

The Role of ISPs in Botnet Mitigation

An Empirical Analysis Based on Spam Data

Michel van Eeten*
Johannes M. Bauer**
Hadi Asghari*
Shirin Tabatabaie*
Dave Rand***

*** Faculty of Technology, Policy and Management , Delft University of Technology**
**** Quello Center for Telecommunication Management & Law, Michigan State University**
***** Trend Micro**

Contact: m.j.g.vaneeten@tudelft.nl

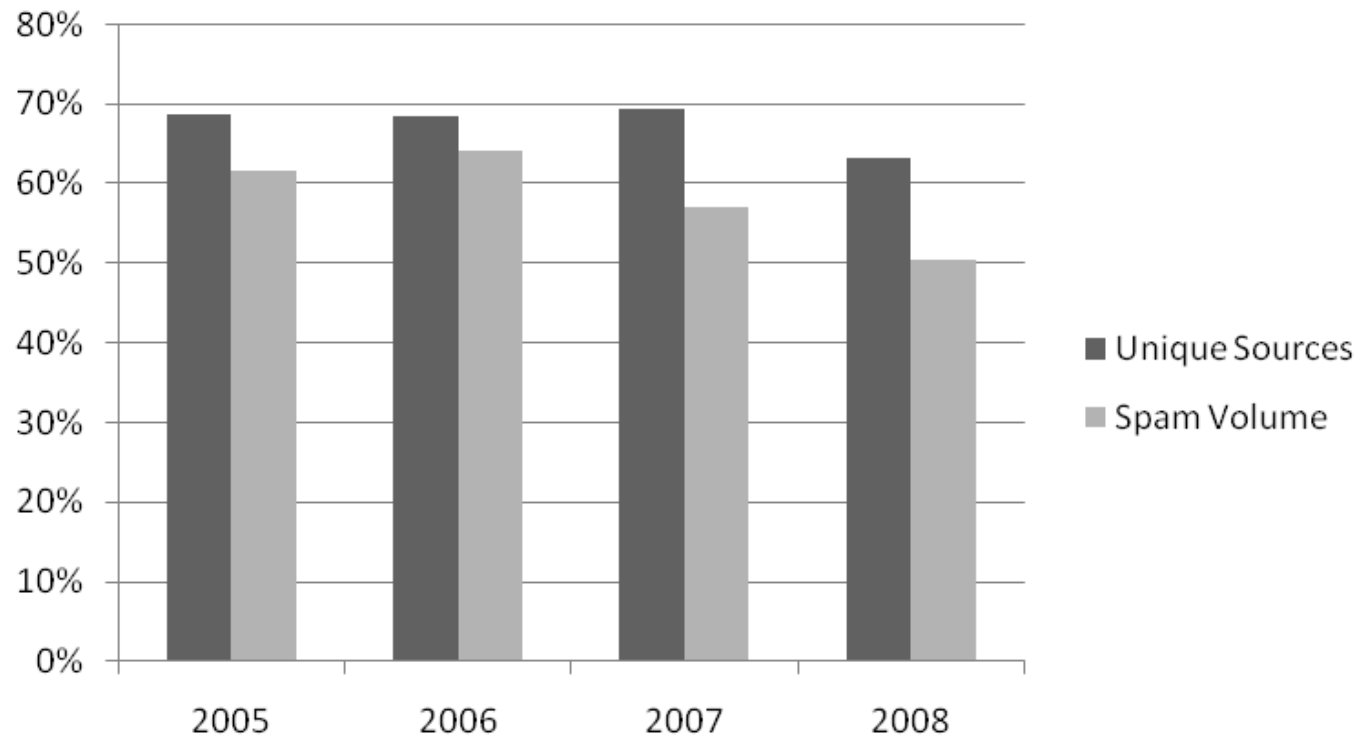
Focus on ISPs as intermediaries

- Two assumptions behind focus on ISPs as key intermediaries for botnet mitigation
 - the ISPs are a critical control point for infected machines
 - the ISPs that would carry the burden of (self-) regulation are also the ones who control the bulk of the problem
- Both of these assumptions can be tested empirically

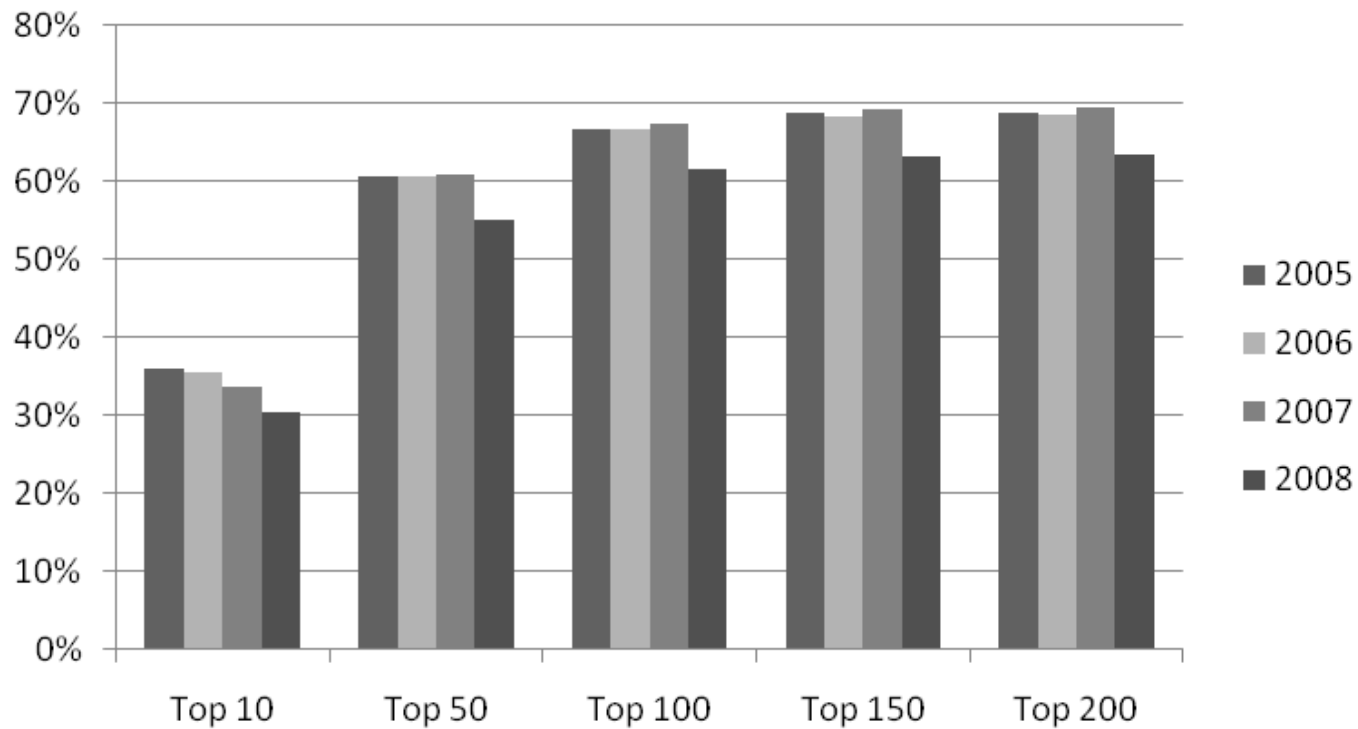
Approach

- Spam distribution as a proxy for infected machines
 - Spam trap: 138 mln unique sources, 63 bln spam messages
- For each spam-sending IP address, we looked up the originating AS and, using geo-IP, the country
 - We triangulated our findings by comparing them to public reports of commercial security providers
- For 40 countries (OECD+), we mapped the ASNs to ISPs or non-ISPs (e.g., hosting providers, university networks, webmail providers)
- Result: time series of unique sources and spam volume at level of ISPs and countries

Percentage of sources/volume of all 200 ISPs compared to global total



Percentage of sources located in top ISPs (compared to global total)

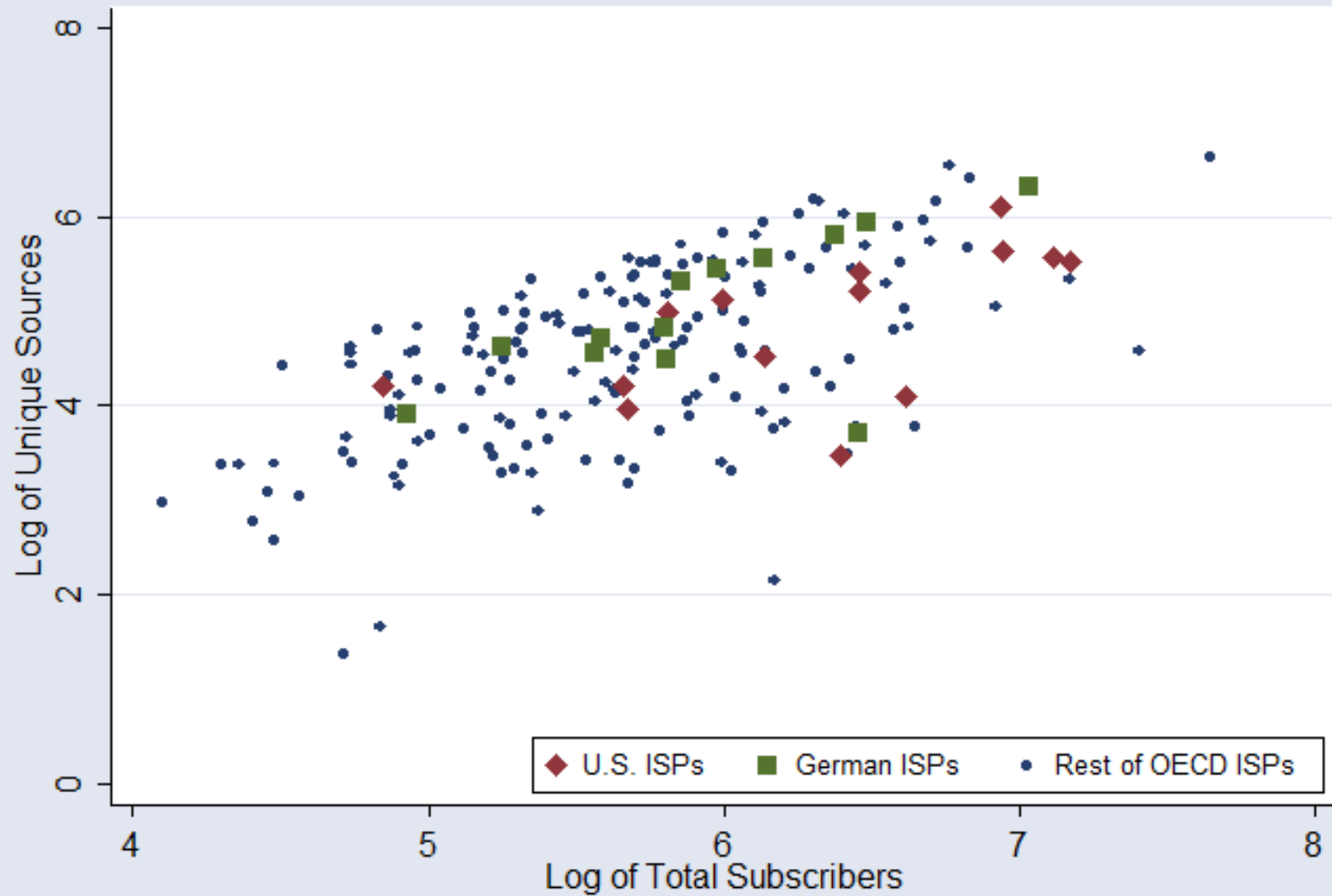


Findings (1) – ISPs are control points

- Data confirms both assumptions behind focusing on ISPs as key intermediaries
 - 63-69% of all global sources were located within networks of ISPs in 40 countries of OECD+
 - concentrated pattern: 50 ISPs control over 50% of all infected machines worldwide
 - Significant differences between countries: from 42% (Canada) to 96% (Turkey)
 - Remaining sources belong to non-ISPs or ISPs for which we do not have market data

Findings (2) – ISPs differ significantly

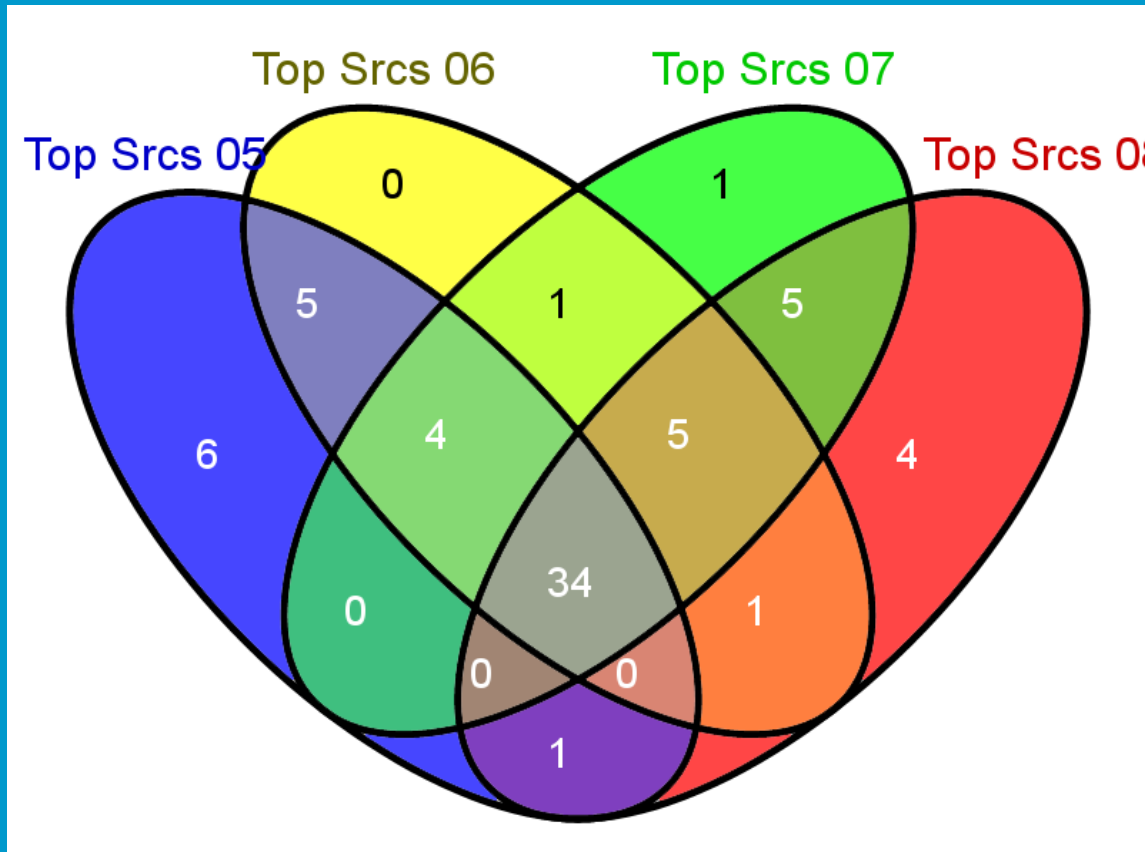
- Do market incentives force ISPs to similar levels of botnet mitigation?



Findings (2) – ISPs differ significantly

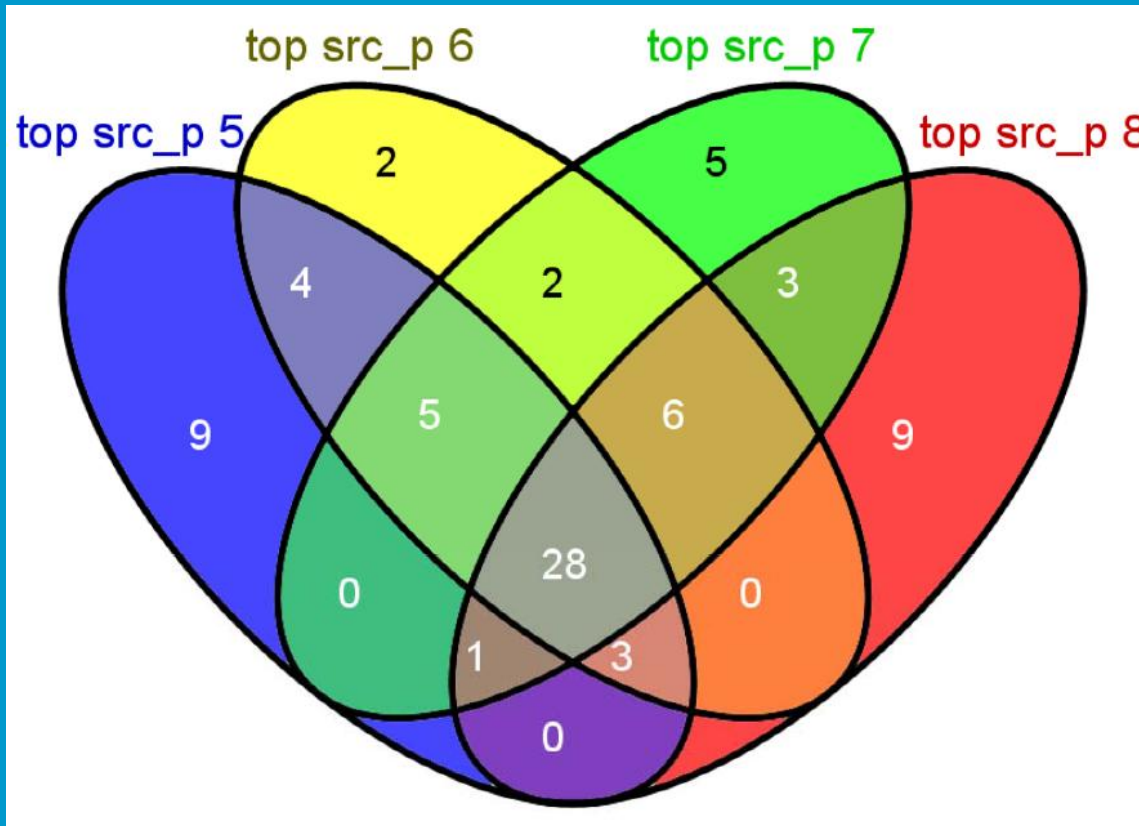
- Substantial differences exist in the security performance of ISPs, even when working under similar conditions
 - Variability among ISPs is larger than among countries – i.e., within each country there are good and not-so-good ISPs
 - Number of infected machines at ISPs of similar size in the same county can vary in some cases by as much as two orders of magnitude
 - Variability among ISPs suggests that ISP security practices may make a substantial difference
- The set of top-contributing ISPs is quite stable over time

Variability in number of sources



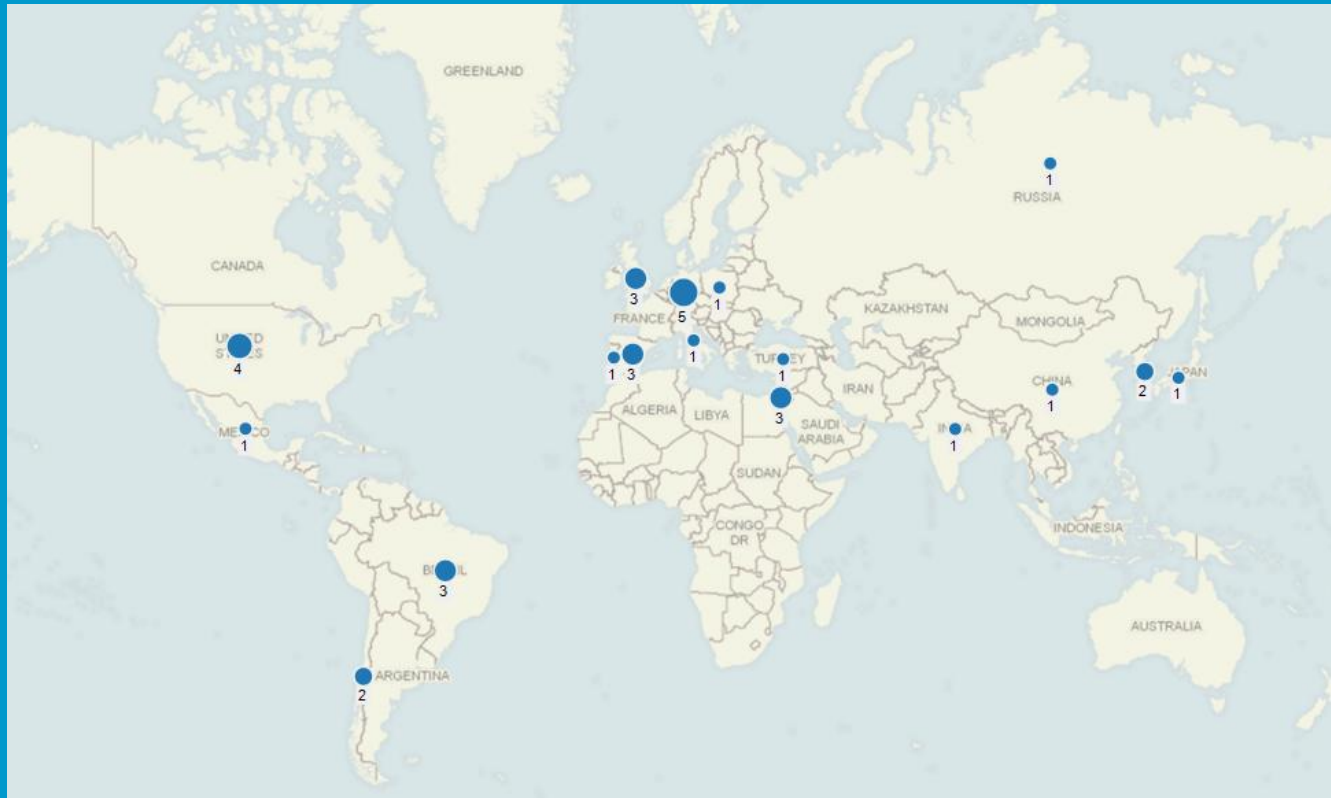
Variability in absolute performance, as measured by the overlap of the 50 ISPs with the highest number of infected machines in their network 2005-2008:
34 ISPs are in the top 50 in all four years

Variability in sources per subscriber



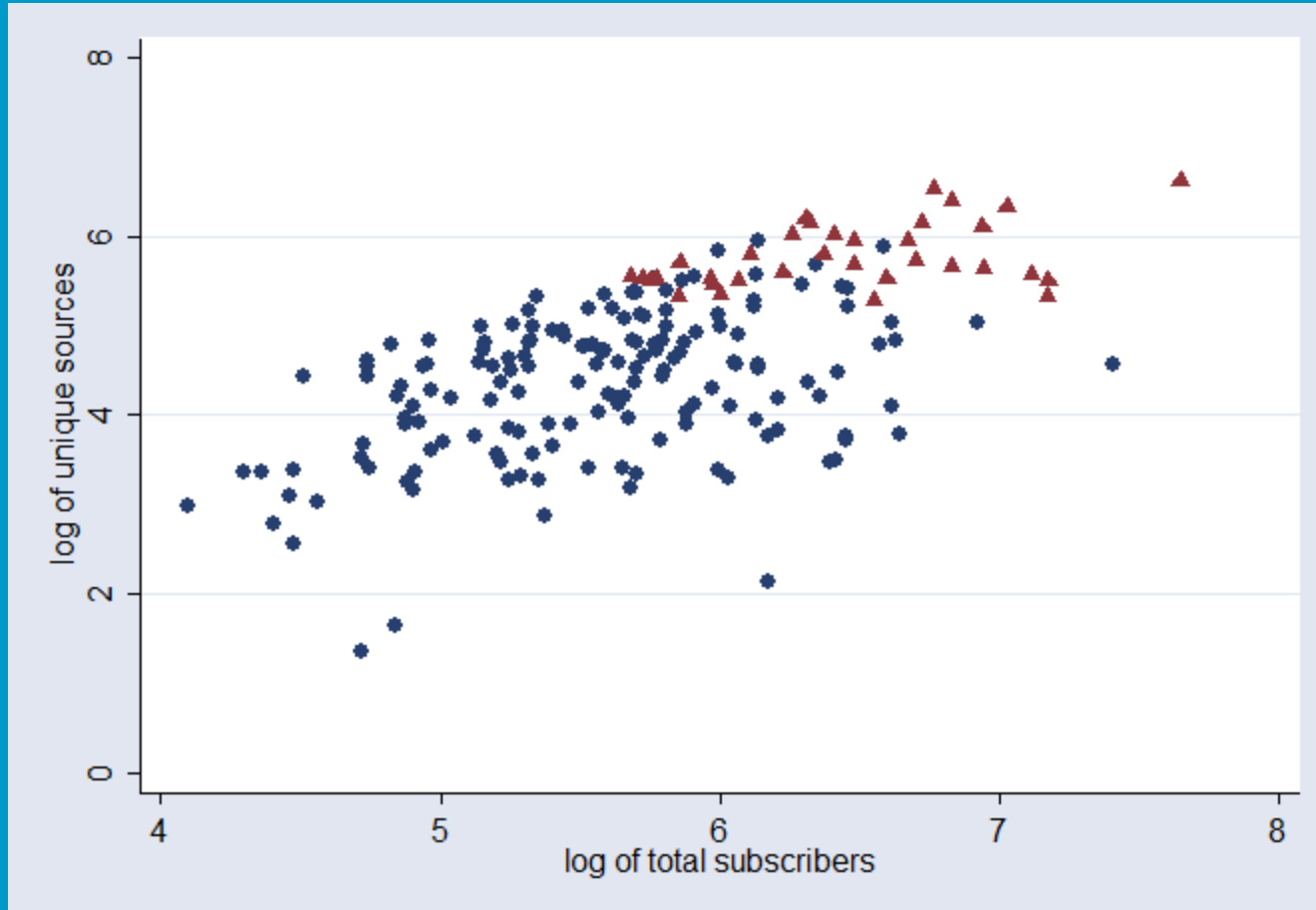
Variability in relative performance as measured by the overlap of the 50 ISPs with the highest number of infected machines *per subscriber* in 2005-2008:
28 ISPs are in the top 50 in all four years

Geographic location



Location of 34 ISPs that were in the top 50 of ISPs with the highest number of infected machines in all years (2005-2008)

Sources and size of ISPs in 2008

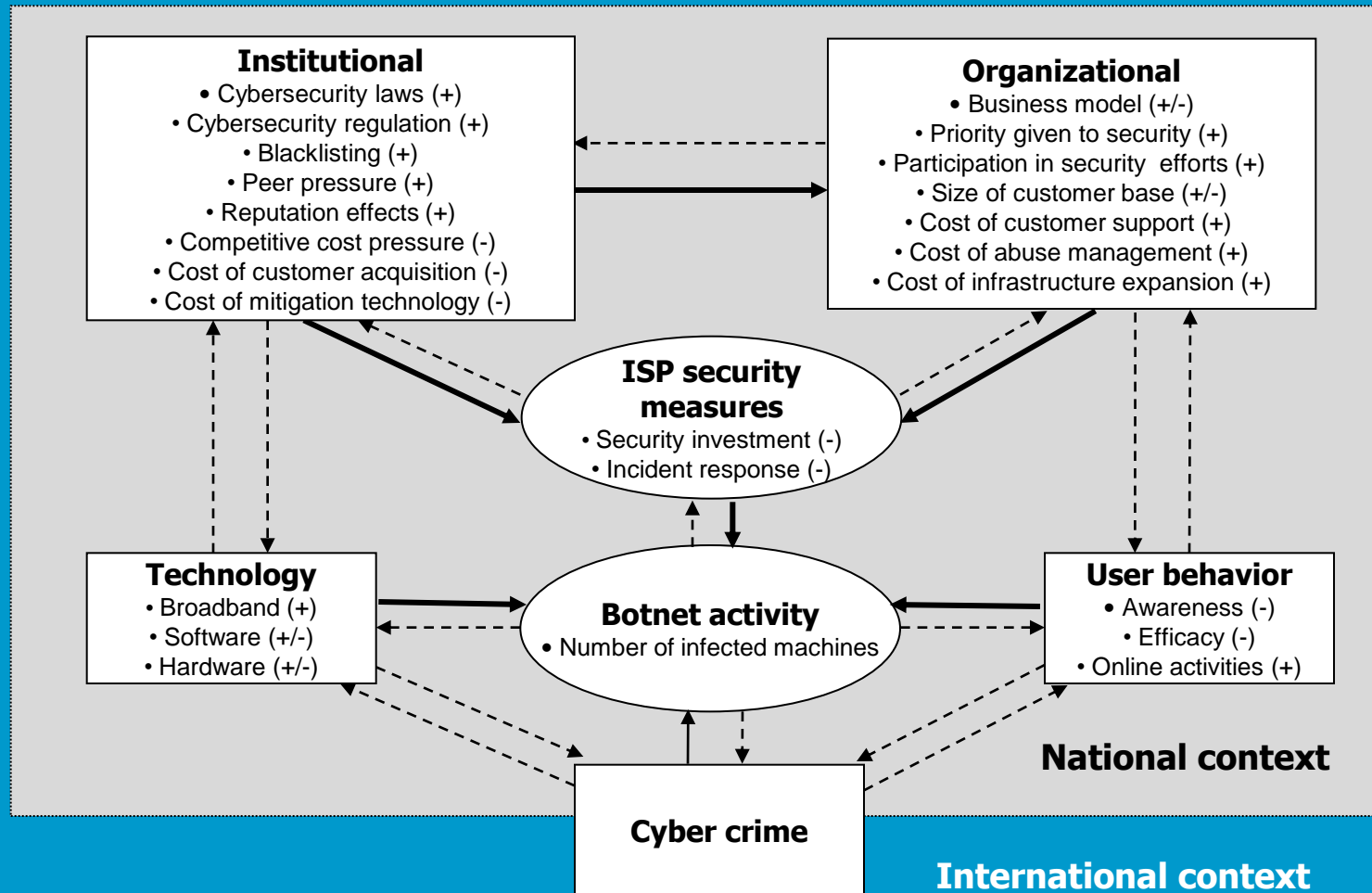


Red triangles indicate 34 ISPs that were in the top 50 of ISPs with the highest number of infected machines in all years (2005-2008)

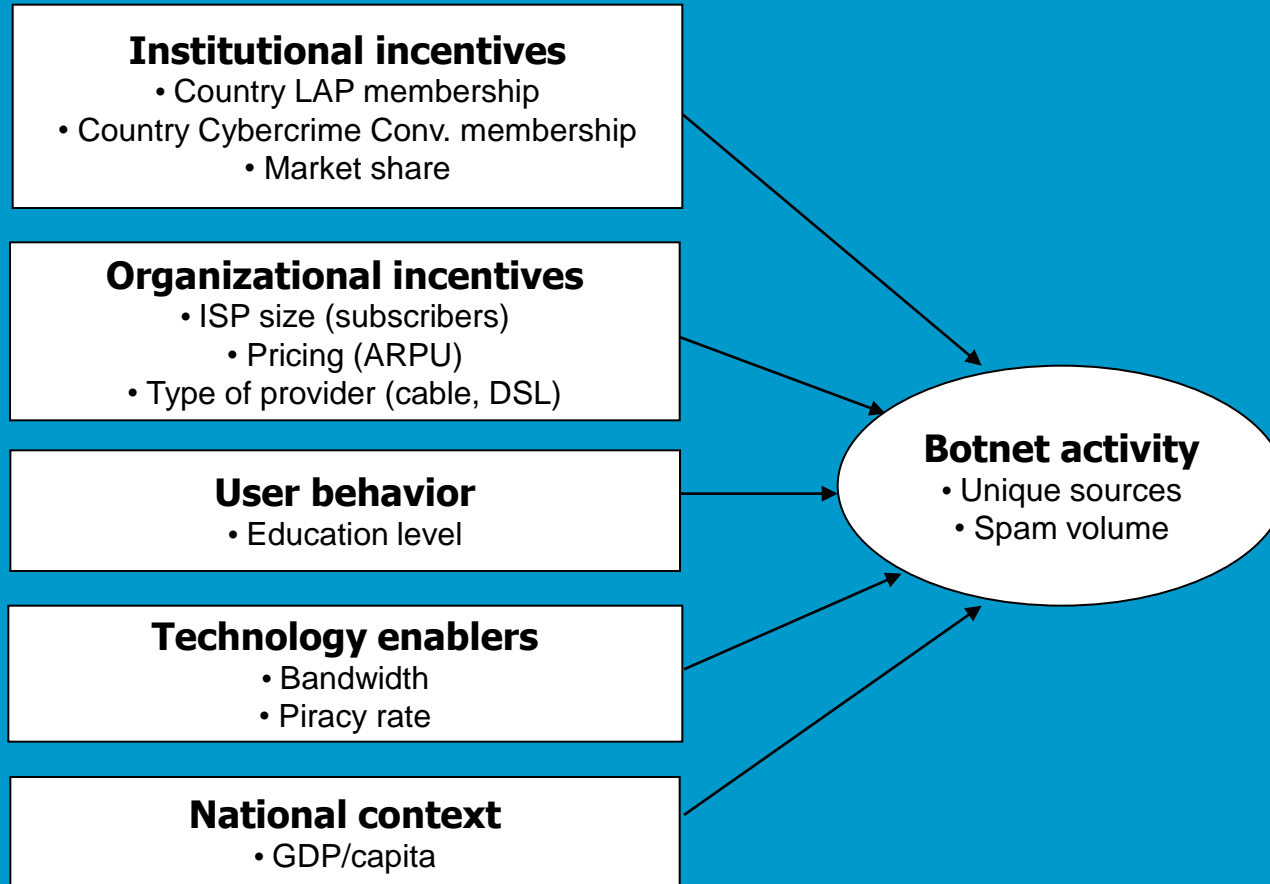
Findings (3) – exploring differences

- How can the differences in performance (as measured in the number of unique sources per subscriber) be explained?

Conceptual framework



Empirical framework



Findings (3) – exploring differences

- *“Very large ISPs are effectively exempt from peer pressure as others cannot afford to cut them off. Much of the world’s bad traffic comes from the networks of these ‘too big to block’ providers.”*
(Moore, Clayton and Anderson, Journal of Economic Perspectives, 2009)
- Hypothesis: Large ISPs have higher infection rates than small ISPs

Findings (3) – exploring differences

Dependent variable: unique sources (log)	All ISPs (β)	Small ISPs (β)	Large ISPs (β)
# Subscribers (log)	0.650 **	0.558 **	0.428 **
Market share	0.077 *	-0.020	0.143 **
Cable provider	-0.086 **	-0.192 **	-0.010
Located in CC country	-0.068	-0.023	-0.072
Located in LAP country	-0.139 **	-0.125 *	-0.234 **
Education index	-0.024	-0.111	0.028
Piracy rate	0.104 **	0.102	0.165 *
_cons	0.466	0.527	-0.498
N	639	300	339
R ² _{adj}	51.4%	36.6%	34.0%

- Finding: on average, large ISPs have lower infection rates than small ISPs

Findings (3) – exploring differences

Dependent variable: unique sources per subscriber (sqrt)	All ISPs
# Subscribers (log)	-0.034 **
Cable provider	-0.451 **
icableXsub(ln)	0.065 **
Located in CC country	-0.040
Located in LAP country	5.055 **
Piracy rate	-0.040 **
Education index	-3.084**
ilapXeducation	-5.597**
ilapXpiracy	0.125**
ieduXpiracy	0.044**
ilapXeducationXpiracy	0.139**
_cons	5.535
N	664
R ² _{adj}	35.9%

In sum

- Worldwide botnet mitigation efforts may have more manageable proportions than previously thought
- External conditions do not seem to dictate ISP efforts
- User base, government regulation, and automation are among possible factors explaining differences among ISPs

Next steps

- Include 2009 data
 - Model improves by including 2009 data
 - Same patterns hold
- Include other data sources on infected machines
 - Conficker sinkhole data
 - DShield/SANS incident data
- Include other independent variables
- Develop metrics and benchmarks on ISP performance
 - In collaboration with Dutch ISPs