Government agencies with particularly vast resources, such as the NSA, may be able to circumvent the protection provided by Tor through what is known as the “Global Network Adversary” attack. If the Global Network Adversary (GNA) controls the relay through which you enter the Tor network and the relay through which you exit, the GNA can correlate the size and timing of your traffic to identify you on the Tor network. In this scenario, the GNA will have the origin and destination of your traffic, but if you are using HTTPS, they will not be able to read the content. You can help combat the GNA by running a Tor relay, adding to the strength and diversity of the Tor network.

Różnice tor vs Freenet

Freenet is a self-contained network, while Tor allows accessing the web anonymously, as well as using "hidden services" (anonymous web servers). Freenet is not a proxy: You cannot connect to services like Google or Facebook using Freenet. However, Freenet has websites, filesharing, forums, chat, microblogging, email etc, all anonymous and hosted within Freenet.

Freenet is a distributed datastore, so once content is uploaded to Freenet, it will remain on Freenet forever, as long as it remains popular, without fear of censorship or denial of service attacks, and without needing to run your own web server and keep it online constantly.

The other big difference is that Freenet has the "darknet" or Friend to Friend mode, where your Freenet node (software on your computer) only connects to the Freenet nodes run by your friends, i.e. people you know (and maybe to their friends, to speed things up). This makes blocking Freenet, e.g. on a national firewall, extremely difficult.

However, most people currently use Freenet in "opennet" mode (that is, connecting automatically to whoever the network assigns, rather than connecting only to their friends). This is much less secure than using Freenet in "darknet" mode, and is relatively easy to block, as it does have some central servers ("seed nodes").