



## The “DarkNet” Quandary

P2P2-W04: The “Darknet” Quandary

Masarah Paquet-Clouston, Researcher, GoSecure, Inc.

In the past few years, the idea that a “DarkNet” or a “DarkWeb” exists has gained popularity. Although never officially defined, there seems to be a consensus that the “DarkNet” refers to the unindexed and anonymous internet, which has mostly been enabled by the prominence of The Onion Router (Tor) protocol. Due to the anonymity it brings, the network continuously raises controversial debates over its purpose today.

This discussion brought together security professionals from different organizations to share stories about what they have experienced on the “DarkNet” and discuss the societal implications of anonymous technologies. Most participants were from the information security industry and wished to learn more on the matter. Interesting stories were shared, and a lively discussion took place.

## The Debate

Inevitably, some individuals strongly argue in favor of online anonymity while others are adamantly against any kind of anonymous technologies. While discussing the “DarkNet”, three main arguments often come up in favor of anonymous networks, which are that it:

- Makes political dissension safer
- Skirts governmental censorship
- Enables discussions on sensitive topics

These arguments are based on what Tor can hypothetically provide through strong anonymity. Very few studies have been published to empirically evaluate its practical benefits. Findings on the matter could greatly help policy makers better understand the positive aspects of strong online anonymity.

Conversely, the “DarkNet”’s negative elements are often linked to the lack of accountability that comes with strong anonymity. The opposition’s main arguments center around the idea that the “DarkNet”:

- Enables online illegal markets
- Fosters anti-normative or illegal behaviors
- Leads to defamation and the promotion of untrue stories

The extent to which the “DarkNet” enables illicit activities and behaviors, however, or if these same acts would occur otherwise simply through another medium, is still unclear. Further studies on the matter could certainly help clarify the negative effects of the network.

## Assessing the Risks

During the discussion, an interesting societal implication was raised relating to how most of the population (and even many specialists in the information security field) don’t understand the technologies behind this anonymous network and what it can truly do. This misunderstanding, coupled with various sensationalist media stories and advertising campaigns, foster a mythic idea of the “DarkNet”. Participants noted that this general misconception prevents them from accurately assessing

the risks their company faces, especially in terms of the sharing and selling of sensitive information about them.

They had very legitimate questions, such as:

- “Should I buy a service to hunt for information on the “DarkNet” about my company? Or would that be just a waste of money?”
- “What kind of companies find their data available on the “DarkNet”? Are they only the Top500?”

Without much data available on the matter, information security specialists can hardly evaluate whether the idea of an active “DarkNet” is overinflated due to sensationalism, or if the threat is real. Yet, they still have to answer to upper-management concerns on the matter, putting them in a difficult position.

Overall, the discussion illustrated that there are serious needs for:

- Additional studies on the practical harms and benefits of anonymous technologies
- Further explanations to the public and to information security specialists on how the technologies behind the “DarkNet” work and what they can truly do
- Tempering the sensationalist coverage of the “DarkNet”
- Providing a comprehensive assessment on the kind of information available on this anonymous network, which would help security specialists assess the risks their company faces.