# 3. Existing metrics

Security metrics are very important. Nowadays, the economic climate does not allow spilling resources for information security: they are limited. The security spending must be justified and allocated. Therefore, the right metrics are necessary. If one invests a lot in information security, he wants to get actual security, and reap certain benefits (bron: online lecture 2.2).

But what ‘information security’ is a wide concept. In this project, the main focus is Spam, regarding the project SpamHaus.

If one takes a look at current literature, more and more articles are written about metrics and information security: an upcoming field. Already in 2008, Zhuang was talking about metrics in the world of spam. His metrics mainly focused on botnets, and listed three metrics (Zhuang, 2008):

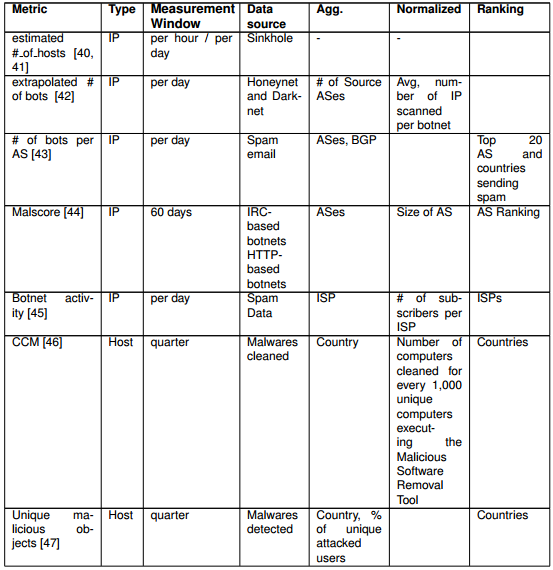
1. **Capability of botnet controllers**: estimate the total size of each botnet based on their 9 days of observation in the experiment
2. **Level of activity (botnet**): estimate the active working set of each botnet in a short time window, such as one hour. Think of the spam sent (such as the number of spam emails) per botnet
3. **Active size (botnet)**: the number of machines/IPs used for sending spam email messages by this botnet during this short time window

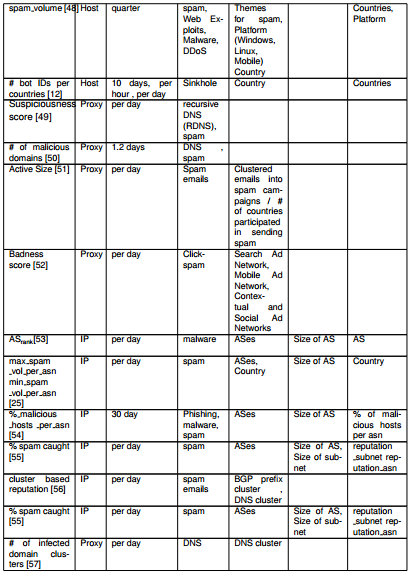
If one looks a bit further in literature, you might find a surprising amount of information. But there is one very useful paper, summarizing all this information and insights about spam metrics. Moura and Van Eeten (2015) listed a summary of current botnet metrics. First, they pointed out what the requirements of useful metrics are, such as ‘comparative over time’ and ‘comparability’.

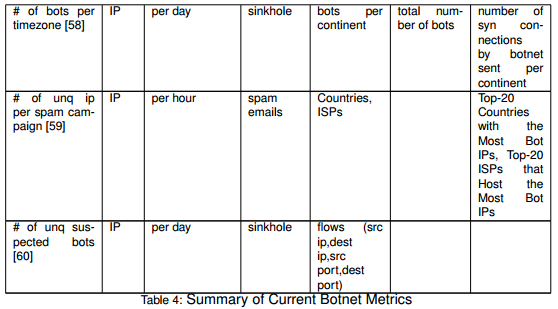
Secondly, they carried a literature review on the current metrics, and proposed a classification of these metrics into three categories:

1. **IP-based**: metrics using the originating IP address of traffic related to infected machines
2. **Host-based**: metrics based on data that directly and reliably indentifies individual hosts on the internet.
3. **Proxy-based**: metrics that are estimations based on traffic volume associated with botnets (Moura&van Eeten, 2015)

These categories are shown in the second column of the table. The other columns quite speak for themselves, the last three might need some more explanations. The categories presented above can be further extended: by aggregation (per country for example), by normalization, or by ranking: being turned in a rating, based on a different scale than the original metric.

Table 1: summary of current botnet metrics (Moura & van Eeten, 2015)





## Reflection of current metrics

To reflect on the current metrics might be the most important part of reviewing spam metrics. What are the issues with those current metrics, or do they work perfectly fine? The shortcomings of the spam metrics will be discussed in the same categories as used before.

IP-based metrics violate several requirements (such as reliability) due to DHCP and NAT effects. For example, it is possible three bots are operating, from three different laptops, behind a single public router IP address. This shows it is very complex to count botnet presence in ISP network: the IP addresses do not correspond to the number of operating bots.

Host-based metrics are known as more reliable than IP metrics and proxy metrics. The data used for these metrics is very precise, but this is exactly the problem. The data requires access to the hosts themselves, but the access to this data is either restricted or presented to the public in aggregated levels. These metrics are very reliable, but it is hard to obtain the necessary data.

Proxy based metrics are not very precise. This occurs because they mainly express estimates on the number of infected machine, they do not express actual data. It would not be a big problem, if the estimation could me made precisely. Unfortunately, there are many factors influencing the measurements, which make the estimation unreliable. Proxy based metrics are not completely useless, but should be used with caution, and only for purposes that fit with their shortcomings. (Moura & Van Eeten, 2015).