THE TRUTH ABOUT THE DARK WEB

Intended to protect dissidents, it has also cloaked illegal activity

Aditi Kumar and Eric Rosenbach

In the late 1990s, two research organizations in the US Department of Defense drove efforts to develop an anonymized and encrypted network that would protect the sensitive communications of US spies. This secret network would not be known or accessible to ordinary internet surfers. And while the original clandestine intention was never fully realized, some of the researchers saw a different value proposition at hand—launching a nonprofit focused on anonymity for human rights and privacy activists.

Enter the Tor network, short for “The Onion Router,” given the many layers of encryption that guard passing information. Tor lives on the fringe of the internet and serves as the underlying technology of the dark web—a collection of hidden sites inaccessible via a regular browser and not indexed by search engines such as Google. The Tor browser—a free download—is all you need to unlock this hidden corner of the web where privacy is paramount. Radical anonymity, however, casts a long shadow.

The truth about the dark web is that in addition to offering extreme privacy and protection from the surveillance of authoritarian governments, it facilitates a growing underground marketplace that sophisticated criminals use to traffic drugs, stolen identities, child pornography, and other illicit products and services. And with untraceable cryptocurrency as the primary means of payment, close cooperation between law enforcement, financial institutions, and regulators around the world is required to tighten the screws on nefarious activity.

The gray areas

Today, over 65,000 unique URLs ending with .onion exist on the Tor network. A 2018 study by computer security firm Hyperion Gray catalogued about 10 percent of these sites and found that the most prevalent functions facilitate communication via forums, chat rooms, and file and image hosts, as well as commerce via marketplaces. These functional roles, particularly related to communication, support many uses that are considered legal and legitimate in free societies. Furthermore, a 2016 study by research firm Terbium Labs analyzing 400 randomly selected .onion sites suggests that over half of all domains on the dark web are in fact legal.

For individuals living under oppressive regimes that block large parts of the internet or punish

political dissent, the dark web is a lifeline that provides access to information and protection from persecution. In freer societies, it can be a critical whistle-blowing and communication tool that shields people from retribution or judgment in the workplace or community. Alternatively, it can simply deliver privacy and anonymity for those wary of how corporations and governments are tracking, using, and potentially monetizing their data. Today, many organizations maintain a hidden website on Tor, including nearly every major newspaper, Facebook, and even the US Central Intelligence Agency (CIA). This is because a Tor website demonstrates a (sometimes symbolic) commitment to privacy. The *New York Times* and the CIA, for example, are both hoping to facilitate communication with virtual walk-ins who can provide sensitive information.

For individuals living under oppressive regimes that block large parts of the internet or punish political dissent, the dark web is a lifeline.

On the flip side, the same privacy and anonymity that deliver protection from tyrants and targeted advertisements also make the dark web a springboard for crime. Some of the more prevalent illicit activities include arms trafficking, drug dealing, and the sharing of exploitative content—often involving children—such as pornography and images of violence and other types of abuse. Websites support the rhetoric of neo-Nazis, white supremacists, and other extremist groups.

The pairing of dark web services with cryptocurrencies has led to expectations of a boom in crime. A decade ago, an unknown cryptography expert (with particular expertise in cracking passwords) who used the alias Satoshi Nakamoto developed the world's first currency and payment network not controlled by a national government: Bitcoin. Originally a niche medium of exchange for the technology community, Bitcoin emerged in 2011 as the currency of choice for drug dealers conducting transactions on a dark-web site known as the Silk Road. Over the past five years, the combination of an encrypted network hidden from most of the world and a transactional currency that is nearly untrackable by law enforcement officials resulted in a small, but significant, marketplace of illicit vendors selling illegal wares.

Of the close to 200 domains catalogued as illegal by Terbium Labs, more than 75 percent appear to be marketplaces. Many of these are fueled by Bitcoin and other cryptocurrencies, such as Monero. Recreational and pharmaceutical drugs

ART: ISTOCK / TETIANA LAZUNOVA

Many of the most corrosive threats to society today operate in the shadows of the Tor network and thus merit the attention of international investigators.

are the most popular products, followed by stolen and counterfeit documents such as identities, credit cards, and bank credentials. Some sites offer hacking and technological crime services, including malware, distributed denial of service attacks, and hacking for hire. A good number offer a mix of these and other products, including pornography and counterfeit goods.

Although the serious nature and rapid growth of illicit transactions on the dark web should concern governments and global financial institutions, the overall portion of worldwide commerce transacted on the dark web is minuscule compared with global illicit commerce. A recent report by a leading crypto-payment analytic firm, Chainalysis, shows that Bitcoin transactions on the dark web grew from approximately $250 million in 2012 to $872 million in 2018. The firm projected that Bitcoin transactions on the dark web will reach more than $1 billion in 2019. If correct, it would represent a record-setting level of illegal transactions in this arena. The report also noted that the proportion of Bitcoin transactions tied to illicit deals has declined by 6 percent since 2012 and now accounts for less than 1 percent of all Bitcoin activity. Even more broadly, the United Nations estimates that the amount of money laundered globally in one year is 2 to 5 percent of global GDP—between $1.6 trillion and $4 trillion.

Even though the total economic volume of illicit dark web activity remains relatively small, many of the most corrosive threats to society today operate in the shadows of the Tor network and thus merit the attention of international regulators, financial institutions, and law enforcement agencies.

Policing the shadows

Protecting political dissidents, privacy advocates, and whistle-blowers should not come at the expense of empowering child abusers, arms traffickers, and drug lords. Therein lies the challenge for regulators and law enforcement agencies: to devise approaches that walk the fine line of protecting liberal principles in an age of information control while identifying and eradicating the most insidious activities on the dark web. Over the past several years, the international community has made significant progress addressing these challenges by improving information sharing, sharpening law enforcement's technical capabilities to take down major illicit marketplaces, and regulating the transfer of cryptocurrency transactions.

Addressing the most nefarious activities on the dark web starts with improved information sharing among law enforcement agencies and financial institutions. The global nature of the dark web makes international cooperation imperative. During 2018–19, Interpol and the European Union brought together law enforcement agencies from 19 countries to identify 247 high-value targets and shared the type of operational intelligence necessary for enforcement. The results are promising: just this year, efforts allowed members of the group to make arrests and shut down 50

illicit dark-web sites, including Wall Street Market and Valhalla, two of the largest drug markets.

The growth of illegal dark web transactions has also spurred many governments around the world to disrupt criminal activities by improving the capabilities of domestic law enforcement agencies such as the US Federal Bureau of Investigation (FBI). For example, the FBI has reportedly conducted operations that allow it to "de-anonymize" Tor servers. The FBI does this by establishing nodes in the network that allow the agency to see the identities and locations of some illegal Tor-based webpages. The first significant action was the FBI's takedown of the "Silk Road 2.0" website, the leading illicit dark web marketplace in 2014. The investigation revealed that, during its two and a half years in operation, the site had been used by several thousand drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other illicit goods and services to well over 100,000 buyers. The site was used to launder hundreds of millions of dollars from these unlawful transactions. All told, the site had generated sales totaling more than 9.5 million in Bitcoin valued, at the time, at approximately $1.2 billion. AlphaBay and Hansa market, two of the biggest successors of Silk Road, were shut down in 2017.

Dark web enforcement capabilities have continued to grow, including a recent Dutch operation to hijack a leading dark web merchant, anonymously run it for a month, and then use the information collected to disrupt dozens of other dark web merchants.

Need for new regulations

In addition to conducting disruption operations, governments and international institutions are attempting to directly regulate the cryptocurrencies that are fueling dark web marketplaces. In June 2019, for example, the Financial Action Task Force issued guidance that urges companies processing cryptocurrency transfers to identify both the sender and receiver of fund transfers. The guidance follows the recommendation of the 2018 G20 Summit, in which leaders asked international regulatory agencies to consider policy responses for crypto assets, particularly related to know your customer, anti–money laundering, and countering the financing of terrorism. The start-up ecosystem of exchanges, wallets, and other crypto payment facilitators is far from having the necessary infrastructure to adopt such financial-sector-like standards, but supervisors need to begin laying the groundwork for enhanced scrutiny. The impending launch of Libra, Facebook's cryptocurrency, will only make this a more pressing concern as the barriers to adopting virtual assets are lowered for Facebook's nearly 2 billion-plus users.

A fine line

Authoritarian regimes will continue efforts to block access to the dark web and the threats to legitimacy that it poses by enabling dissidents and activists. Faced with this threat, the natural reflex of liberal civil societies will be to advocate that Tor remain unmonitored and unpoliced to protect free expression and privacy. The reality of the dark web is much more complicated, requiring a nuanced approach from supervisors and law enforcement agencies to thwart activities that are considered illegal and immoral in free societies, all the while protecting the very real benefits of an anonymized network.

ADITI KUMAR is the executive director of the Belfer Center for Science and International Affairs at Harvard University's John F. Kennedy School of Government. **ERIC ROSENBACH** is codirector at the Belfer Center and was previously US assistant secretary of defense for global security.