**Part 2: DDoS Discovery: Industry and Academic perspective**

The monitoring technologies mentioned in the papers are: Network telescopes, Flow monitoring, Honey pots and hybrid approaches combining them together.

Differences in monitoring DDoS attacks across technologies arise from:

* **Vantage Point**: The position of a technology within the network influences what portions of traffic it can observe.
* **Detection**: Distinguishing legitimate traffic peaks from attack traffic is challenging, as each technology highlights unique traffic or attack attributes using varied feature sets.
* **Scope**: A technology monitoring range defines its capabilities. Monitoring range shapes capabilities. Telescopes target spoofed direct-path attacks, missing reflection attacks, while flow monitoring at IXPs broadly captures attacks but is path-limited (as it captures only specific ones)
* **Data Access**: Data sharing impacts attack visibility. For example the authors of the paper mentioned Flow monitoring by Netscout integrates ISP data for broader insights, but proprietary limits restrict sharing, unlike shareable but narrower telescope data