Exploring the Dark Web: Public Perception

Tuesday, February 5, 2019

by Scott Michell

Is the dark web a haven of criminal activity? Mainstream news media headlines gesture towards the actions of dangerous groups and threats to those who unwittingly find themselves in a risky online space. Headlines about the "dark web drug trade" abound (Southwick, 2017) while other articles caution parents to keep "children safe from dark web dangers" (Moore, 2018) or raise the alarm about the "'Crazy dangerous' drug" from the dark web that put a teen in the hospital (Rizzo, 2018). Many other articles promise to explain how the dark web works or push back against the idea that it is "just for paedophiles, drug dealers and terrorists" – reflecting the general lack of public awareness and widespread concerns (Murray, 2014).

This article briefly describes what the dark web is, explores the news media discourses about the dark web, and considers public perceptions.

What is the dark web?

Source: https://pixabay.com/tr/photos/korsan-siluet-kesmek-hack-anonim-3342696/

Most of us are familiar with the 'Surface Web' or visible web – the sites that are indexed by search engines like Google. It's also referred to as the 'crawlable' or 'public' web, and includes, for example, Amazon, Facebook, Reddit, or your personal public blog with the default Wordpress template that you started two years ago and never update.

The "dark web" is often conflated with the "deep web. An article about "Insider Trading on the Dark Web" from *Forbes*, for example, seems to mix the two up (Atlas, 2014). Perhaps, coming from *Forbes*, the mistake shouldn't be all that shocking. After all, they published a much-maligned article that called for shutting down public libraries because apparently Amazon is basically the same thing. But here's the difference between the dark web and the deep web: the deep web is essentially anything that a search engine can't find. The web is indexed through links, and search engines can't find pages behind search boxes or in certain databases or libraries. So unindexed deep web material might include, for example, "mundane databases such as LexisNexis or the rolls of the U.S. Patent Office" (Goodman, 2015). Some estimates claim that the deep web is 500 times larger than the surface web (Thompson, 2015), while a study in Nature found that Google indexes less than 16 percent of the surface web (and of course, misses all of the deep web).

The dark web is actually a portion of the deep web, and it's "intentionally hidden and is inaccessible through standard web browsers" (Jarmon & Yannakogeorgos, 2018, p. 56). You can't just launch Chrome or Firefox: to access the dark web (or 'dark net' as it's sometimes called), users need to go through specific software such as TOR, which stands for "The Onion Router" ("About Tor," n.d.). Yes, it sounds like a weird name, but 'onion routing' is how people navigate the dark web or communicate anonymously, with data being transmitted through a series of network nodes that each "peel" away a layer of encryption (and, you know, onions have layers). Each node or intermediary only knows the location of the previous or next node, keeping the sender anonymous.

Public perceptions

Past surveys and studies have found fairly widespread public animosity to the dark web. A survey from the Center for International Governance Innovation asked over 24,000 people in 24 countries their opinion on the dark web; it found that 71 percent of respondents thought the dark web should be shut down. The survey's authors contend that media coverage – which focuses on child pornography sites and drug markets – have negatively impacted public perceptions, overshadowing the fact that journalists, human rights activists, protestors, and whistleblowers use the dark web to circumvent state oppression, organize protests, or bring corruption to light (CIGI, 2016).

This naturally brings to mind long-standing questions about the power of 'media effects,' with early communications and media theorists contending that the public could be easily swayed through exposure to media messages; the so-called hypodermic needle theory famously described how media messages were powerfully injected into the minds of audiences. Risk perception research was essentially built on this model, with early risk theorists arguing that public perceptions of hazards were largely constructed through exposure to various 'signs' and 'symbols' that signified risk (Kasperson et al., 1988). In the following decades, work on media effects attempted to present a more nuanced and complex relationship, exploring how the quantity of coverage on a certain issue may impact public perceptions (Young et al., 2008), describing the news media as providing an interpretative framework to the public which could subtly influence beliefs (Tomes, 2002), or characterizing the various social and cultural factors that intersect with media representations to shape perceptions (Orbe, 2016).

All this is to say that although public perceptions of the dark web can't be reduced to the impact of media messages, it would seem as though there is a relationship between the widespread conception that the dark web is mostly used for harmful, illegal activities, and the predominately negative news coverage – which almost exclusively focuses on dangerous drugs that have harmed teenagers, or pedophiles distributing child pornography. There is indeed criminal activity on the dark web, yet there is much less news coverage about other uses: human rights activists fighting against oppressive governments who use TOR to access sites like Facebook or to blog anonymously, or whistleblowers who share files with journalists to expose corruption. Interestingly enough, some researchers have found that awareness of privacy issues is a predictor of someone being less opposed to the dark web (Jardine, 2017).

Public perceptions of the dark web matter, because these beliefs influence policymakers and push them towards policies that would harm human rights activists and journalists, such as the announcement in the U.K. that the National Crime Agency, alongside a new police and intelligence unit, would be set up to police the dark web (NCA, 2018).

Some of the recent proposed policies aiming to take on the dark web may have also been inspired, at least in part, by studies that have claimed more than 80% of dark web traffic is to child abuse sites (Owen & Savage, 2014). Yet commentators were quick to point out that this was characterizing total traffic – not the proportion of dark web users – and the online habits of different types of users could have distorted the findings. As Nick Mathewson described:

> Suppose 10 people use hidden services to look at conspiracy theories, 100 people use hidden services to buy Cuban cigars, and 1000 people use it for online chat. But suppose that the average cigar purchaser visits only one or two sites to make purchases, and the average chat user joins one or two networks, whereas the average conspiracy theorist needs to visit several dozen forums and wikis (Mathewson, 2014).

Others have raised concerns that policymakers may be feeding into the sensationalism and public fear, to galvanize support for infiltrating the dark web and stripping away the anonymity of TOR – not because of concerns around criminal activity, but rather, as part of longstanding efforts by intelligence agencies to subvert these privacy tools. Policymakers might argue that shining a light on the dark web will prevent criminals and terrorists from hiding their actions – yet it would also dismantle an important tool for journalists and activists, or at least, make it a shadow of its former self.

Works Cited

About Tor. (n.d.). Retrieved from: https://www.torproject.org/about/overview.html.en

Atlas, J. (2014, March 25). Insider Trading On The Dark Web. Forbes. Retrieved from: https://www.forbes.com/sites/realspin/2014/03/25/insider-trading-on-the-dark-web/#264a8d7a6a61

CIGI-Ipsos Global Survey on Internet Security and Trust. (2016). Retrieved from: https://www.cigionline.org/internet-survey-2016

Goodman, M. (2015). Future Crimes: How Our Radical Dependence on Technology Threatens Us All. Toronto, Canada: Doubleday Canada.

Jardine, E. (2018). Privacy, censorship, data breaches and internet freedom: The drivers of support and opposition to dark web technologies.*New Media & Society,20*(8), 2824-2843.

Jarmon, J.A., & Yannakogeorgos, P. (2018). The Cyber Threat and Globalization: The Impact on U.S. National and International Security. New York, NY: Rowman & Littlefield.

Mathewson, N. (2014, December 30). Some thoughts on Hidden Services. Tor Blog. Retrieved from: https://blog.torproject.org/some-thoughts-hidden-services

Moore, S. (2018, October 2). Keep your children safe from dark web dangers. ABC10. Retrieved from: https://www.abc10.com/article/news/local/keep-your-children-safe-from-dark-web-dangers/103-600249384

Murray, A. (2014, December 12). The dark web is not just for paedophiles, drug dealers and terrorists. Independent. Retrieved from: https://www.independent.co.uk/voices/comment/the-dark-web-is-not-just-for-paedophiles-drug-dealers-and-terrorists-9920667.html

NCA (2018). Boost to operations against dark web criminality. National Crime Agency. Retrieved from: www.nationalcrimeagency.gov.uk/news/1326-boost-to-law-enforcement-s-operations-against-dark-web-criminality

Owen, G., & Savage, N. (2015). The Tor Dark Net. Global Commission on Internet Governance. Retrieved from: https://www.cigionline.org/sites/default/files/no20_0.pdf

Rizzo, T. (2018, October 31). 'Crazy dangerous' drug from dark web put teen in hospital. The Kansas City Star. Retrieved from: https://www.kansascity.com/news/local/crime/article220843385.html

Southwick, R. (2017). Inside the dark web drug trade. CBC. Retrieved from: https://newsinteractives.cbc.ca/longform/the-new-frontier-of-the-drug-trade

Thompson, C. (2015, December 16). Beyond Google: Everything you need to know about the hidden internet. Business Insider. Retrieved from: https://www.businessinsider.com/difference-between-dark-web-and-deep-web-2015-11?r=UK

About the author

Scott Mitchell

A former newspaper columnist and writer, blogger, and cartoonist with Maclean's magazine, Scott Mitchell is a PhD student in Carleton University's School of Journalism and Communication. His research interests include public communication of science, risk communication, social and digital media platforms, and visual culture. His current research is examining how contagious diseases such as Ebola are visually constructed across news, social, and entertainment media, and how this may impact public health responses. When he's not busy boring people with lengthy descriptions of his research interests, Scott enjoys making illustrations, infographics, and animations that are also related to his research interests.

Scott Mitchel is ALiGN researcher, writer, and cartoonist.

Tuesday, February 5, 2019 | Categories: Illuminate, Issue I: Exploring the Dark Web
Post tagged with Dark Web, Darknet, Digital Technologies, Governance, Policy, TOR
Share: Twitter, Facebook
Short URL: https://carleton.ca/align/?p=1687