth, depth, content, and users.

The furthest corners of the Deep Web, known as the Dark Web, contain content that has been intentionally concealed. The Dark Web may be accessed both for legitimate purposes and to conceal criminal or otherwise malicious activities. It is the exploitation of the Dark Web for illegal practices that has garnered the interest of officials and policy makers. Take for instance the Silk Road—one of the most notorious sites formerly located on the Dark Web. The Silk Road was an online global bazaar for illicit services and contraband, mainly drugs. Vendors of these illegal substances were located in more than 10 countries around the world, and contraband goods and services were provided to more than 100,000 buyers.[2] It has been estimated that the Silk Road generated about $1.2 billion in sales between January 2011 and September 2013, after which it was dismantled by federal agents.[3]

The use of the Internet, and in particular the Dark Web, for malicious activities has led policy makers to question whether law enforcement and other officials have sufficient tools to combat the illicit activities that might flow through this underworld.[6] This report illuminates information on the various layers of the Internet, with a particular focus on the Dark Web. It discusses both legitimate and illicit uses of the Dark Web, including how the government may rely upon it. Throughout, the report raises issues that policy makers may consider as they explore means to curb malicious activity online.

Silk Road

The Silk Road was reportedly launched in 2011 by Ross William Ulbricht, who was known online as the "Dread Pirate Roberts." In September 2013 federal agents seized the Silk Road site, and in October 2013 the Federal Bureau of Investigation (FBI) arrested Ulbricht.[4] He received over $13 million in commissions from sales on the Silk Road. While the Silk Road was primarily used to sell illegal drugs, it also offered digital goods, including malicious software and pirated media; forgeries, including fake passports and Social Security cards; and services, such as computer hacking.[5] In May 2015, Ulbricht was sentenced to life in prison for his role in operating the Silk Road.

[1] Michael K. Bergman, *The Deep Web: Surfacing Hidden Value*, Bright Planet, September 24, 2001.

[2] Department of Justice, United States Attorney's Office, "Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced In Manhattan Federal Court To Life In Prison," press release, May 29, 2015.

[3] Department of Justice, United States Attorney's Office, "Manhattan U.S. Attorney Announces Seizure Of Additional $28 Million Worth Of Bitcoins Belonging To Ross William Ulbricht, Alleged Owner And Operator Of "Silk Road" Website," press release, October 25, 2013.

[4] Ibid.

[5] Department of Justice, United States Attorney's Office, "Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced In Manhattan Federal Court To Life In Prison," press release, May 29, 2015.

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

Layers of the Internet

Many may consider the Internet and World Wide Web (web) to be synonymous; they are not. Rather, the web is one portion of the Internet, and a medium through which information may be accessed.[7] In conceptualizing the web, some may view it as consisting solely of the websites accessible through a traditional search engine such as Google. However, this content—known as the "Surface Web"—is only one portion of the web. The *Deep Web* refers to "a class of content on the Internet that, for various technical reasons, is not indexed by search engines," and thus would not be accessible through a traditional search engine.[8] Information on the Deep Web includes content on private intranets (internal networks such as those at corporations, government agencies, or universities), commercial databases like Lexis Nexis or Westlaw, or sites that produce content via search queries or forms. Going even further into the web, the *Dark Web* is the segment of the Deep Web that has been *intentionally* hidden. The Dark Web is a general term that describes hidden Internet sites that users cannot access without using special software. Users access the Dark Web with the expectation of being able to share information and/or files with little risk of detection.

In 2005, the number of Internet users reached 1 billion worldwide. This number surpassed 2 billion in 2010 and crested over 3 billion in 2014.[9] As of June 2015, more than 40% of the world population was connected to the Internet. While data exist on the number of Internet users, data on the number of users accessing the various layers of the web and on the breadth of these layers are less clear.

Surface Web. The magnitude of the web is growing. In the United States alone, about 100,000 new web domains are reportedly registered every day. Simultaneously, it is estimated that 40,000–70,000 web domains go offline each day. If these estimates are accurate, there are at least 30,000 web domains added daily.[10]

Deep Web. The Deep Web, as noted, cannot be accessed by traditional search engines because the content in this layer of the web is not indexed. Information here is not "static and linked to other pages" as is information on the Surface Web.[11] As researchers have noted, "[i]t's almost impossible to measure the size of the Deep Web. While some early estimates put the size of the Deep Web at 4,000–5,000 times larger than the surface web, the changing dynamic of how information is accessed and presented means that the Deep Web is growing exponentially and at a rate that defies quantification."[12]

Dark Web. Within the Deep Web, the Dark Web is also growing as new tools make it easier to navigate.[13] Because individuals may access the Dark Web assuming little risk of detection, they

[7] The Internet is also used for email, file transfers, and instant messaging, among other things. Michael Chertoff and Toby Simon, *The Impact of the Dark Web on Internet Governance and Cyber Security*, Global Commission on Internet Governance, Paper Series: No. 6, February 2015.

[8] Michael Chertoff and Toby Simon, *The Impact of the Dark Web on Internet Governance and Cyber Security*, Global Commission on Internet Governance, Paper Series: No. 6, February 2015, p. 1.

[9] Internet Live Stats, *Internet Users*, http://www.internetlivestats.com/internet-users/.

[10] Bright Planet, *Deep Web: Advanced,* http://www.brightplanet.com/deep-web-university-2/deep-web-advanced/.

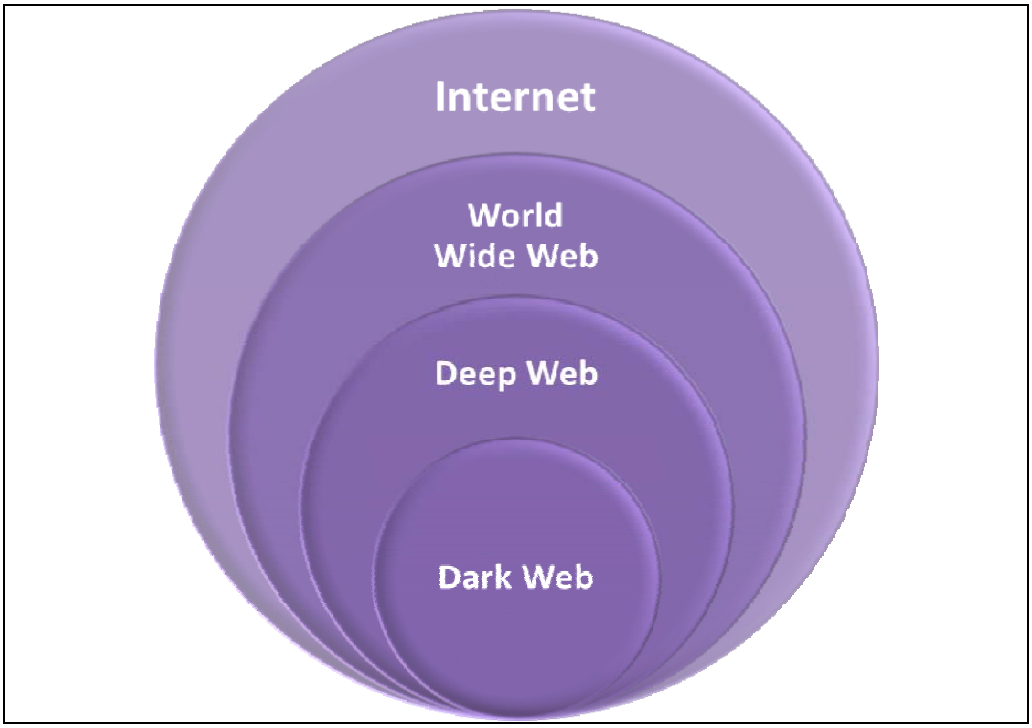
[11] Bright Planet, *Deep Web: A Primer*, http://www.brightplanet.com/deep-web-university-2/deep-web-a-primer/.

[12] Ibid.

[13] DarkNet Stats, for instance, is a website that outlines historical statistics on select Dark Web sites, providing (continued...)

may use this arena for a variety of legal and illegal activities. It is unclear, however, how much of the Deep Web is taken up by Dark Web content and how much of the Dark Web is used for legal or illegal activities.

Figure 1. Layers of the Internet



Source: Congressional Research Service (CRS).

Notes: The World Wide Web is made up of the Surface Web and the Deep Web. Proportions in the figure may not be to scale.

Accessing and Navigating the Dark Web

The Dark Web can be reached through decentralized, anonymized nodes on a number of networks including Tor (short for The Onion Router)[14] or I2P (Invisible Internet Project)[15]. Tor, which was initially released as The Onion Routing project in 2002,[16] was originally created by the U.S. Naval Research Laboratory as a tool for anonymously communicating online.

(...continued)

information such as notification of website outages.

[14] More information on Tor is available at https://www.torproject.org/. Tor is the most widely used anonymous network and thus is the focus of discussion in this report.

[15] Originally designed as a way to be able to use Internet Relay Chat (IRC) anonymously, I2P has become one of the more popular anonymous networks. While similar to Tor, key differences include the fact that I2P focuses on gaining access to sites within the network, and not to the Internet at large. Not as much academic research has been done on this project as on Tor. This service is very popular in Russia and about half the routers appear to be located there. For more information, see https://geti2p.net.

[16] Roger Dingledine, Nick Mathewson, and Paul Syverson, "Tor: The Second-Generation Onion Router," Proceedings (continued...)

Tor "refers both to the software that you install on your computer to run Tor and the network of computers that manages Tor connections."[17] Tor's users connect to websites "through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy."[18] Users route their web traffic through other users' computers such that the traffic cannot be traced to the original user. Tor essentially establishes layers (like layers of an onion) and routes traffic through those layers to conceal users' identities.[19] To get from layer to layer, Tor has established "relays" on computers around the world through which information passes.[20] Information is encrypted between relays, and "all Tor traffic passes through at least three relays before it reaches its destination."[21] The final relay is called the "exit relay," and the IP address of this relay is viewed as the source of the Tor traffic. When using Tor software, users' IP addresses remain hidden. As such, it appears that the connection to any given website "is coming from the IP address of a Tor exit relay, which can be anywhere in the world."[22]

While data on the magnitude of the Deep Web and Dark Web and how they relate to the Surface Web are not clear, data on Tor users do exist. According to metrics from the Tor Project, the mean number of daily Tor users in the United States across the first three months of 2015 was 360,775—or 16.56% of total mean daily Tor users.[23] The United States has the largest number of mean daily Tor users, followed by Germany (over 9%) and Russia (nearly 8%).

Communicating On (and About) the Dark Web

There are several different ways to communicate about the Dark Web. One of the first places individuals may turn is Reddit.[24] There are several subreddits[25] pertaining to the Dark Web, such as DarkNetMarkets, Onions, or Tor. These forums often provide links to sites within the Dark Web. Reddit provides a public platform for Dark Web users to discuss different aspects of the Tor. It is not encrypted or anonymous, as users who wish to engage in forum discussion must create an account.[26] Individuals who wish to use a more secure form of communication may choose to utilize email, web chats, or personal messaging hosted on Tor:

(...continued)

of the 13th USENIX Security Symposium, San Diego, CA, August 9-13, 2004, https://www.usenix.org/legacy/events/sec04/tech/full_papers/dingledine/dingledine.pdf.

[17] Adam Clark Estes, "Tor: The Anonymous Internet, and If It's Right for You," *Gizmodo*, August 30, 2013.

[18] Tor Project, *Tor: Overview*, https://www.torproject.org/about/overview.html.en.

[19] Adam Clark Estes, "Tor: The Anonymous Internet, and If It's Right for You," *Gizmodo*, August 30, 2013.

[20] Individuals can volunteer their computers to be "relays" through which information may pass.

[21] Electronic Frontier Foundation, *What is a Tor Relay?*, https://www.eff.org/pages/what-tor-relay.

[22] Ibid. According to the Electronic Frontier Foundation, "[a]n exit relay is the final relay that Tor traffic passes through before it reaches its destination. Exit relays advertise their presence to the entire Tor network, so they can be used by any Tor users. Because Tor traffic exits through these relays, the IP address of the exit relay is interpreted as the source of the traffic."

[23] Data available at https://metrics.torproject.org/userstats-relay-table.html.

[24] Reddit is a website for online content ranging from news and entertainment to social networking where registered members can enter and share content. Members can also vote and comment on important stories and discussions. For more information, see https://www.reddit.com/about.

[25] A subreddit is a feed within Reddit on which users discuss a particular topic.

[26] Recently, the Department of Homeland Security subpoenaed Reddit for the information of five Reddit users that were active in discussion of the Dark Web. See Andy Greenberg, "Feds Demand Reddit Identify Users of a Dark-Web (continued...)

- Email service providers, for instance, typically only require users to input a username and password to sign up.[27] In addition, email service providers generally offer anonymous messaging and encrypted storage.
- A number of anonymous, real-time chat rooms such as The Hub and OnionChat are hosted on Tor. Feeds are organized by topic. While some sites do not require any information from users before participating in chats, others require a user to register with an email address.
- Personal messaging is another option for Tor users who wish to communicate with an added layer of anonymity. Bitmessage is a popular messaging system which offers encryption and strong authentication.[28] Secure Messaging System for Tor allows a user to write a message and generates a unique link for that message. The messages are encrypted and self-destruct after the link is used once. Specific vendor sites may host private messaging as well.[29]

Navigating the Deep Web and Dark Web

Traditional search engines often use "web crawlers" to access websites on the Surface Web. This process of crawling searches the web and gathers websites that the search engines can then catalog and index.[30] Content on the Deep (and Dark) Web, however, may not be caught by web crawlers (and subsequently indexed by traditional search engines) for a number of reasons, including that it may be unstructured, unlinked, or temporary content.[31] As such, there are different mechanisms for navigating the Deep Web than there are for the Surface Web.

Users often navigate Dark Web sites through directories such as the "Hidden Wiki," which organizes sites by category, similar to Wikipedia. In addition to the wikis, individuals can also search the Dark Web with search engines. These search engines may be broad, searching across the Deep Web, or they may be more specific. For instance, Ahmia, an example of a broader search engine, is one "that indexes, searches and catalogs content published on Tor Hidden Services."[32] In contrast, Grams is a more specific search engine "patterned after Google" where users can find illicit drugs, guns, counterfeit money, and other contraband.[33]

(...continued)

Drug Forum," *Wired.com*, March 30, 2015.

[27] Examples include Mailtor, Mail2tor and Ruggedinbox, all only accessible through the Tor browser.

[28] For more information about how Bitmessage works, see Jonathan Warren, "Bitmessage: A Peer-to-Peer Message Authentication and Delivery System," http://www.bitmessage.org, November 27, 2012.

[29] Andy Greenberg, "An Interview with Darkside, Russia's Favorite Dark Web Drug Lord," *Wired.com*, December 4, 2014.

[30] For a detailed description of this process, see Google, *Inside Search, How Search Works, Crawling & Indexing*, http://www.google.com/insidesearch/howsearchworks/crawling-indexing.html.

[31] Caroline Craig, "'Google Search on Steroids' Brings Dark Web Into the Light," *InfoWorld*, February 13, 2015.

[32] TorProject blog, *Ahmia Search After GSoC Development*, September 7, 2014. Ahmia is available at https://ahmia.fi/search/.

[33] Kim Zetter, "New 'Google' for the Dark Web Makes Buying Dope and Guns Easy," *Wired.com*, April 17, 2014.

When using Tor, website URLs change formats. Instead of websites ending in .com, .org, .net, etc., domains usually end with an "onion" suffix, identifying a "hidden service."[34] Notably, when searching the web using Tor, an onion icon displays in the Tor browser.

Tor is notoriously slow, and this has been cited as one drawback to using the service. This is because all Tor traffic is routed through at least three relays, and there can be delays anywhere along its path. In addition, speed is reduced when more users are simultaneously on the Tor network.[35] On the other hand, increasing the number of users who agree to use their computers as relays can increase the speed on Tor.

Tor and similar networks are not the only means to reach hidden content on the web. Other developers have created tools—such as Tor2web—that may allow individuals access to Tor-hosted content without downloading and installing the Tor software.[36] Using bridges such as Tor2web, however, does not provide users with the same anonymity that Tor offers. As such, if users of Tor2web or other bridges access sites containing illegal content—for instance, those that host child pornography—they could more easily be detected by law enforcement than individuals who use anonymizing software such as Tor.

Is the Dark Web Anonymous?

Guaranteed anonymity is not foolproof. While tools such as Tor aim to anonymize content and activity, researchers and security experts are constantly developing means by which certain hidden services or individuals could be identified or "deanonymized."[37]

- For example, in October 2011 the "hacktivist"[38] collective Anonymous, through its Operation Darknet, crashed a website hosting service called Freedom Hosting—operating on the Tor network—which was reportedly home to more than 40 child pornography websites.[39] Among these websites was Lolita City,

[34] InfoSec Institute, *Diving in the Deep Web*, March 14, 2013, http://resources.infosecinstitute.com/diving-in-the-deep-web/. These .onion addresses "are 16-character alpha-semi-numeric hashes which are automatically generated based on a public key created when the hidden service is configured."

[35] Adam Clark Estes, "Tor: The Anonymous Internet, and If It's Right for You," *Gizmodo*, August 30, 2013. Speed issues are reportedly most noticeable for audio and video content.

[36] Kim Zetter, "New Service Makes Tor Anonymized Content Available to All," *Wired.com*, December 12, 2008.

[37] Rob Jansen, Florian Tschorsch, and Aaron Johnson, et al., "The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network," December 2013; TorProject, "Tor Security Advisory: "Relay Early" Traffic Confirmation Attack," press release, July 30, 2014; Yixin Sun, Anne Edmundson, and Laurent Vanbever, et al., "RAPTOR: Routing Attacks on Privacy in Tor," March 13, 2015; and Cammy Harblson, "Deanonymizing Tor Hidden Service Traffic Through HSDir Is A Cake Walk, Say Researchers: HITB Presenters Showcase New Threats," *iDigitalTimes*, May 29, 2015.

[38] Hacktivism is a term often used to refer to the use of computers and online networks to conduct politically or socially motivated protest. For more information on hacktivism and the collective known as Anonymous, see CRS Report R42547, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*, by Kristin Finklea and Catherine A. Theohary.

[39] Sean Gallagher, "Anonymous Takes Down Darknet Child Porn Site on Tor Network," *ArsTechnica*, October 23, 2011. See also Mathew Schwartz, "Anonymous Attacks Child Pornography Websites," *InformationWeek*, October 24, 2011. Some later estimates put the number of child porn websites hosted by Freedom Hosting to be over 100. See Kevin Poulsen, "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack," *Wired.com*, September 13, 2013.

cited as one of the largest child pornography sites with over 100GB of data.[40] Anonymous had "matched the digital fingerprints of links on [Lolita City] to Freedom Hosting" and then launched a Distributed Denial of Service (DDoS) attack against Freedom Hosting.[41] In addition, through Operation Darknet, Anonymous leaked the user database—including username, membership time, and number of images uploaded—for over 1,500 Lolita City members.[42]

- In 2013, the Federal Bureau of Investigation (FBI), reportedly took control of Freedom Hosting and infected it with "custom malware designed to identify visitors."[43] Since 2002, the FBI has supposedly been using some form of a "computer and internet protocol address verifier"—consistent with the malware in the Freedom Hosting takeover—to "identify suspects who are disguising their location using proxy servers or anonymity services, like Tor."[44]

Why Anonymize Activity?

A number of reasons have been cited why individuals might use services such as Tor to anonymize online activity. Anonymizing services have been used for legal and illegal activities ranging from keeping sensitive communications private to selling illegal drugs. Of note, while a wide range of legitimate uses of Tor exist, much of the research on and concern surrounding anonymizing services involves their use for illegal activities. As such, the bulk of this section focuses on the illegal activities.

Online Privacy

Tor is used to secure the privacy of activities and communications in a number of realms. Privacy advocates generally promote the use of Tor and similar software to maintain free speech, privacy, and anonymity.[45] There are several examples of how it might be used for these purposes:

- **Anti-Censorship and Political Activism.** Tor may be used as a "censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content."[46] Because individuals may rely upon Tor to access content that may be blocked in certain parts of the world, some governments have reportedly suggested tightening regulations around using Tor.[47] Some have purportedly

[40] Sean Gallagher, "Anonymous Takes Down Darknet Child Porn Site on Tor Network," *ArsTechnica*, October 23, 2011.

[41] Ibid. A denial-of-service attack attempts to prevent legitimate users from accessing a resource—in this case a network or website. This is most commonly done by "flooding" a network with information and overloading the server with so many requests for information that it cannot process other, legitimate requests. A distributed denial-of-service (DDoS) attack utilizes other computers—often from unwitting individuals—to assist in flooding a network. For more information, see the U.S. Computer Emergency Readiness Team, http://www.us-cert.gov/cas/tips/ST04-015.html.

[42] Mathew Schwartz, "Anonymous Attacks Child Pornography Websites," *InformationWeek*, October 24, 2011.

[43] Kevin Poulsen, "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack," *Wired.com*, September 13, 2013.

[44] Ibid.

[45] Cooper Quintin, *7 Things You Should Know About Tor*, Electronic Frontier Foundation, July 1, 2014.

[46] Tor Project, *Tor: Overview*, https://www.torproject.org/about/overview.html.en.

[47] See, for example, Jeff Stone, "Russian Censorship: Tor, Anonymous VPNs Could Be Target Of Next Crackdown, (continued...)

blocked access to it.[48] Political dissidents may also use Tor to secure and anonymize their communications and locations, as they have reportedly done in dissident movements in Iran and Egypt.[49]

- **Sensitive Communication.** Tor may also be used by individuals who want to access chat rooms and other forums for sensitive communications—both for personal and business uses. Individuals may seek out a safe haven for discussing private issues such as victimization or physical or mental illnesses. They may also use Tor to protect their children online by concealing the IP addresses of children's activities.[50] Businesses may use it to protect their projects and help prevent spies from gaining a competitive advantage.[51]
- **Leaked Information.** Journalists may use Tor for communicating "more safely with whistleblowers and dissidents."[52] *The New Yorker*'s Strongbox, for instance, is accessible through Tor and allows individuals to communicate and share documents anonymously with the publication.[53] In addition, Edward Snowden reportedly used Tails (an "operating system optimized for anonymity")—which automatically runs Tor—to communicate with journalists and leak classified information on U.S. mass surveillance programs.[54] Among the documents leaked by Snowden was a top-secret presentation outlining National Security Agency (NSA) efforts to exploit the Tor browser and de-anonymize users.[55]

Illegal Activity and the Dark Web

Just as nefarious activity can occur through the Surface Web, it can also occur on the Deep Web and Dark Web. A range of malicious actors leverage cyberspace, from criminals to terrorists to state-sponsored spies. The web can serve as a forum for conversation, coordination, and action. Specifically, they may rely upon the Dark Web to help carry out their activities with reduced risk of detection. While this section focuses on *criminals* operating in cyberspace, the issues raised are certainly applicable to other categories of malicious actors.

Twenty-first century criminals increasingly rely on the Internet and advanced technologies to further their criminal operations.[56] For instance, criminals can easily leverage the Internet to carry out traditional crimes such as distributing illicit drugs and sex trafficking. In addition, they exploit

(...continued)

Kremlin Warns," *International Business Times*, February 12, 2015.

[48] China, for instance, has reportedly been able to block access to Tor. See, for example, Tor blog, *A Closer Look at the Great Firewall of China*, October 6, 2014.

[49] Free Software Foundation, "2010 Free Software Awards Announced," press release, March 22, 2011.

[50] Tor Project, *Tor: Who Uses Tor*, https://www.torproject.org/about/torusers.html.en.

[51] Tor Project, *Tor: Overview*, https://www.torproject.org/about/overview.html.en.

[52] Ibid.

[53] *The New Yorker*, Strongbox, https://projects.newyorker.com/strongbox/.

[54] Klint Finley, "Out in the Open: Inside the Operating System Edward Snowden Used to Evade the NSA," *Wired.com*, April 14, 2014.

[55] Bruce Schneier, "Attacking Tor: How the NSA Targets Users' Online Anonymity," *The Guardian*, October 4, 2013.

[56] For more information on cybercrime, see CRS Report R42547, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*, by Kristin Finklea and Catherine A. Theohary.

the digital world to facilitate crimes that are often technology driven, including identity theft, payment card fraud, and intellectual property theft. The FBI considers high-tech crimes to be the most significant crimes confronting the United States.[57]

The Dark Web has been cited as facilitating a wide *variety* of crimes. Illicit goods such as drugs, weapons, exotic animals, and stolen goods and information are all sold for profit. There are gambling sites, thieves and assassins for hire, and troves of child pornography.[58] Data on the prevalence of these Dark Web sites, however, are lacking. Tor estimates that only about 1.5% of Tor users visit hidden services/Dark Web pages.[59] The actual percentage of these that serve a particular illicit market at any one time is unclear, and it is even less clear how much Tor traffic is going to any given site.

- One study from the University of Portsmouth examined Tor traffic to hidden services. Researchers "ran 40 'relay' computers in the Tor network ... which allowed them to assemble an unprecedented collection of data about the total number of Tor hidden services online—about 45,000 at any given time—and how much traffic flowed to them."[60] While about 2% of the Tor hidden service websites identified were sites that researchers deemed related to child abuse, 83% of the visits to hidden services sites were to these child abuse sites—"just a small number of pedophilia sites account for the majority of Dark Web http traffic."[61] As has been noted, however, there are a number of variables that may have influenced the results.[62]

The Dark Web can play a number of *roles* in malicious activity. As noted, it can serve as a forum—through chat rooms and communication services—for planning and coordinating crimes. For instance, there have been reports that some of those engaged in tax-refund fraud discussed techniques on the Dark Web.[63] The Dark Web can also provide a platform for criminals to sell illegal or stolen goods. Take the role of the Dark Web in data breaches, for example:

- Malware used in large-scale data breaches to capture unencrypted credit and debit card information has been purchased on the Dark Web. One form of malware, RAM scrapers, can be purchased and remotely installed on point-of-sale systems, as was done in the 2013 Target breach, among others.[64]

[57] See remarks by James B. Comey, Director, Federal Bureau of Investigation before the RSA Cyber Security Conference, San Francisco, CA, February 26, 2014.

[58] See, for example, Michael Chertoff and Toby Simon, *The Impact of the Dark Web on Internet Governance and Cyber Security*, Global Commission on Internet Governance, Paper Series: No. 6, February 2015.

[59] Tor Project Blog, *Tor: 80 Percent of ??? Percent of 1-2 Percent Abusive*, December 30, 2014. See also Andy Greenberg, "No, Department of Justice, 80 Percent of Tor Traffic is Not Child Porn," *Wired.com*, January 28, 2015.

[60] Andy Greenberg, "Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds," *Wired.com*, December 30, 2014. A majority of traffic to the Tor hidden services came from botnets, most of which were defunct. Researchers evaluated the remaining non-automated traffic.

[61] Ibid.

[62] Ibid. Some traffic to these sites may have come from law enforcement tracking criminals or hackers launching denial of service attacks against these sites, for instance.

[63] Brian Krebs, "Tax Fraud Advice, Straight From the Scammers," *Krebs on Security*, March 24, 2015.

[64] Kim Zetter, "How RAM Scrapers Work: The Sneaky Tools Behind the Latest Credit Card Hacks," *Wired.com*, September 30, 2014.

- Thieves can sell stolen information for profit on the Dark Web. For instance, within weeks of the Target breach, the underground black markets were reportedly "flooded" with the stolen credit and debit card account information, "selling in batches of one million cards and going for anywhere from $20 to more than $100 per card."[65] Such "card shops" are just one example of the specialty markets on the Dark Web.
- Not only can data be stolen and sold through the Dark Web, it can happen *quickly*. In a recent experiment by a security vendor, BitGlass, researchers created a treasure trove of fake "stolen" data including over 1,500 names, social security numbers, credit card numbers, and more. They then planted these data on DropBox and seven well-known black market sites. Within 12 days, the data had been viewed nearly 1,100 times across 22 countries.[66]

Cybercriminals can victimize individuals and organizations alike, and they can do so without regard for borders. How criminals exploit borders is a perennial challenge for law enforcement, particularly as the concept of borders and boundaries has evolved.[67]

Physical Borders. For law enforcement purposes, jurisdictional boundaries have been drawn between nations, states, and other localities. Within these territories, various enforcement agencies are designated authority to administer justice. When crimes cross boundaries, a given entity may no longer have sole responsibility for criminal enforcement, and the laws across jurisdictions may not be consistent.[68] Criminals have long understood these phenomena—and exploited them.

Physical–Cyber Borders. The relatively clear borders within the physical world are not always replicated in the virtual realm. High-speed Internet communication has not only facilitated the growth of legitimate business, but it has bolstered criminals' abilities to operate in an environment where they can broaden their pool of potential targets and rapidly exploit their victims. Frauds and schemes that were once conducted face-to-face can now be carried out remotely from across the country or even across the world. For instance, criminals can rely upon botnets[69] to target victims across the globe without crossing a single border themselves.

Cyber Borders. While cyberspace crosses physical borders, boundaries *within* cyberspace—both jurisdictional and technological—still exist. Some web addresses, for instance, are country-specific, and the administration of those websites is controlled by particular nations. Another barrier in cyberspace involves the lines between the Surface Web and the Deep Web. Crossing these boundaries may involve subscriptions or fee-based access to particular website content.

---

[65] Brian Krebs, "Cards Stolen in Target Breach Flood Underground Markets," *Krebs on Security*, December 20, 2013.

[66] Kelly Jackson Higgins, "What Happens When Personal Information Hits The Dark Web," *Information Week*, April 7, 2015. See also Pierluigi Paganini, "How Far Do Stolen Data Get in the Deep Web After a Breach?," *Security Affairs*, April 12, 2015.

[67] CRS Report R41927, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*, by Kristin Finklea.

[68] For more information, see Daniel C. Richman, "The Changing Boundaries Between Federal and Local Law Enforcement," *Boundary Changes in Criminal Justice Organizations*, pp. 81-111, http://www.ncjrs.gov/criminal_justice2000/vol_2/02d2.pdf.

[69] Botnets are groups of computers that are remotely controlled by hackers. They have been infected by downloading malicious software and are used to carry out malicious activities on behalf of the hackers.

Certain businesses—news sites, journals, file-sharing sites, and others—may require paid access. Other sites may only be accessed through an invitation.

Do malicious actors need, or benefit from, the Dark Web to carry out their activities? Researchers have pointed to pros and cons of relying upon the anonymity of the Dark Web. Criminals selling illicit goods may benefit from the Dark Web's added protection of anonymity by being better able to evade law enforcement. However, they may have more trouble getting business. Trend Micro's 2013 study of the Dark Web notes that on it, "[s]ellers suffer from lack of reputation caused by increased anonymity. Being untraceable can present drawbacks for a seller who cannot easily establish a trust relationship with customers unless the marketplace allows for it."[70] In other words, anonymity can be a barrier online if one is trying to sell goods and has not been otherwise vetted.

Payment on the Dark Web

Bitcoin is the currency often used in transactions on the Dark Web.[71] It is a decentralized digital currency that uses anonymous, peer-to-peer transactions.[72] Individuals generally obtain bitcoins by accepting them as payment, exchanging them for traditional currency, or "mining" them.[73]

When a bitcoin is used in a financial transaction, the transaction is recorded in a public ledger, called the block chain. The information recorded in the block chain is the bitcoin addresses of the sender and recipient. An address does not uniquely identify any particular bitcoin; rather, the address merely identifies a particular transaction.[74]

Users' addresses are associated with and stored in a wallet.[75] The wallet contains an individual's private key,[76] which is a secret number that allows that individual to spend bitcoins from the corresponding wallet,[77] similar to a password. The address for a transaction and a cryptographic signature are used to verify transactions.[78] The wallet and private key are not recorded in the public ledger; this is where Bitcoin usage has heightened privacy. Wallets may be hosted on the web, by software for a desktop or mobile device, or on a hardware device.[79]

---

[70] Vincenzo Ciancaglini, Marco Balduzzi, and Max Goncharov, et al., *Deepweb and Cybercrime: It's Not All About TOR*, Trend Micro, p. 21.

[71] Pierluigi Paganini, "What is the Deep Web? A First Trip Into the Abyss," *Security Affairs*, May 24, 2012. Of note, a number of digital currencies exist, though Bitcoin is the most prominent. These currencies include Ripple and Litecoin, among others. See https://coinmarketcap.com/.

[72] For more information on Bitcoin, see CRS Report R43339, *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, by Craig K. Elwell, M. Maureen Murphy, and Michael V. Seitzinger. See also Timothy Lee, "12 Questions About Bitcoin You Were Too Embarrassed To Ask," *The Washington Post*, November 19, 2013.

[73] More information is available at https://bitcoin.org/en/faq#how-does-one-acquire-bitcoins.

[74] If users are concerned with attribution to themselves from multiple bitcoin transactions, a new address can be used for each transaction. See "Protect your privacy" at https://bitcoin.org/en/protect-your-privacy.

[75] Elli Androulaki et al., Evaluating User Privacy in Bitcoin, ETH Zurich and NEC Laboratories Europe, n.d., at http://fc13.ifca.ai/proc/1-3.pdf.

[76] See "Some Bitcoin words you might hear," https://bitcoin.org/en/vocabulary/.

[77] See, "Elliptical Curve Digital Signature Algorithm," https://en.bitcoin.it/wiki/ECDSA.

[78] These transactions are confirmed by miners. See "Some Bitcoin words you might hear," https://bitcoin.org/en/vocabulary/.

[79] For information on different types of wallets, see https://bitcoin.org/en/choose-your-wallet.

Government Use of the Dark Web

Because of the anonymity provided by Tor and other software such as I2P, the Dark Web can be a playground for nefarious actors online. As noted, however, there are a number of areas in which the study and use of the Dark Web may provide benefits. This is true not only for citizens and businesses seeking online privacy, but also for certain government sectors—namely the law enforcement, military, and intelligence communities.

Law Enforcement

Just as criminals can leverage the anonymity of the Dark Web, so too can law enforcement. It may use this to conduct online surveillance and sting operations and to maintain anonymous tip lines.[80] While individuals may anonymize activities, some have speculated about means by which law enforcement can still track malicious activity.

As noted, the FBI has put resources into developing malware that can compromise servers in an attempt to identify certain users of Tor. Since 2002, the FBI has reportedly used a "computer and internet protocol address verifier" (CIPAV) to "identify suspects who are disguising their location using proxy servers or anonymity services, like Tor."[81] It has been using this program to target "hackers, online sexual predators, extortionists, and others."[82]

In addition to developing technology to infiltrate and deanonymize services such as Tor, law enforcement may rely upon more traditional crime fighting techniques; some have suggested that law enforcement can still rely upon mistakes by criminals or flaws in technology to target nefarious actors. For instance, in 2013 the FBI took down the Silk Road, then the "cyber-underworld's largest black market."[83] Reportedly, "missteps" by the site's operator led to its demise; some speculate that "federal agents found weaknesses in the computer code used to operate the Silk Road website and exploited those weaknesses to hack the servers and force them to reveal their unique identifying addresses. Federal investigators could then locate the servers and ask law enforcement in those locations to seize them."[84]

Less than one month after federal agents disbanded the Silk Road, another site (Silk Road 2.0) came online. After discovering that the site's proprietor made critical errors, such as using his personal email address to register the servers, federal agents seized the servers and shut down the site.[85] While law enforcement may aim to defeat criminals operating in the Dark Web technologically, some of their strongest tools may be traditional law enforcement crime-fighting means. For example, law enforcement can still request information from entities that collect identifying information on users. In March 2015, federal investigators "sent a subpoena to Reddit demanding that the site turn over a collection of personal data about five users of the

[80] Michael Chertoff and Toby Simon, *The Impact of the Dark Web on Internet Governance and Cyber Security*, Global Commission on Internet Governance, Paper Series: No. 6, February 2015.

[81] Kevin Poulsen, "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack," *Wired.com*, September 13, 2013.

[82] Ibid.

[83] Donna Leinwand Leger, "How FBI Brought Down Cyber-Underworld Site Silk Road," *USA Today*, May 15, 2014.

[84] Ibid.

[85] Brian Krebs, "Feds Arrest Alleged 'Silk Road 2 Admin,' Seize Servers," *Krebs on Security*, November 6, 2014.

r/darknetmarkets forum [a subreddit where users discussed anonymous online sales of drugs, weapons, stolen financial data, and other contraband]."[86] Though, as some have suggested, such law enforcement actions could drive these conversations and activities to anonymous forums such as those on Tor.[87]

Military and Intelligence

Anonymity in the Dark Web can be used to shield military command and control systems in the field from identification and hacking by adversaries. The military may use the Dark Web to study the environment in which it is operating as well as to discover activities that present an operational risk to troops. For instance, evidence suggests that the Islamic State (IS) and supporting groups seek to use the Dark Web's anonymity for activities beyond information sharing, recruitment, and propaganda dissemination, using Bitcoin to raise money for their operations.[88] In its battle against IS, the Department of Defense (DOD) can monitor these activities and employ a variety of tactics to foil terrorist plots.

Tor software can be used by the military to conduct a clandestine or covert computer network operation such as taking down a website or a denial of service attack, or to intercept and inhibit enemy communications. Another use could be a military deception or psychological operation, where the military uses the Dark Web to plant disinformation about troop movements and targets, for counterintelligence, or to spread information to discredit the insurgents' narrative. These activities may be conducted either in support of an ongoing military operation or on a stand-alone basis.

DOD's Defense Advanced Research Projects Agency (DARPA) is conducting a research project, called Memex, to develop a new search engine that can uncover patterns and relationships in online data to help law enforcement and other stakeholders track illegal activity. Commercial search engines such as Google and Bing use algorithms to present search results by popularity and ranking, and are only able to capture approximately 5% of the Internet.[89] By sweeping websites that are often ignored by commercial search engines, and capturing thousands of hidden sites on the Dark Web, the Memex project ultimately aims to build a more comprehensive map of Internet content.

Similar to the military's use of the Dark Web, the Intelligence Community's (IC's) use of it as a source of open intelligence is not a secret, though many associated details are classified. According to Admiral Mike Rogers, Director of the National Security Agency (NSA) and Commander of U.S. Cyber Command, they "spend a lot of time looking for people who don't want to be found."[90] Reportedly, an investigation into the NSA's XKeyscore program—one of the programs revealed by Edward Snowden's disclosure of classified information—demonstrated that

[86] Andy Greenberg, "Feds Demand Reddit Identify Users of a Dark-Web Drug Forum," *Wired.com*, March 30, 2015. Reddit is not anonymous and does collect information from users who create accounts.

[87] Ibid.

[88] Patrick Tucker, "How the Military Will Fight ISIS on the Dark Web," *Defense One*, February 24, 2015,

[89] Kim Zetter, "DARPA Is Developing A Search Engine or the Dark Web," *Wired.com*, February 10, 2015.

[90] Interview of Admiral Michael S. Rogers by Jim Sciutto, New America Foundation Conference on Cybersecurity, February 23, 2015, responding to a question concerning the IC's use of the Dark Web.

any user attempting to download Tor was automatically fingerprinted electronically, allowing the agency to conceivably identify users who believe themselves to be untraceable.[91]

While specific IC activities associated with the Deep Web and Dark Web may be classified, at least one program associated with Intelligence Advanced Research Projects Activity (IARPA) may be related to searching data stored on the Deep Web.[92] According to the IARPA website, the IC's "established approaches (e.g., signature-based detection, anomaly detection)" are inadequate for the task of anticipating and "mitigating the 'cause' of cyber-attacks."[93] The Cyber-attack Automated Unconventional Sensor Environment (CAUSE) program "seeks to develop cyber-attack forecasting methods and detect emerging cyber phenomena to assist cyber defenders with the earliest detection of a cyber-attack." It will use factors such as actor behavior models and black market sales to help forecast and detect cyber events.

Going Forward

The Deep Web and Dark Web have been of increasing interest to researchers, law enforcement, and policy makers. However, clear data on the scope and nature of these layers of the Internet are unavailable; anonymity often afforded by services such as Tor for users accessing the deepest corners of the web contributes to this lack of clarity, as does the sometimes temporary nature of the websites hosted there. Individuals, businesses, and governments may all rely upon the digital underground. It may be used for legal and illegal activities ranging from keeping sensitive communications private to selling illegal contraband. Despite some reaching for increased privacy and security online, researchers have questioned whether there will be a corresponding uptick in individuals turning to anonymizing services such as Tor.[94] They've suggested that while there may not be the incentive for individuals to migrate their browsing to these anonymizing platforms, "it is much more likely for technological developments related to the Dark Web to improve the stealthiness of darknets."[95] As such, law enforcement and policy makers may question how best to contend with evolving technology such as encryption and the challenges of attribution in an anonymous environment to effectively combat malicious actors who exploit cyberspace, including the Dark Web.

Author Contact Information

Kristin Finklea
Specialist in Domestic Security
kfinklea@crs.loc.gov, 7-6259

[91] Patrick Tucker, "If You Do This, the NSA Will Spy on You," *Defense One*, July 7, 2014.

[92] IARPA is the research and development arm of the Office of the Director of National Intelligence (ODNI). IARPA invests in "high-risk, high-payoff" research programs. More information is available at http://www.iarpa.gov.

[93] "Cyber-attack Automated Unconventional Sensor Environment (CAUSE)," IARPA website at http://www.iarpa.gov/index.php/research-programs/cause.

[94] Vincenzo Ciancaglini, Marco Balduzzi, and Robert McArdle, et al., *Below the Surface: Exploring the Deep Web*, Trend Micro, June 2015.

[95] Ibid., p. 40.

Acknowledgments

CRS colleagues Stephanie Logan, Anne Daugherty Miles, Rita Tehan, Catherine Theohary, and Eric Weiss contributed to this report.