Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated December 2, 2024

The Dark Web: An Overview

Many observers of the World Wide Web (web) have described it as having layers. One layer, the *surface web*, contains indexed content easily accessible with a traditional search engine such as Google. Another layer, the *deep web*, contains unindexed content that cannot be accessed with a simple Google search. Within the deep web is a segment known as the *dark web*—a layer where content is 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 particular interest from law enforcement officials and policymakers.

Layers of the Web

Many consider the internet and web to be synonymous; they are not. The web is just one portion of the internet, and a medium through which information may be accessed. (The internet is also used for email, file transfers, and direct messaging, among other things.)

- Within the web, one portion is known as the *surface web*, comprised of content that has been indexed and is accessible through traditional search engines such as Google.

- Another portion of the web is the *deep web*, which contains content that has not been indexed and thus is not accessible through traditional search engines. This includes content on private intranets (internal networks such as those at corporations, government agencies, or universities), and commercial databases like Westlaw. Accessing this content often requires authentication (i.e., verification of the user's identity) and permission to access the content.

- Within the deep web is the *dark web*, the segment of the deep web that has been intentionally hidden. It refers to internet sites that users generally cannot access without using special software. While the content of these sites may be accessed using this software, publishers of these sites are often concealed. Users access the dark web with the expectation of being able to share information and/or files with little risk of detection.

Accessing and Navigating the Dark Web

The dark web can be reached through decentralized, anonymized nodes on various networks including Tor (short for The Onion Router) or I2P (Invisible Internet Project). Tor, which was initially released as The Onion Routing project in 2002, was originally created by the U.S. Naval Research Laboratory as a tool for anonymously communicating online. Some privacy and security advocates have noted that using Tor may not be completely anonymous (e.g., some internet service providers can see that an individual is using Tor—but not the content) and have suggested that using Tor in conjunction with a virtual private network (VPN) can provide additional privacy because a VPN may conceal internet activity, including the use of Tor.

How Tor Works

Tor works by routing users' web traffic through other users' computers, thus connecting to internet sites indirectly rather than directly and preventing the traffic from being traced to the original user. To do this, Tor creates layers (like layers of an onion) and routes traffic through those layers to conceal users' identities. To get from layer to layer, Tor establishes *relays* on computers around the world through which information passes. Information is encrypted between relays and is routed through three relays before reaching its destination. 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.

While data on the magnitude of the deep web and dark web and how they relate to the surface web are unclear, 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 10 months of 2024 was 430,054—or 13.7% of total mean daily Tor users worldwide. The United States had the second largest number of mean daily Tor users during this time period, behind Germany (37.7%) and ahead of Finland (3.7%), the Netherlands (3.5%), and India (2.7%).

Navigating the Dark Web

Traditional search engines often use web crawlers to access websites on the surface web. Web crawlers search the web and gather websites that the search engines can then catalog and index. Content on the deep web 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. As such, there are different mechanisms for navigating the deep web and the dark web. Users often navigate dark websites 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. For instance, Ahmia searches across hidden services on the Tor network, and Kilos searches markets, known as *darknet markets*, notorious for serving the cybercriminal underground.

Tor is often slower than other web browsers, in part because Tor traffic is routed through multiple relays and

there can be delays anywhere along its path. Speed can also be reduced when more users are simultaneously on the Tor network. However, increases in users who allow the use of their computers as relays can improve the speed on Tor. There are also tools—such as Tor2web—that may allow access to Tor-hosted content without downloading and installing the Tor software, but these tools do not have the Tor-related privacy protections.

Anonymity and the Dark Web

Anonymity on the dark web is not guaranteed. While tools such as Tor aim to anonymize content and activity, researchers, security experts, hackers, law enforcement, and other officials are constantly developing means by which certain hidden services or individuals could be identified, or *deanonymized*. For instance, law enforcement uses *network investigative techniques*, their term for specially designed malware engineered to take advantage of a specific technology vulnerability and bypass anonymity protections.

Reasons for Anonymizing Online Activity

A number of reasons have been cited for 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 illicit contraband.

Individuals around the world may use internet-based anonymizing services to maintain free speech, privacy, and anonymity. For instance, they may use them as anti-censorship tools to reach and share blocked content or to conduct political activism online as part of dissident movements. Individuals may use Tor and similar services to seek out forums for discussing private issues such as victimization or physical or mental illnesses, and businesses may use them to protect their projects from spies and others who may try to gain a competitive advantage. Journalists may also rely on anonymizing services to communicate with dissidents or whistleblowers who may want to conceal their identity or share leaked documents.

Anonymizing services and the dark web may also be used for nefarious activity. Just as criminal activity can occur through the surface web, it occurs on the deep web and dark web. A range of malicious actors, from criminals to terrorists to state-sponsored spies, leverage cyberspace. The web can serve as a forum for conversation, coordination, and action, and malicious actors may rely on the dark web to help carry out their activities with reduced risk of detection.

Much of the illicit activity on the dark web occurs on darknet markets, where administrators provide a forum for buyers and sellers to communicate and leverage transactions. In some arenas, such as illicit drug sales, vendors rely on reviews from buyers to build their brand and customer base just like they do on the surface web. Researchers have examined the types of malicious activity facilitated through darknet markets, and they have identified some of the major market categories to include illicit drugs (e.g., marijuana, cocaine, methamphetamine, heroin, fentanyl, other illicit opioids); pharmaceuticals (e.g., prescription medication, recalled drugs, unregulated supplements); falsified documents and counterfeits (e.g., materials for creating a fake identity); fraud (e.g., the sale of personal information, credentials, or accounts); hacking and exploits (e.g., malicious software, exploit kits, hackers for hire); exploitation (e.g., child sexual abuse material—distinct from explicit content such as legal pornography); and markets with multiple types of illicit activity (those akin to an Amazon-style site for illicit goods on the dark web). Cryptocurrency, such as Bitcoin and Monero, is the common form of payment on darknet markets.

Investigations and the Dark Web

Just as criminals can leverage the anonymity of the dark web, so too can law enforcement. They can use it to conduct online surveillance and sting operations and to maintain anonymous tip lines. Federal investigations of dark web cases are often multiagency initiatives. For instance, the Joint Criminal and Opioid Darknet Enforcement (JCODE) team is a Department of Justice (DOJ) initiative, led by the Federal Bureau of Investigation (FBI), which coordinates federal investigations focused on dismantling online sales of illicit drugs—particularly opioids—and other illicit goods. In April 2022, the JCODE team supported and helped coordinate the multiagency investigation and seizure of the Hydra Market, which DOJ described as "the world's largest and longest-running darknet market." Hydra enabled users, largely in Russian-speaking countries, to trade in illicit goods and services such as illicit drugs, stolen financial information, and fraudulent identification documents. Reportedly, Hydra accounted for about 80% of darknet market-related cryptocurrency transactions in 2021, and had amassed about $5.2 billion since 2015.

Researchers have helped identify areas in which law enforcement can improve dark web investigations. DOJ's National Institute of Justice, through the RAND Corporation and Police Executive Research Forum, sponsored an expert's workshop to identify law enforcement's high-priority needs with respect to dark web investigations. Recommendations included enhancing training for investigators to spot dark web evidence, improving information sharing between agencies, examining new structures for cross-agency cooperation, developing new standards for collecting dark web evidence, modernizing laws regarding inspections of mail and overseas packages, and increasing research on the relationship between traditional crime and less-visible crime facilitated by the dark web.

Concluding Observations

Policymakers may question how best to contend with evolving technology, such as the challenges of attribution in an anonymous environment, to effectively combat malicious actors who exploit cyberspace, including the dark web. Congress may look to recommendations from researchers and law enforcement as it debates whether or how to bolster knowledge regarding criminal activity online and support law enforcement's dark web investigations.

For more information, see CRS Report R44101, *Dark Web*.

Kristin Finklea, Specialist in Domestic Security

Disclaimer