DDoS Attack Trends Through 2009-2011

Jose Nazario, Ph.D.
jose@arbor.net

Data Sources

- **Actual attack traffic**
  - Arbor Peakflow systems reporting
  - Self-selected group, global

- **'Bladerunner' botnet tracking project**
  - Botnet command, intended victims

- **Worldwide Infrastructure Security Report**
  - Survey data, dozens of participants, global

ARBOR® NETWORKS

Key Findings in the 2011 Survey

- **Any Internet Operator Can Be a Target for DDoS**
  - *Ideologically-motivated 'Hacktivism' and On-line vandalism DDoS attacks are the most commonly identified attack motivations*

- **Size and Scope of Attacks Continue to Grow at an Alarming Pace**
  - *High-bandwidth DDoS attacks are the 'new normal' as over 40% of respondents report attacks greater than 1 Gbps and 13% report attacks greater than 10Gbps*
  - *Increased sophistication and complexity of layer-7 DDoS attacks, multi-vector DDoS attacks becoming more common*

- **First-Ever Reports of IPv6 DDoS Attacks 'in the Wild' on Production Networks**

ARBOR® NETWORKS

Key Findings in the 2011 Survey

- **Attackers Are Going Where the Money Is**
  - *Rarity of IPv6-enabled attacks indicative of low IPv6 market penetration and lack of critical mass*

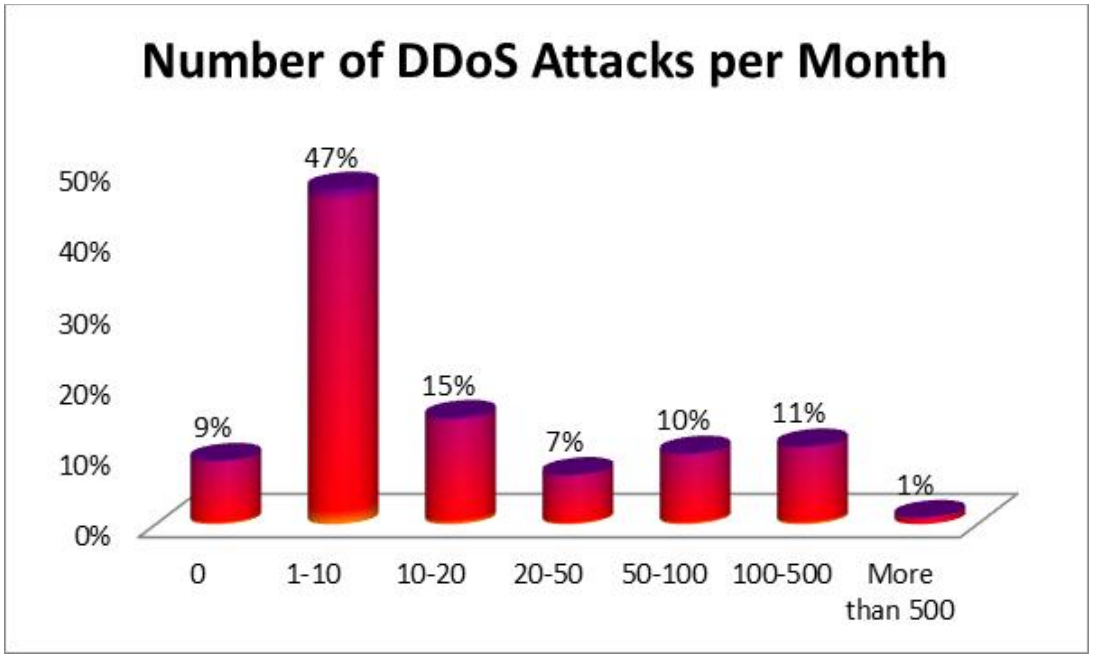
- **Continued Uncertainty Around Visibility & Security of Mobile/Fixed Wireless Networks**

- **Mobile Handsets and Devices Directly Impacted by DDoS Attacks**

- **Trust Issues Abound Across International Boundaries**

ARBOR® NETWORKS

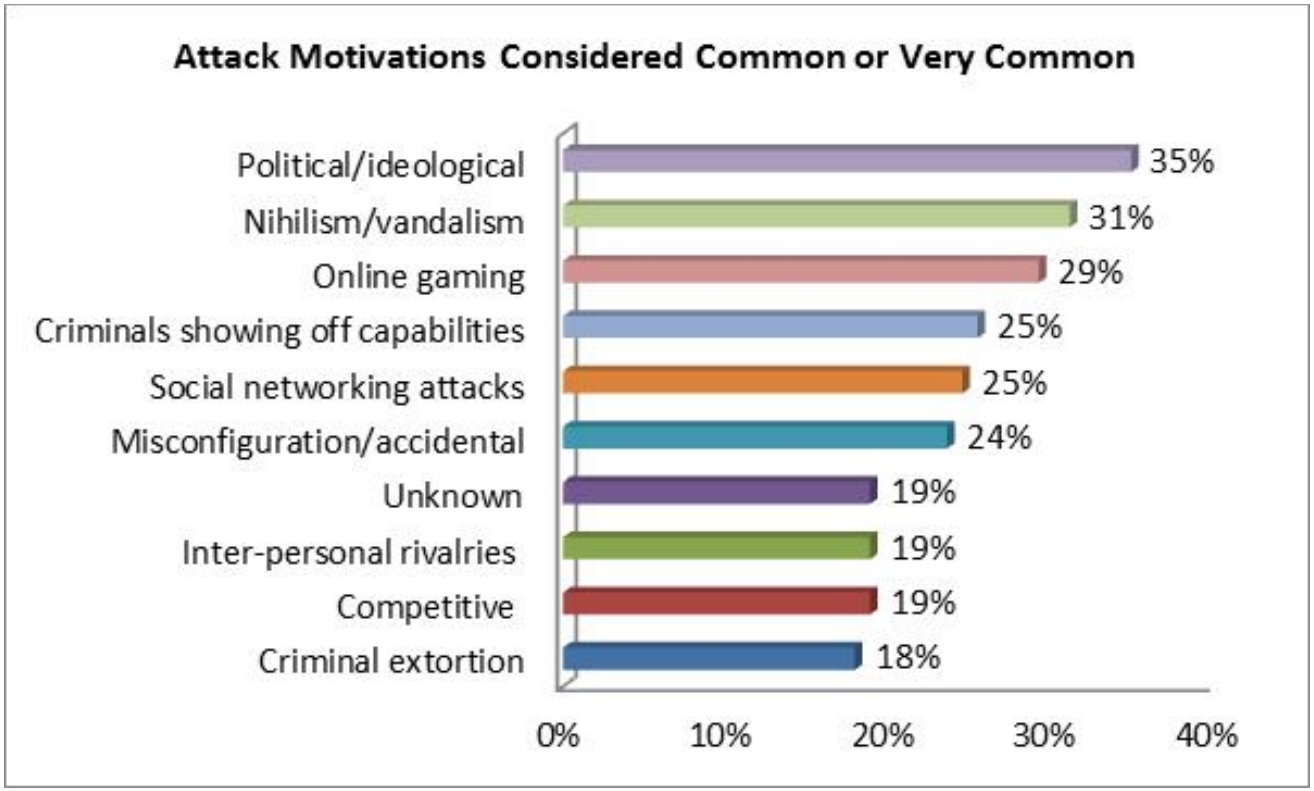
DDoS Attack Frequency over last 12 Months



- 91% of respondents see at least 1 DDoS attack per month up from 76% in 2010
- 44% of respondents see 10 or more attacks per month up from 35% in 2010

ARBOR® NETWORKS

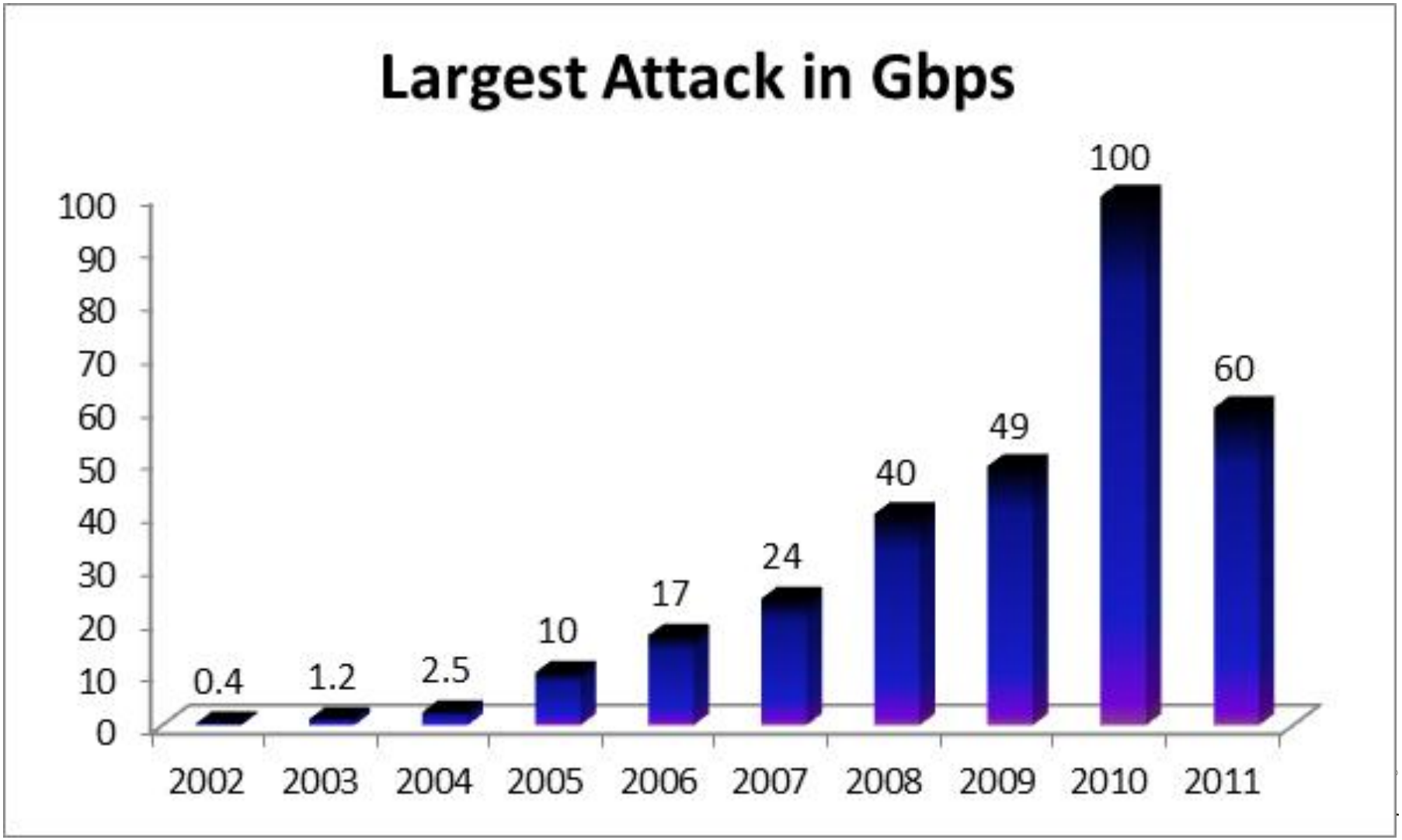
Top DDoS Motivations



- Top two attack motivation categories are fueled by personal beliefs and inclinations of attackers

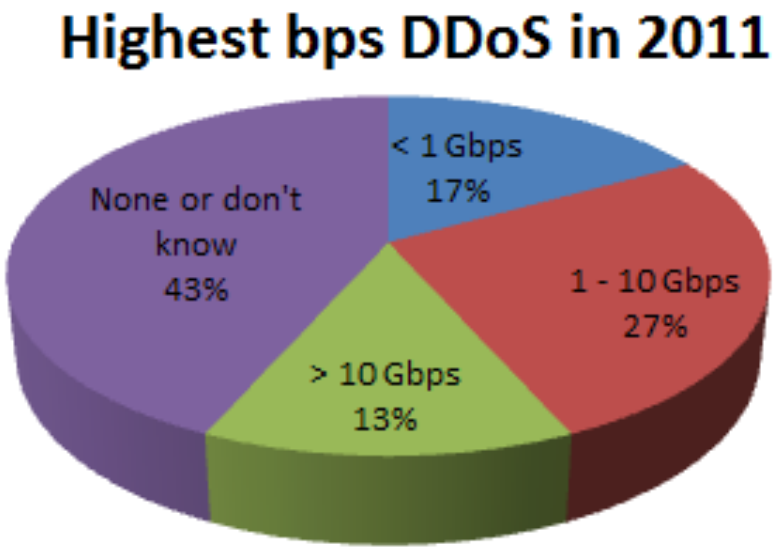
ARBOR NETWORKS

Peak Attack Sizes Down in 2011



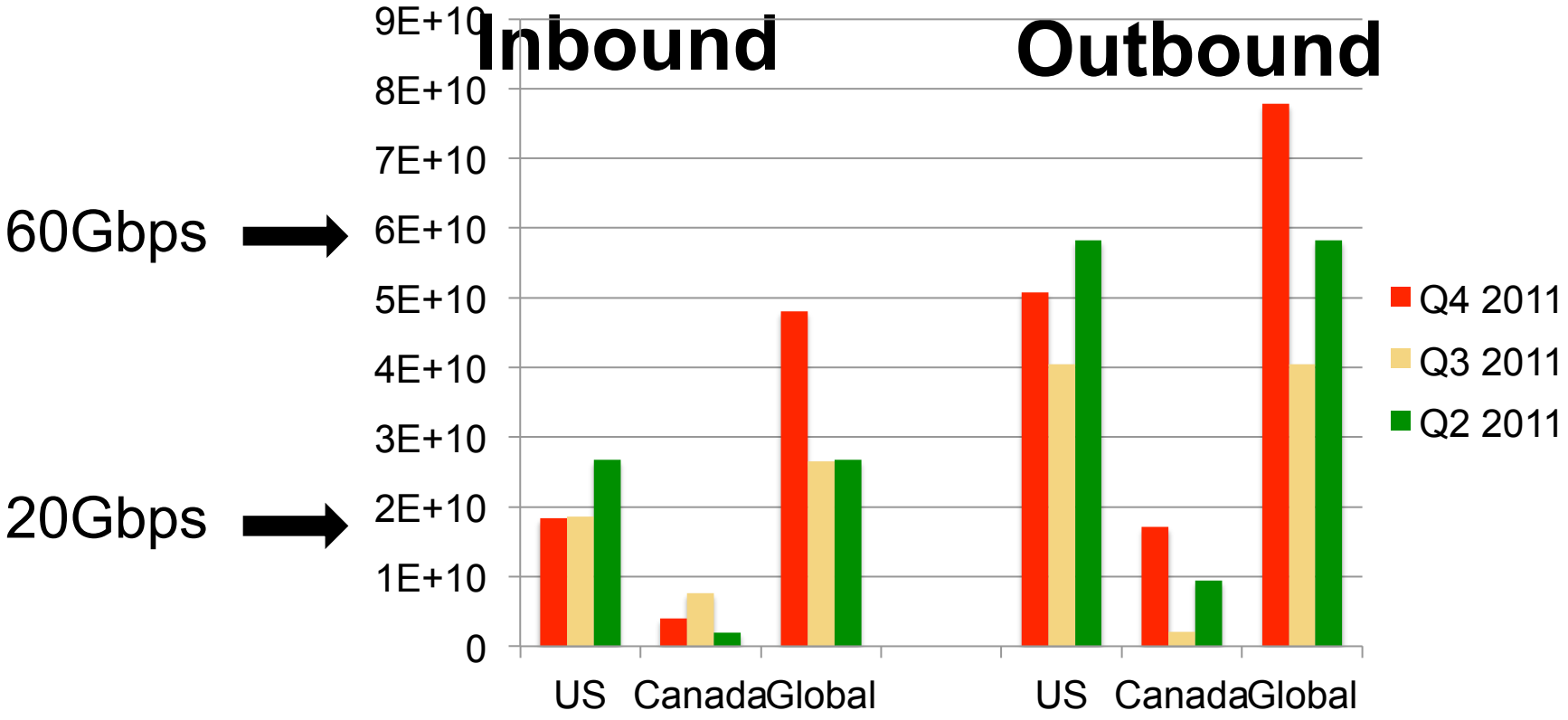
Large Attacks are Now Commonplace

- Aggregate attack sizes have leveled off but remain at levels capable of overwhelming most Internet operators
- 13% of respondents report attacks above 10 Gbps
- 40% of respondents report attacks above 1 Gbps
- Largest pps attack reported is 35 Mpps keeping pace with 2010



ARBOR NETWORKS

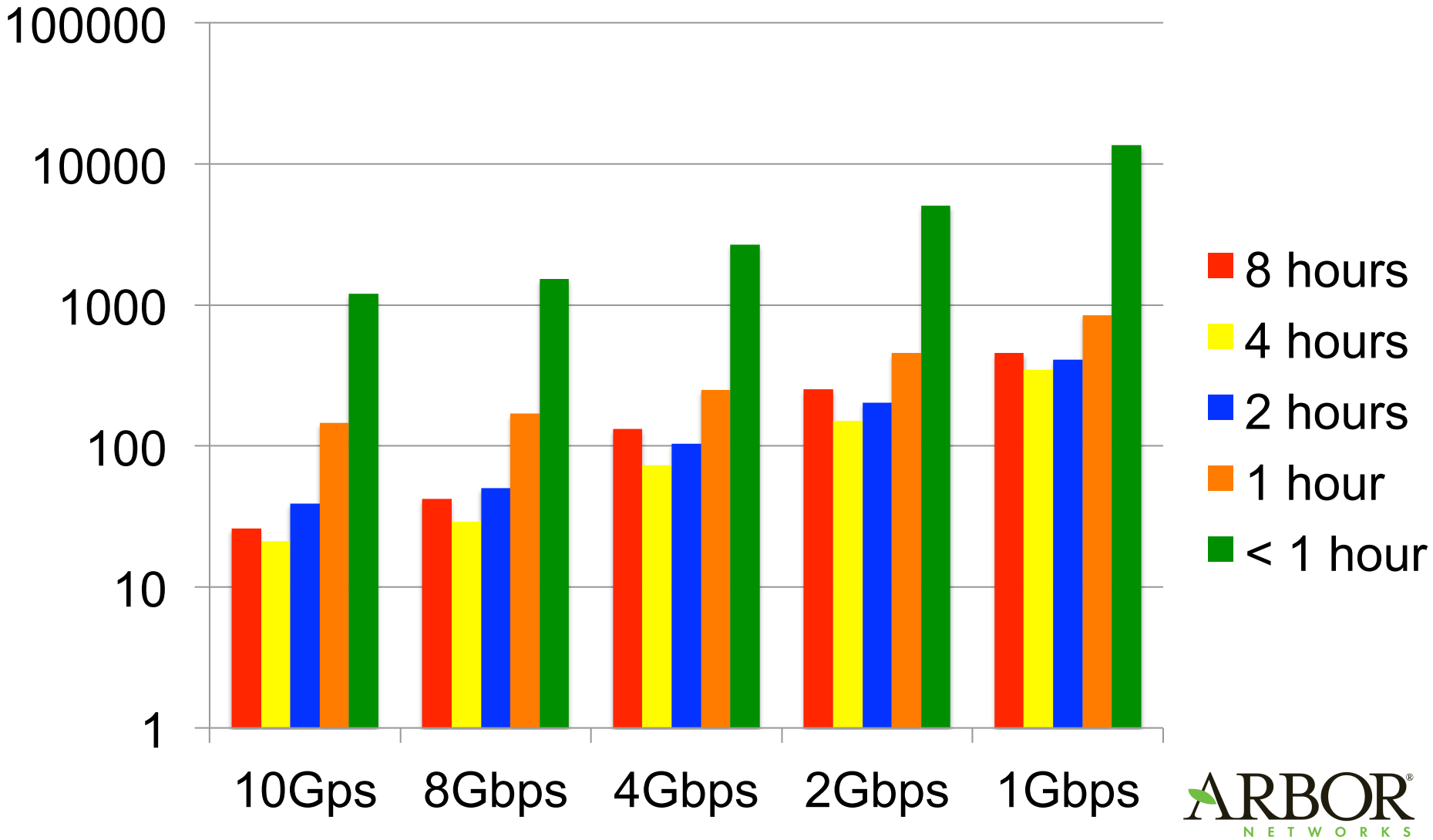
Measured Attacks in 2011 for US, Canada



- Data comes from Peakflow measurements

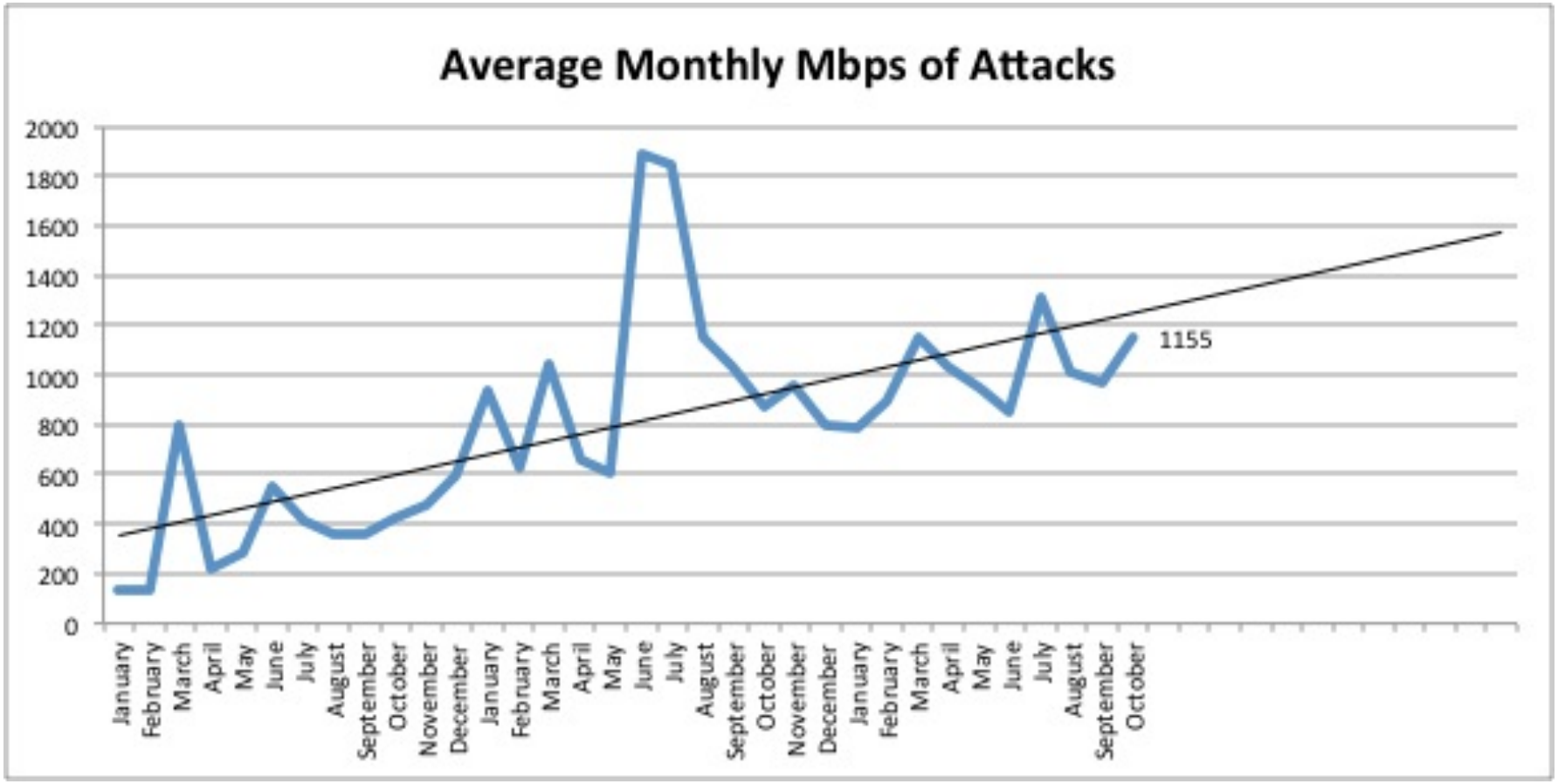
ARBOR NETWORKS

Attack Sizes and Durations (2011)



ARBOR NETWORKS

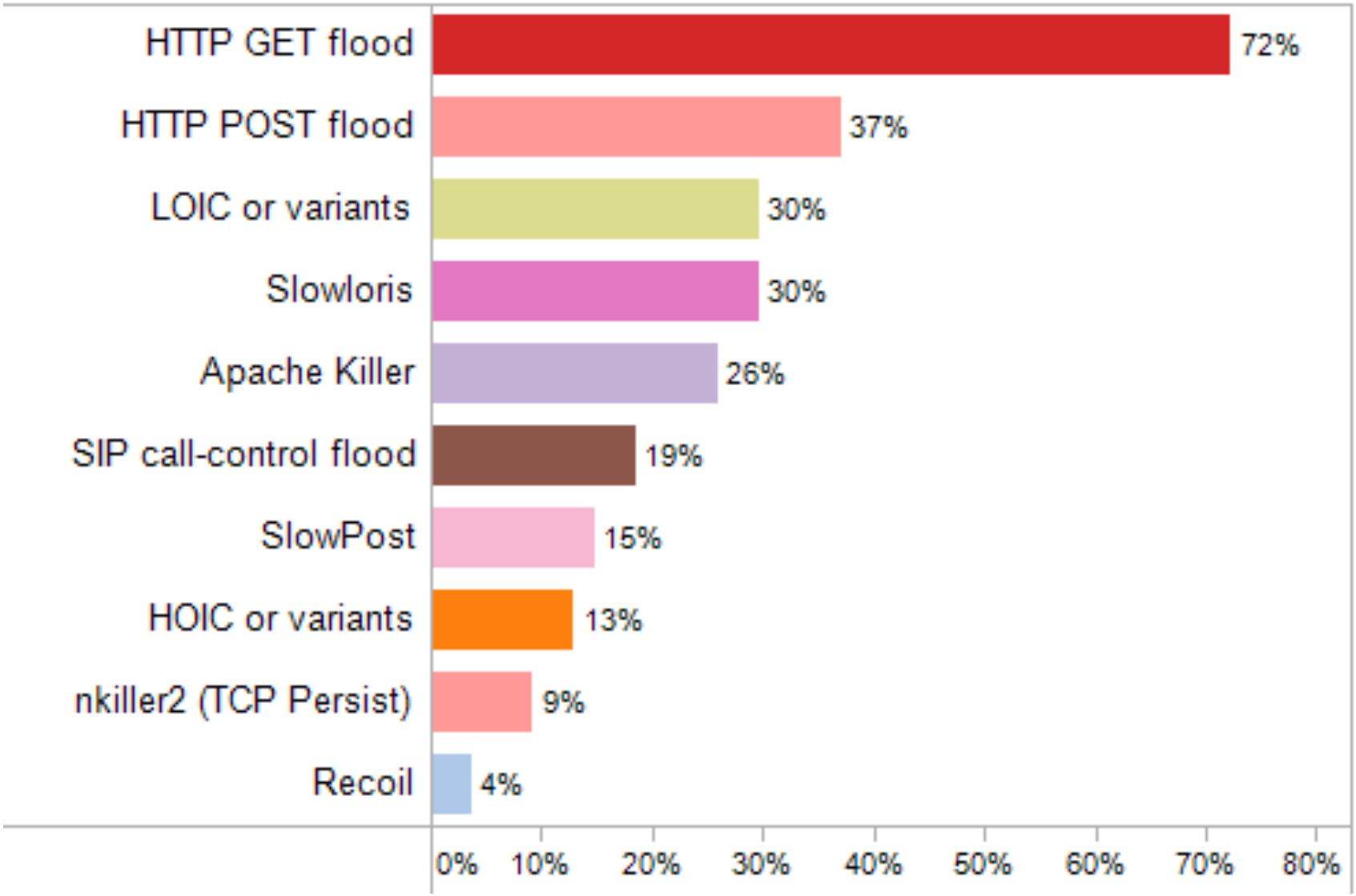
Average Attack Size Still Growing



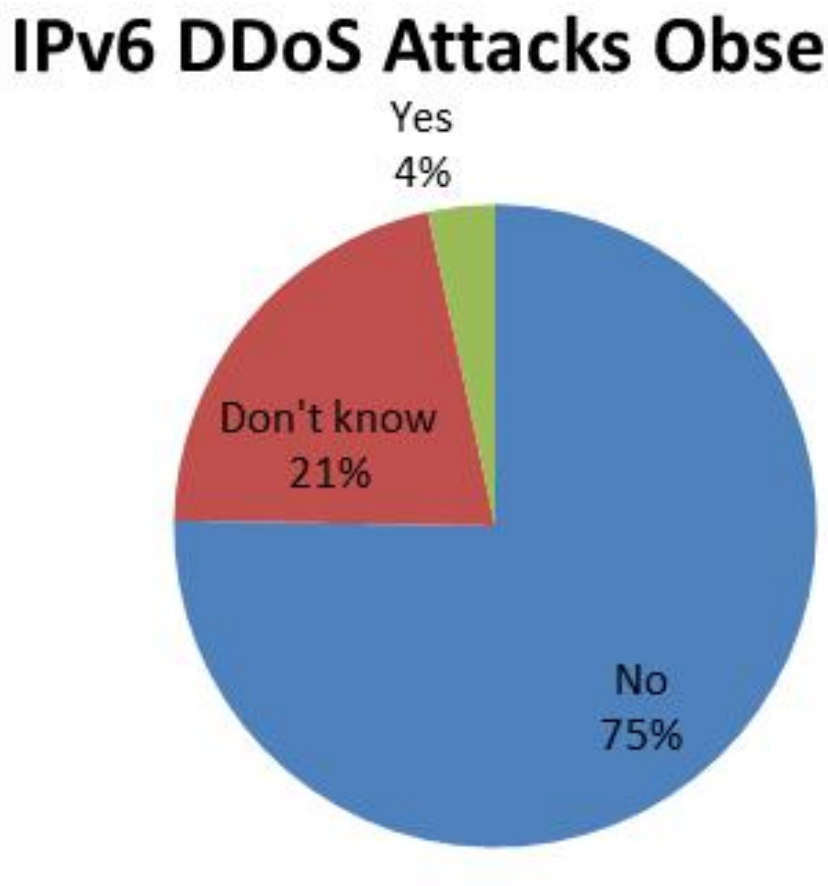
Data from ATLAS via anonymous statistics

ARBOR NETWORKS

Most Common Application Layer Attacks Seen



IPv6 DDoS Attacks

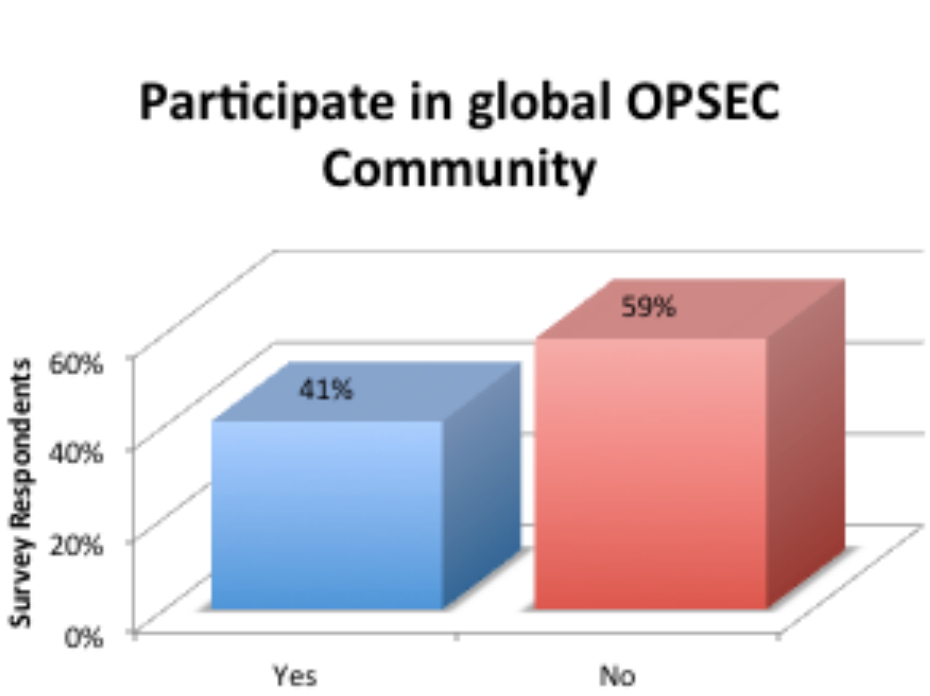


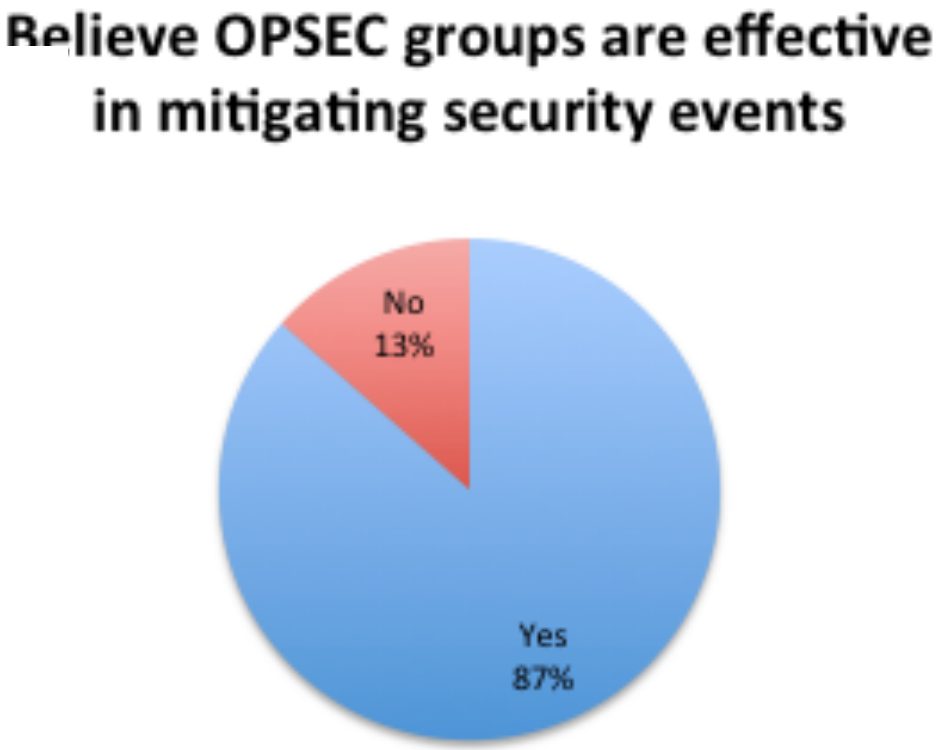
- First report of an IPv6 DDoS attack in the history of the WISR
- Low frequency of attacks reflect low adoption of IPv6 for critical services

ARBOR NETWORKS

Use of OPSEC Communities

- More than half of respondents do not actively participate in the Global OPSEC Community, yet 87% of them believe that the OPSEC Community is effective





Summary

- IPv6 makes an appearance
- Peak bandwidth used in DDoS we see is down from 100Gbps (2010)
- HTTP GET floods becoming widely popular
- Ideological motivations now most prevalent

ARBOR NETWORKS