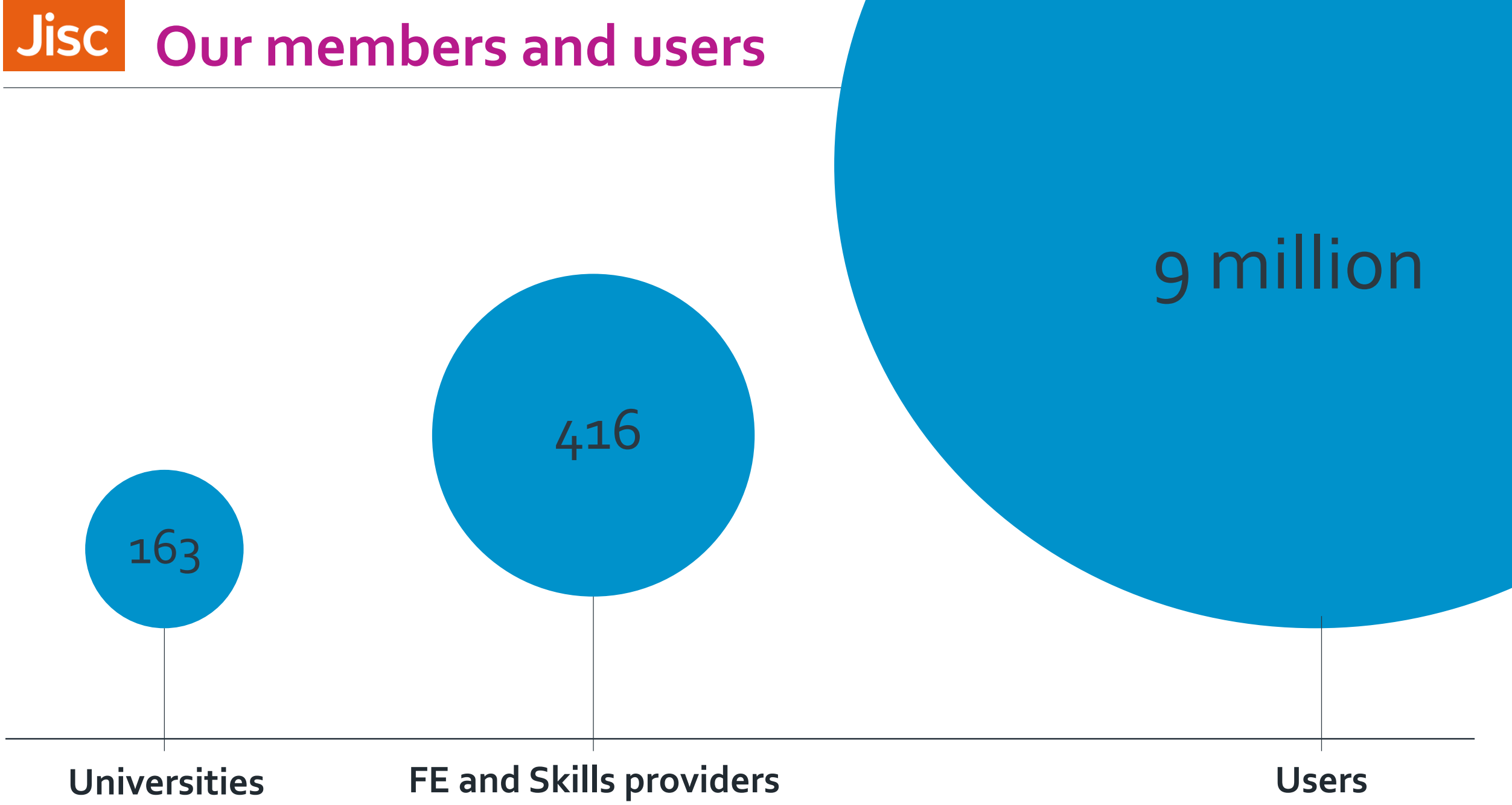
Cyber Security Landscape

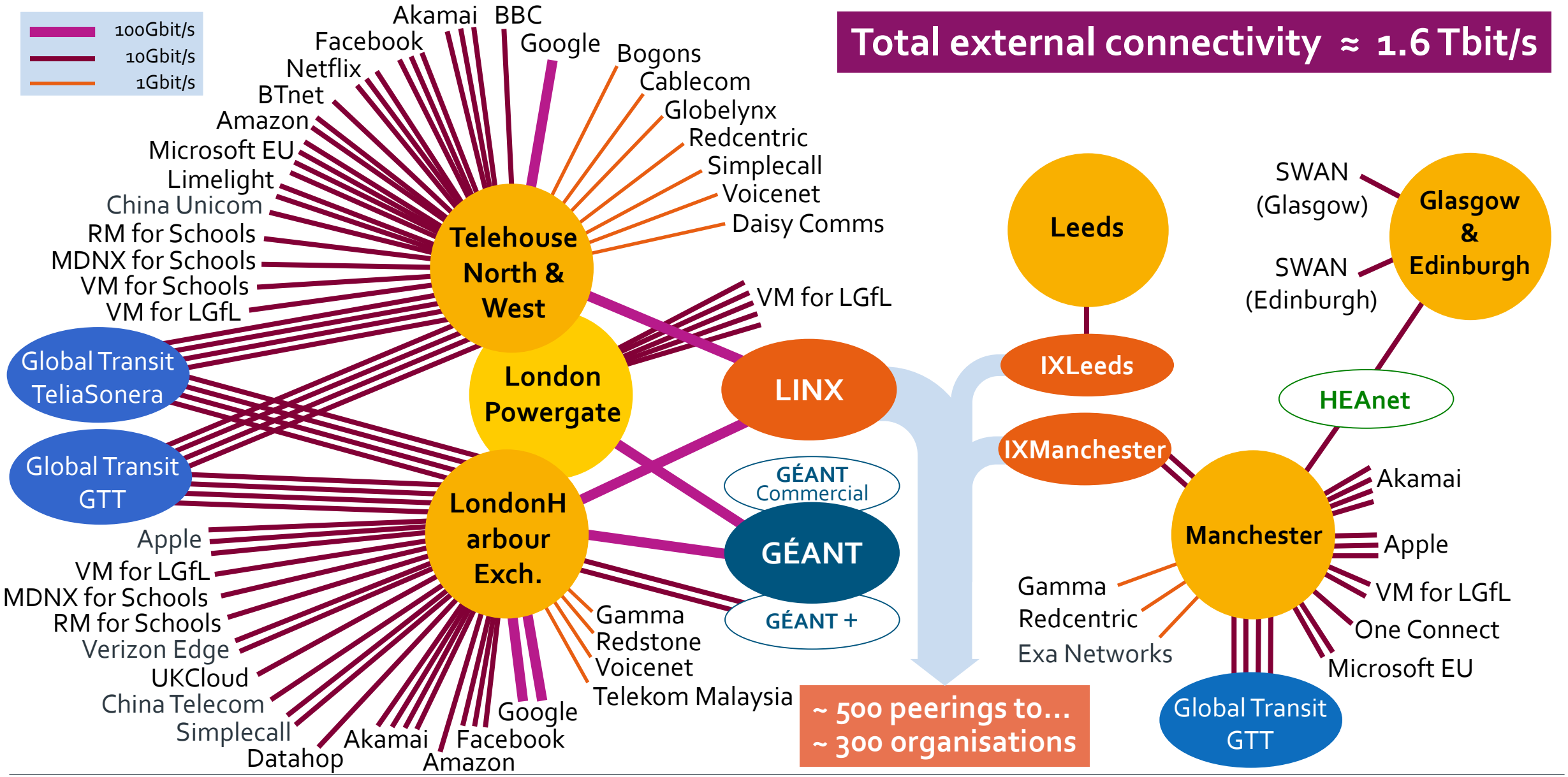
8th May 2018

Henry Hughes Deputy Director of Security

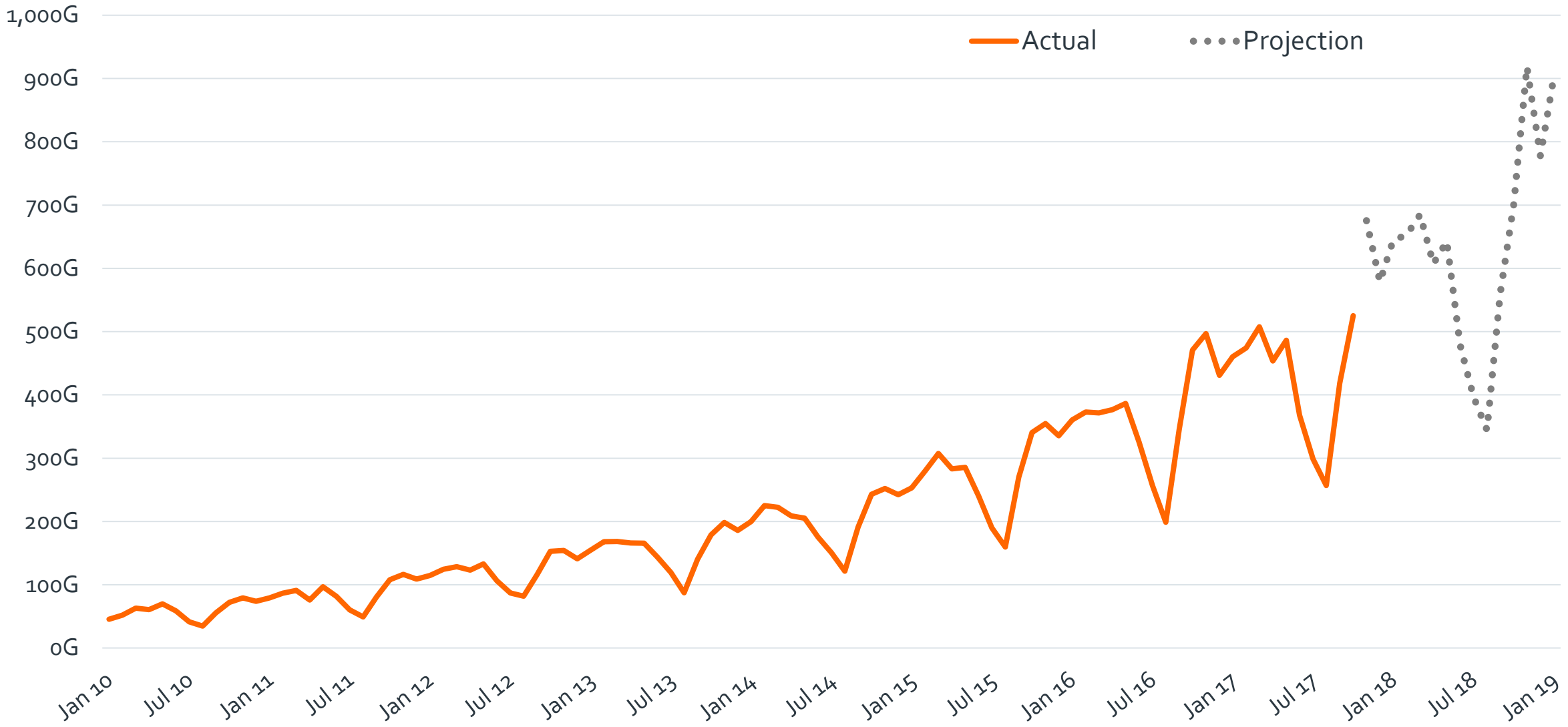
Our members and users



Janet external connectivity



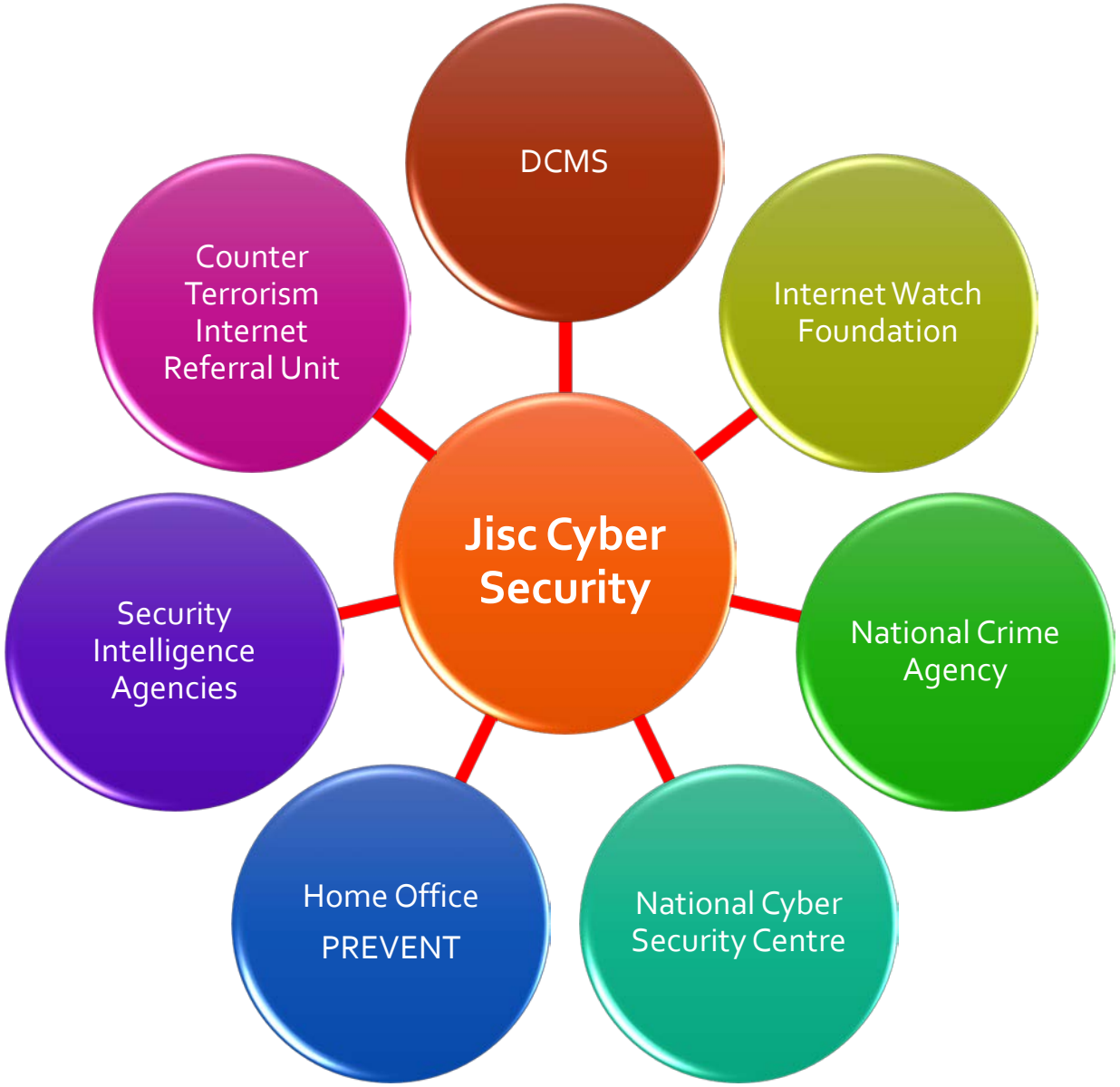
Janet traffic volume



National cyber security strategy

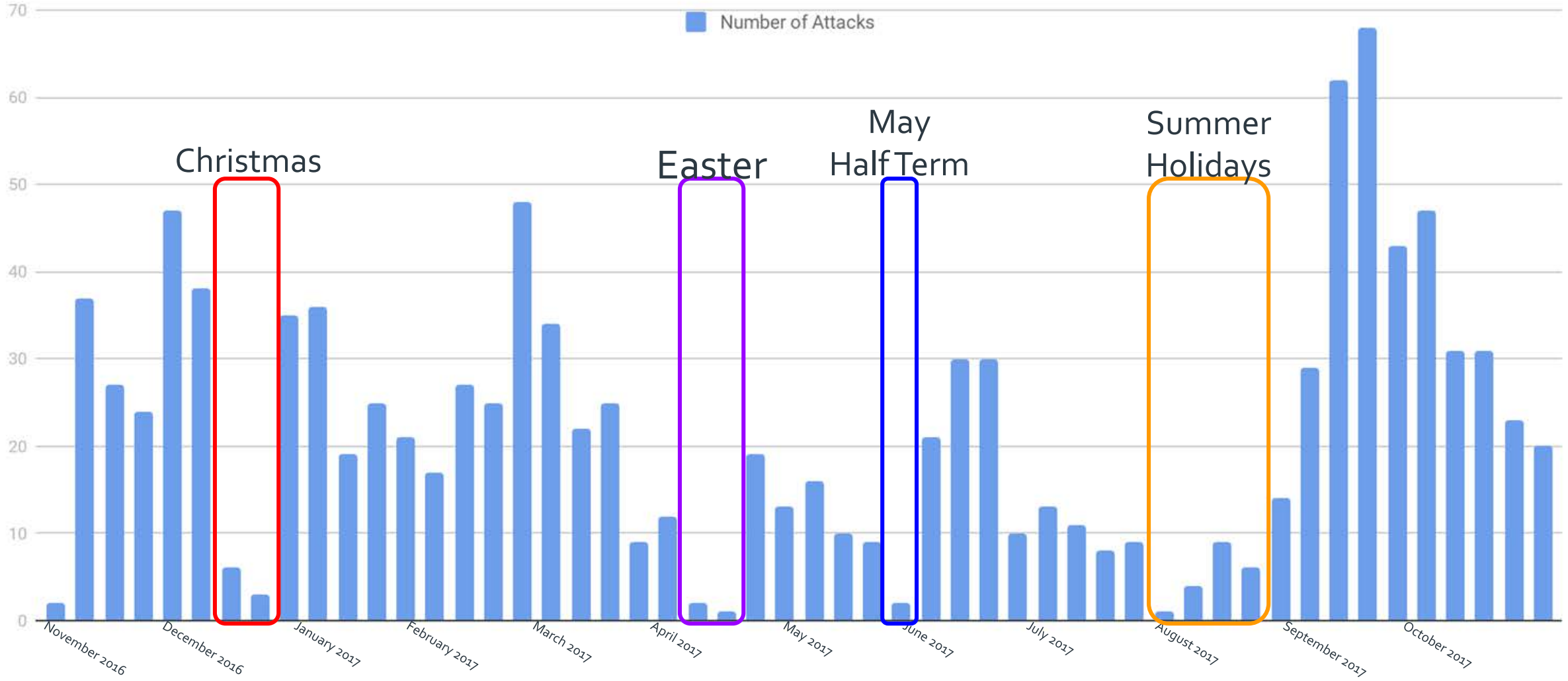
https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

Cyber security landscape

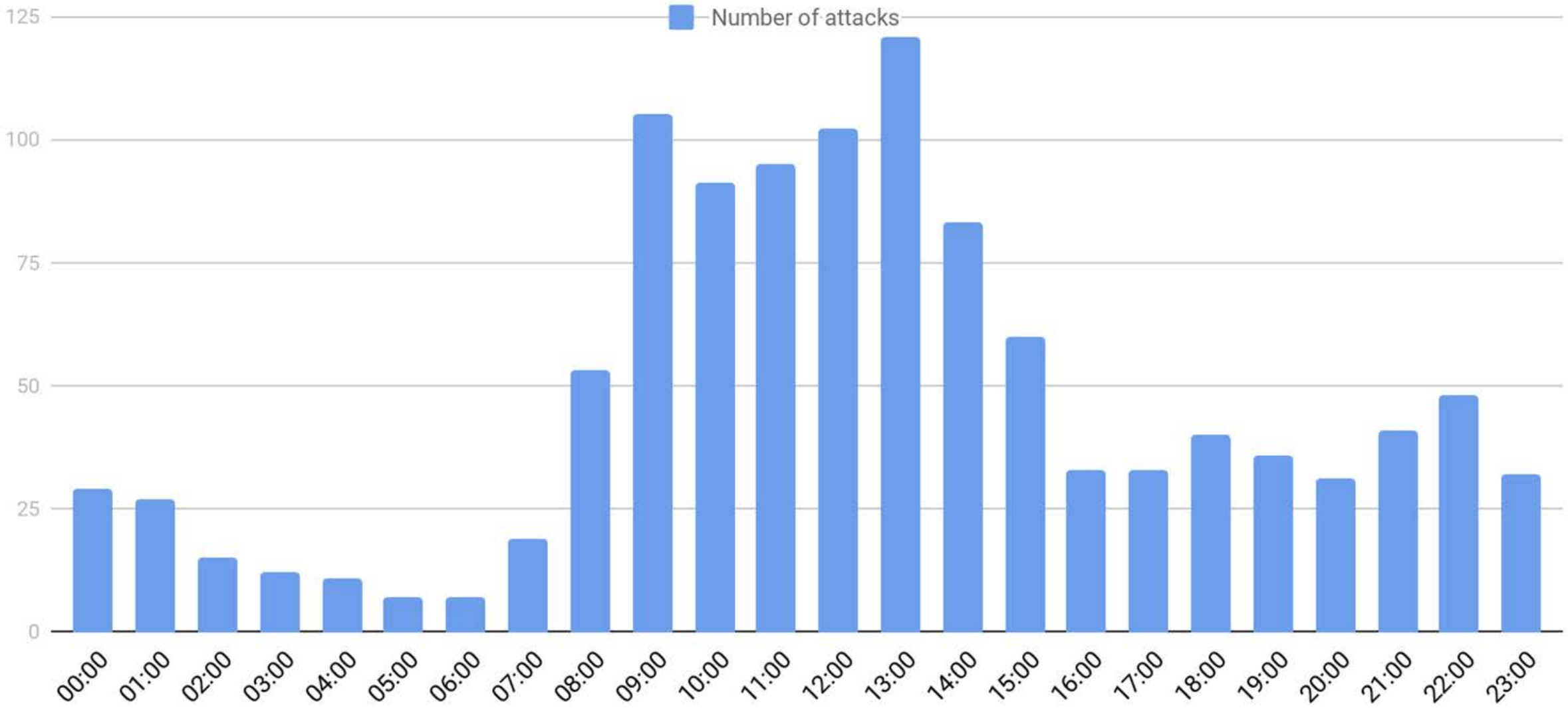


Who is attacking

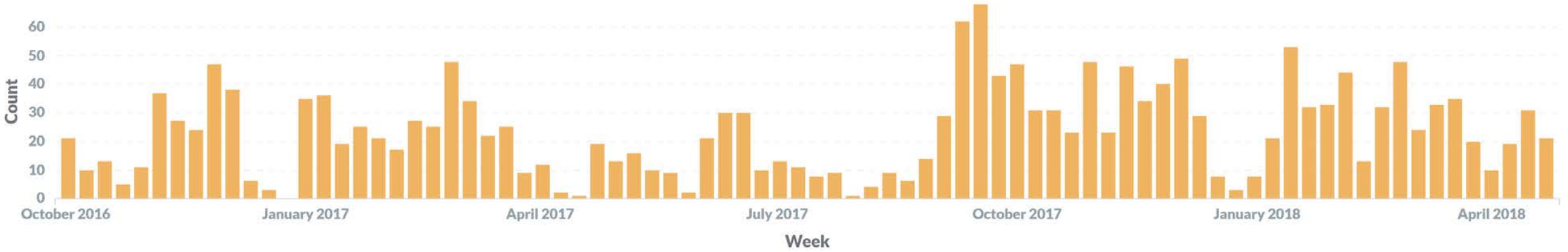
DDoS attack trends



Distribution of attacks over the day



Attacks per week



485 TB
Total attack traffic

55.2 Gbps
Largest attack detected

1,926
Total Inbound Attacks

313
Individual members targeted

55 Hours
Longest attack detected

22.249 Minutes
Average attack duration

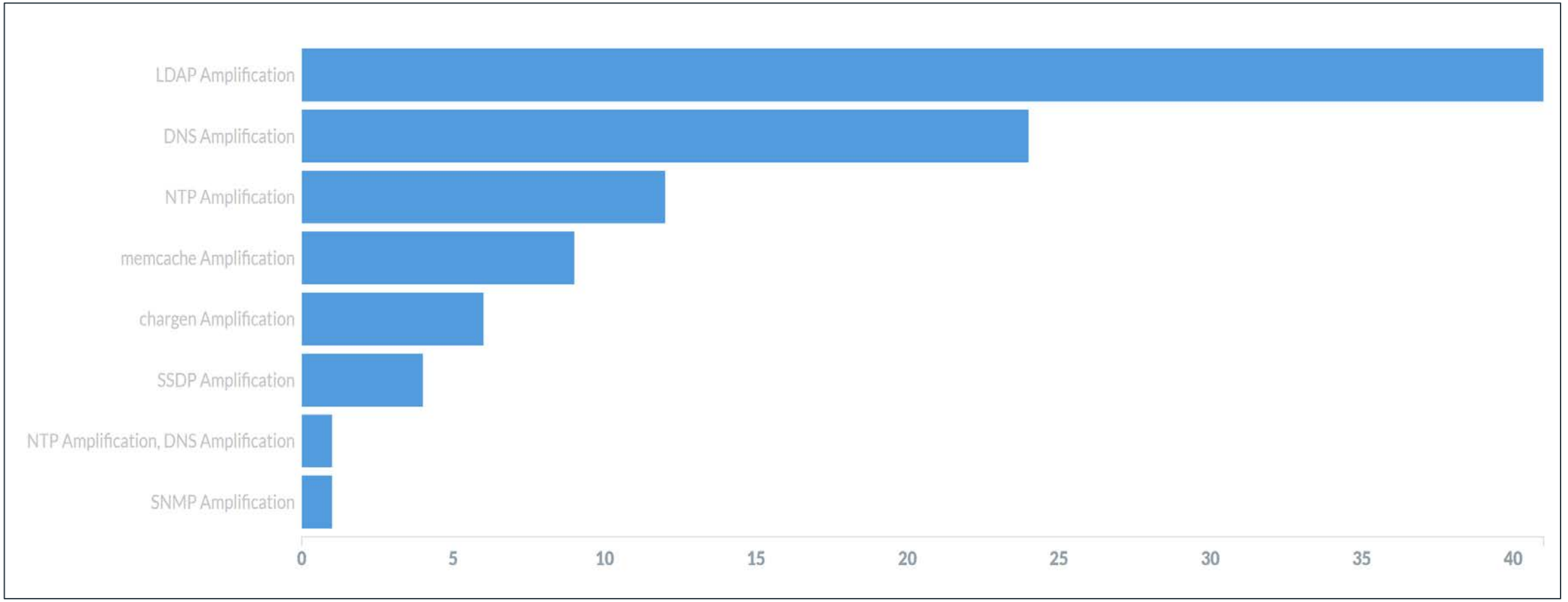
Top attack methods

Do S Method	Count
DNS Amplification	682
UDP	270
NTP Amplification	261
IP Fragmentation	146
LDAP Amplification	127
TCP SYN	91
chargen Amplification	83
SSDP Amplification	39
DNS	29
memcache Amplification	17

UDP Amplification attacks

- Server with a insecure UDP service (LDAP, NTP, Memcache) used to reflect and amplify traffic towards the intended target
- 8 week period in March/April 2018
- 98 out of 191 attacks were UDP Amplification attacks

UDP Amplification methods



German component attack traffic

- 34 of the 98 attacks involved greater than 1% of traffic from German IP addresses
- An average of 4.7% attack traffic was from German IP addresses
- Equates to an average of 218 German IP addresses/servers
- Largest attack of those 34 was 14.85Gbps
- Longest attack of those 34 lasted 4 hours

International comparisons