2021 USENIX Security Symposium

SocialHEISTing:

Understanding Stolen Facebook Accounts

Jeremiah Onaolapo
University of Vermont

Nektarios Leontiadis
Facebook

Despoina Magka
Facebook

Gianluca Stringhini
Boston University

Social Accounts

- Often publicly display demographic attributes (age, gender, location, etc.)
- Interesting contents in social accounts!
- Accumulate personal info + sentimental value over time
- Attributes can be abused by malicious parties

Goal

- Understand the effects of demographic attributes on attacker behavior in stolen social accounts
- Without harming any real users
- Distinct from general characterization of attacker behavior

How?

Pipeline

Create + populate honey accounts

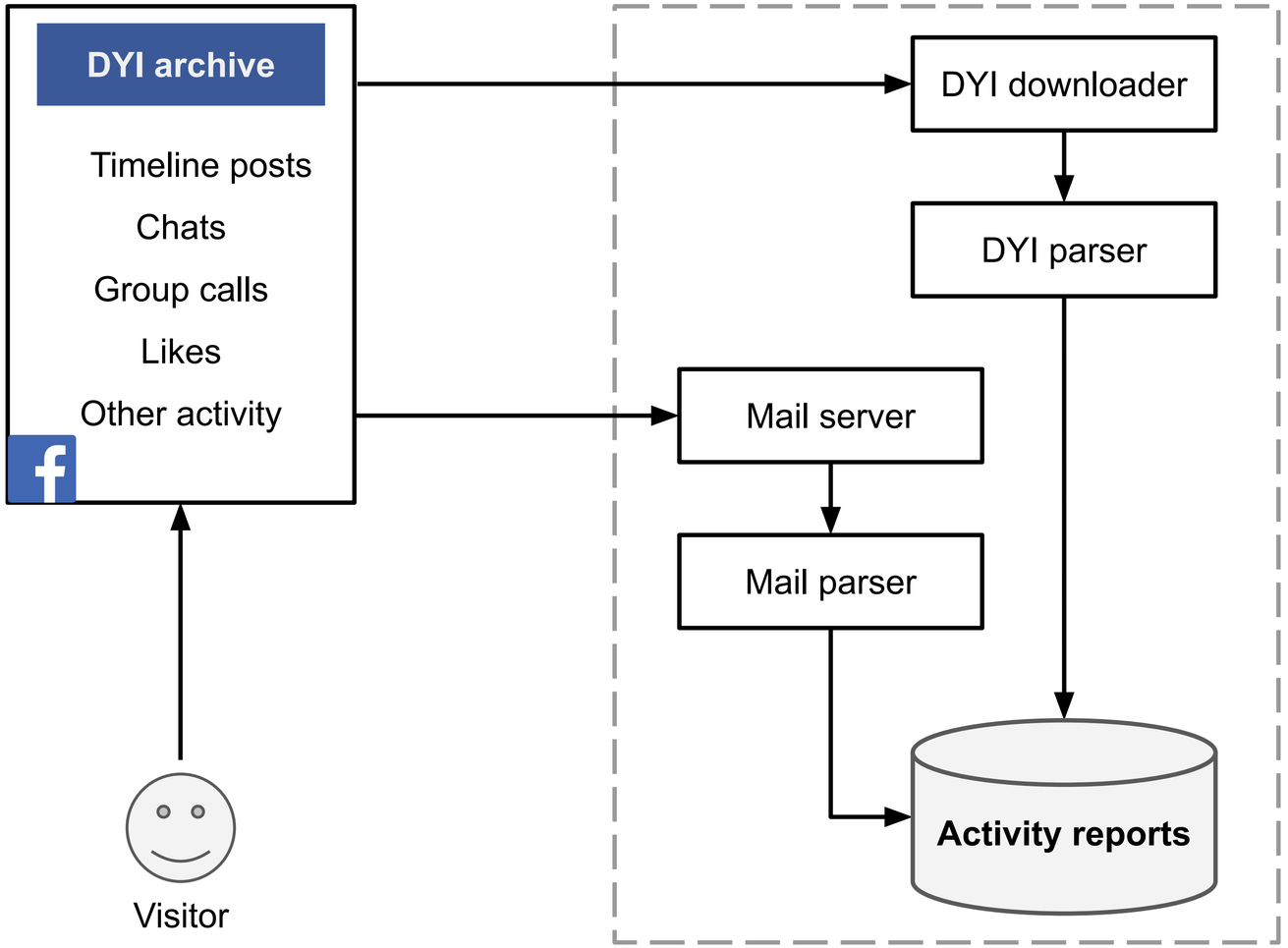
Configure monitor infrastructure

Leak honey credentials

Record + analyze data

Better understand
cybercriminal behavior

Data Collection



Setup

- 1008 realistic Facebook accounts (*age, gender* vars)
- Populated with publicly available data (sanitized)
- Leaked credentials to two-thirds of the accounts
- Via paste sites on Surface Web + Dark Web
- Monitored accounts for 6 months

Results

Actions

- 322 unique accesses to
- 284 accounts, resulting in
- 1,159 actions
- *Curious, Searcher, and Chatty* activity tops the actions table

Age of Account

Criminals...

- **Add/remove friends:** adult accounts > teen accounts
- **Edit profiles:** adult accounts < teen accounts
- **Create posts, chat:** adult accounts < teen accounts

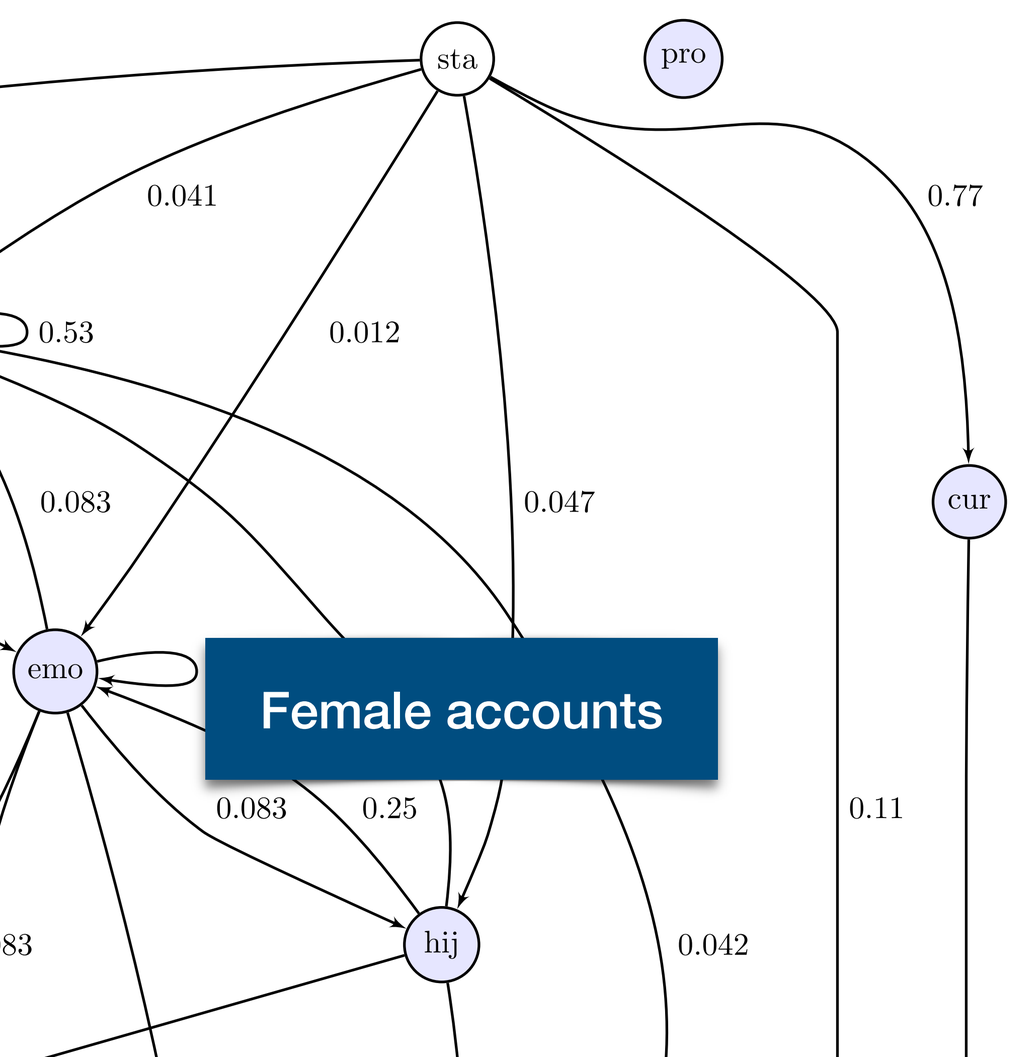
Gender of Account

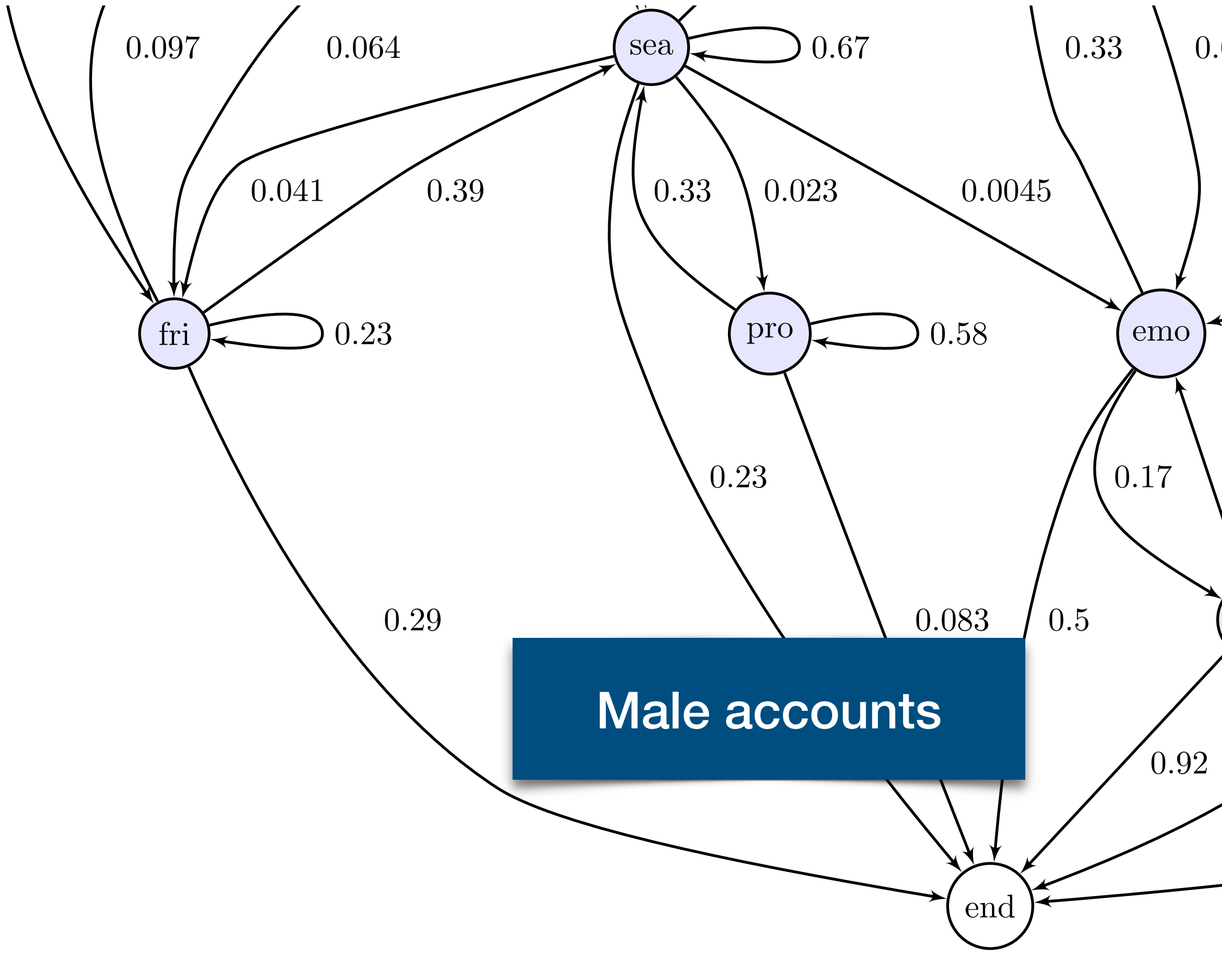
Criminals...

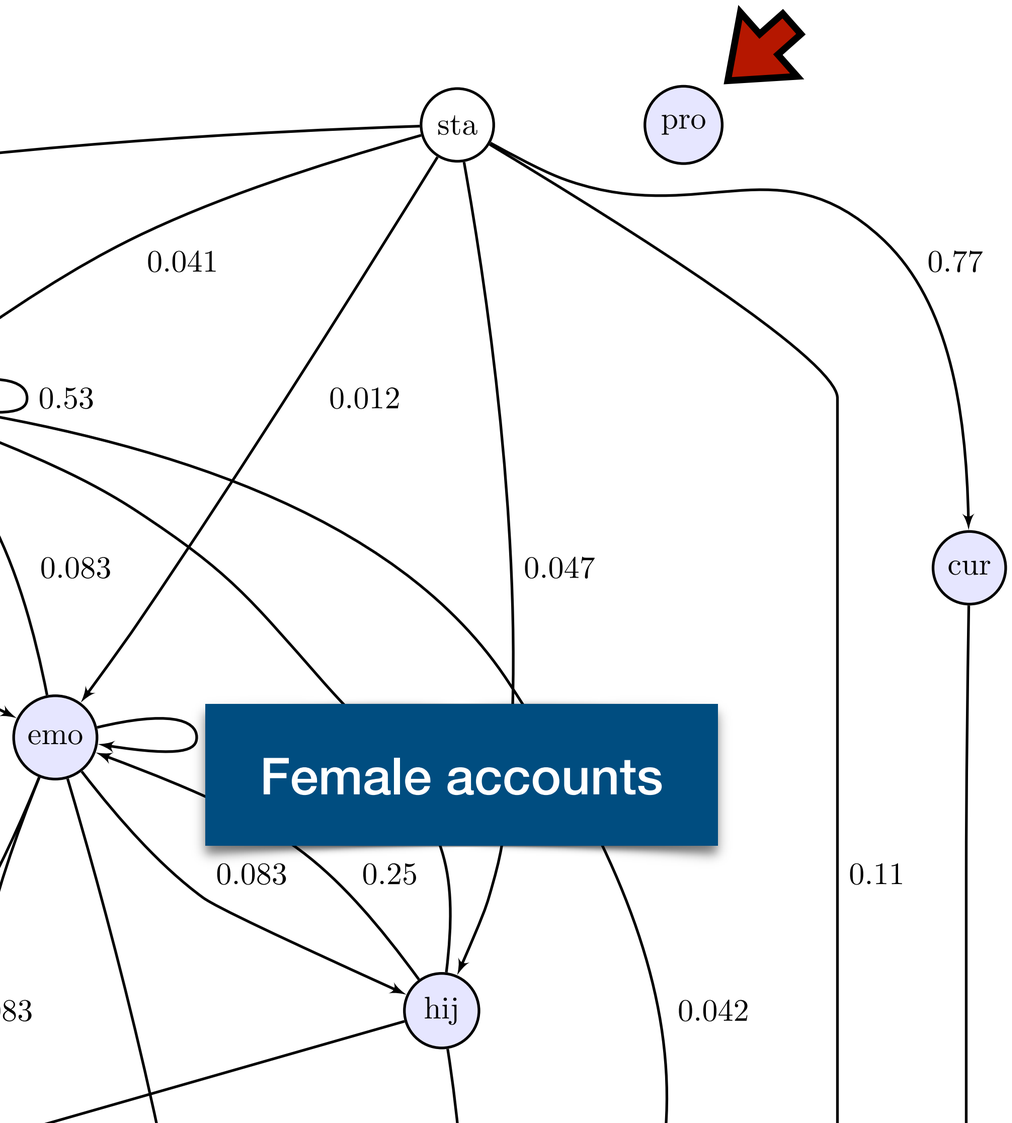
- **Add/remove friends:** female accounts > male accounts
- **Edit profiles:** female accounts (none) < male accounts
- **Search:** female accounts < male accounts

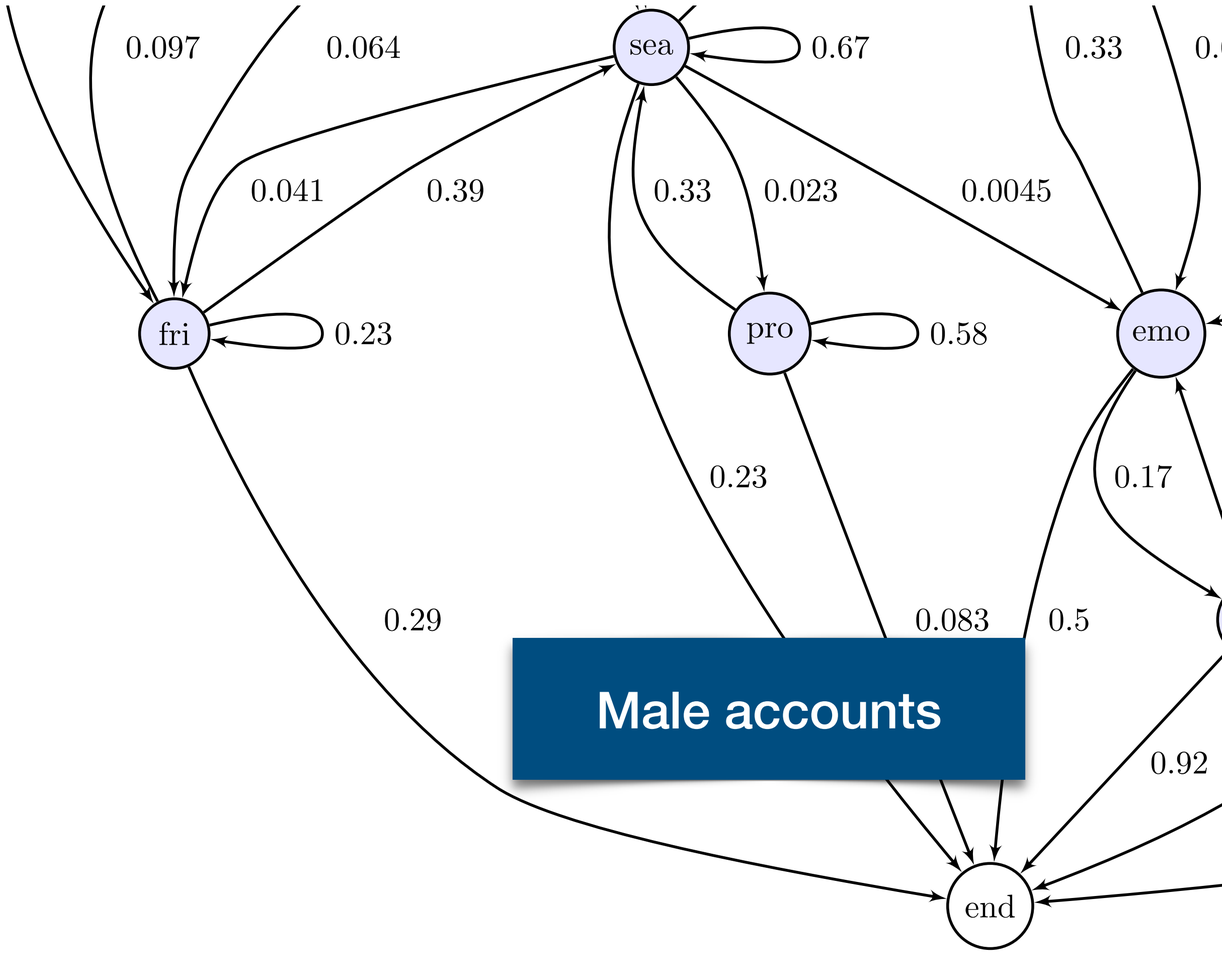
Action Sequences

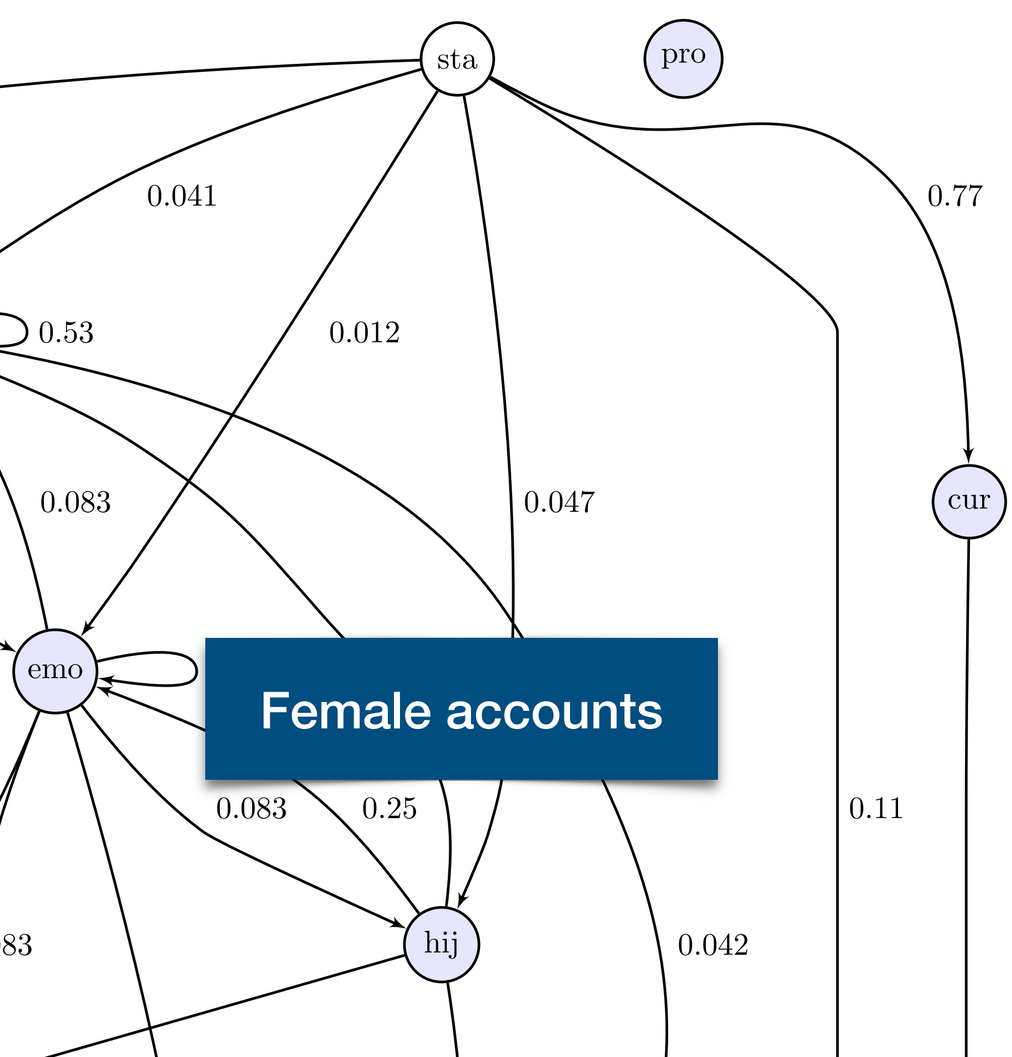
- Modeled action sequences as graphs; edge weights as probabilities of transitions
- Transitions from *action* to *other action* differed across the age and gender dimensions of victim accounts
- Illustrative example: *emo* → *cha* → *hij*

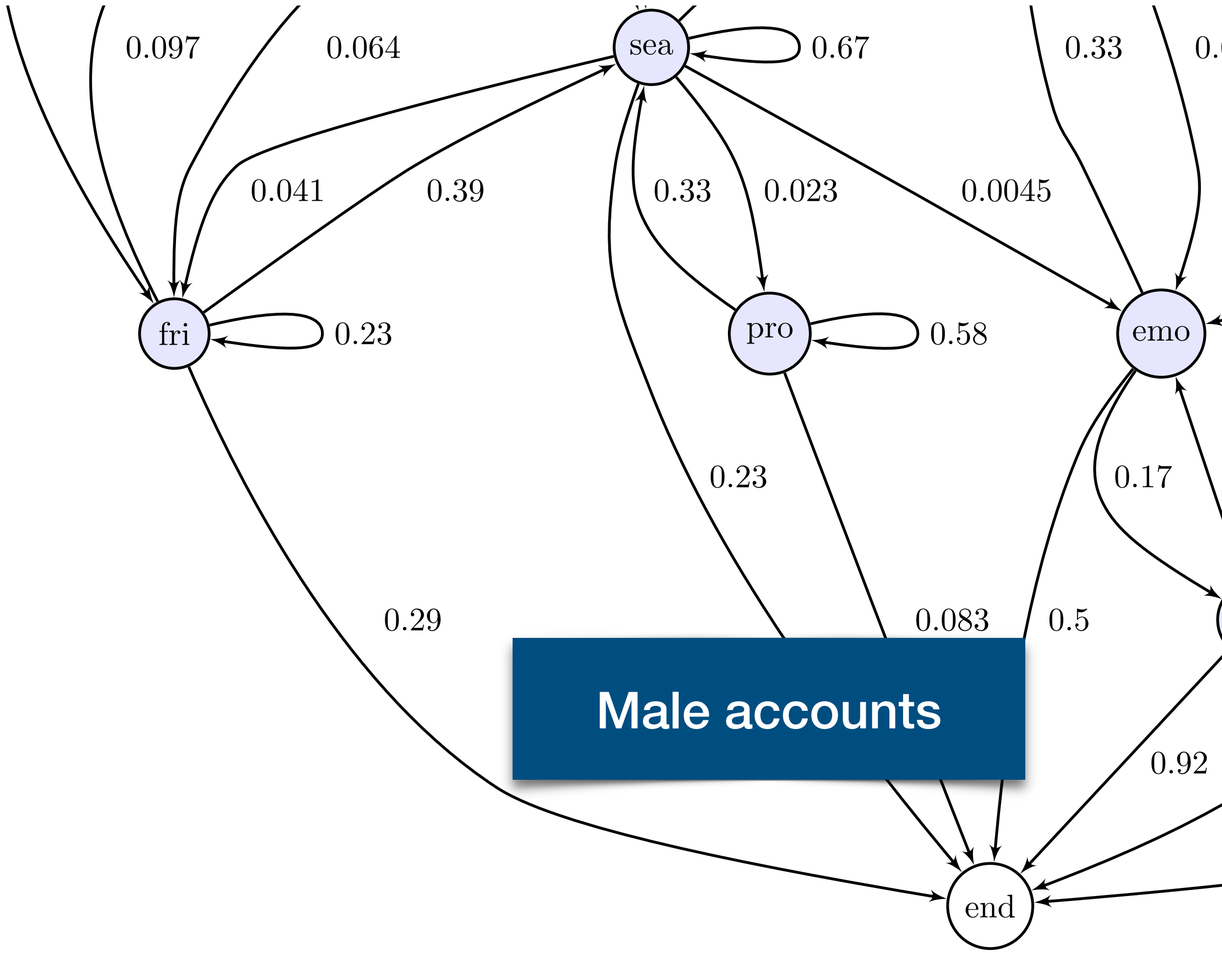

sta
pro
0.041
0.77
0.53
0.012
0.083
0.047
cur
emo
Female accounts
0.083
0.25
0.11
hij
0.042

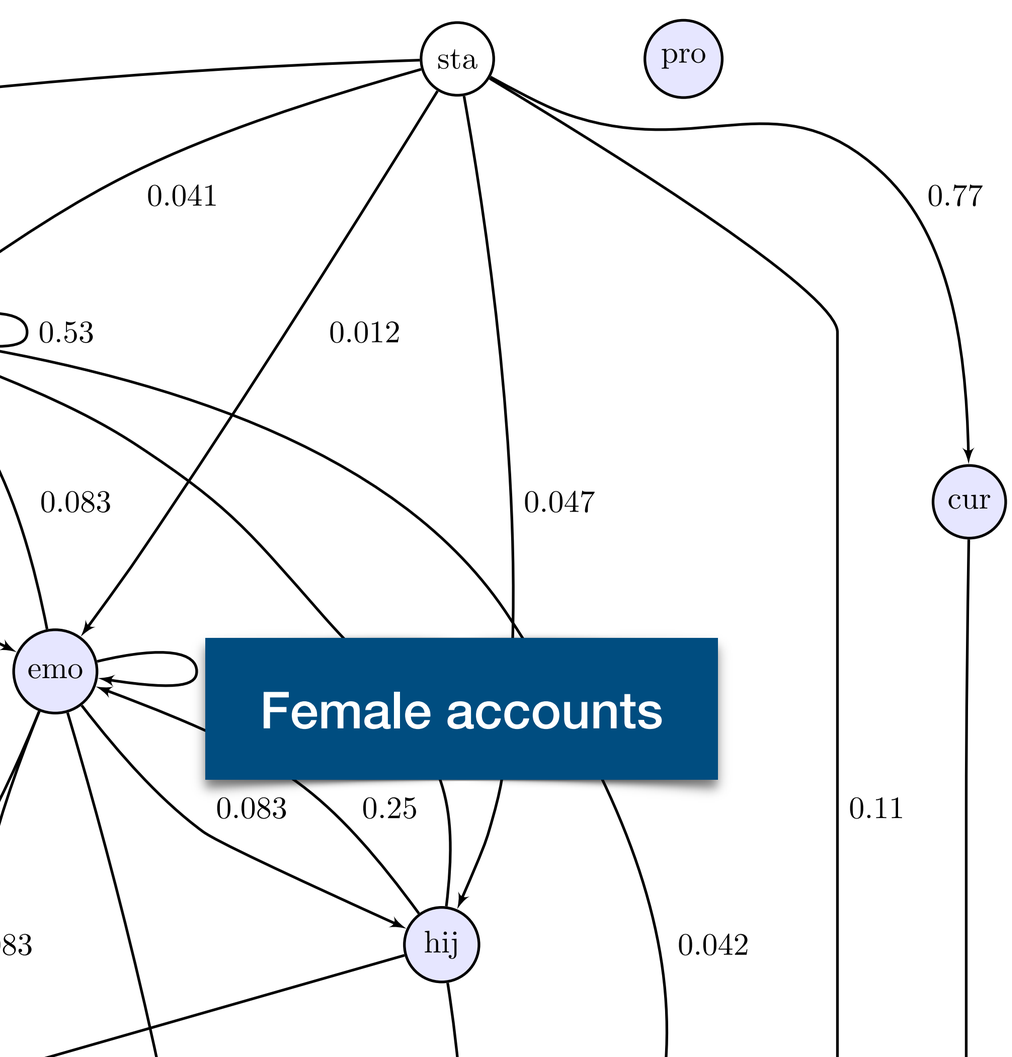

0.097
0.064
sea
0.67
0.33
0.041
0.39
0.33
0.023
0.0045
fri
0.23
pro
0.58
emo
0.23
0.17
0.29
0.083
0.5
Male accounts
0.92
end

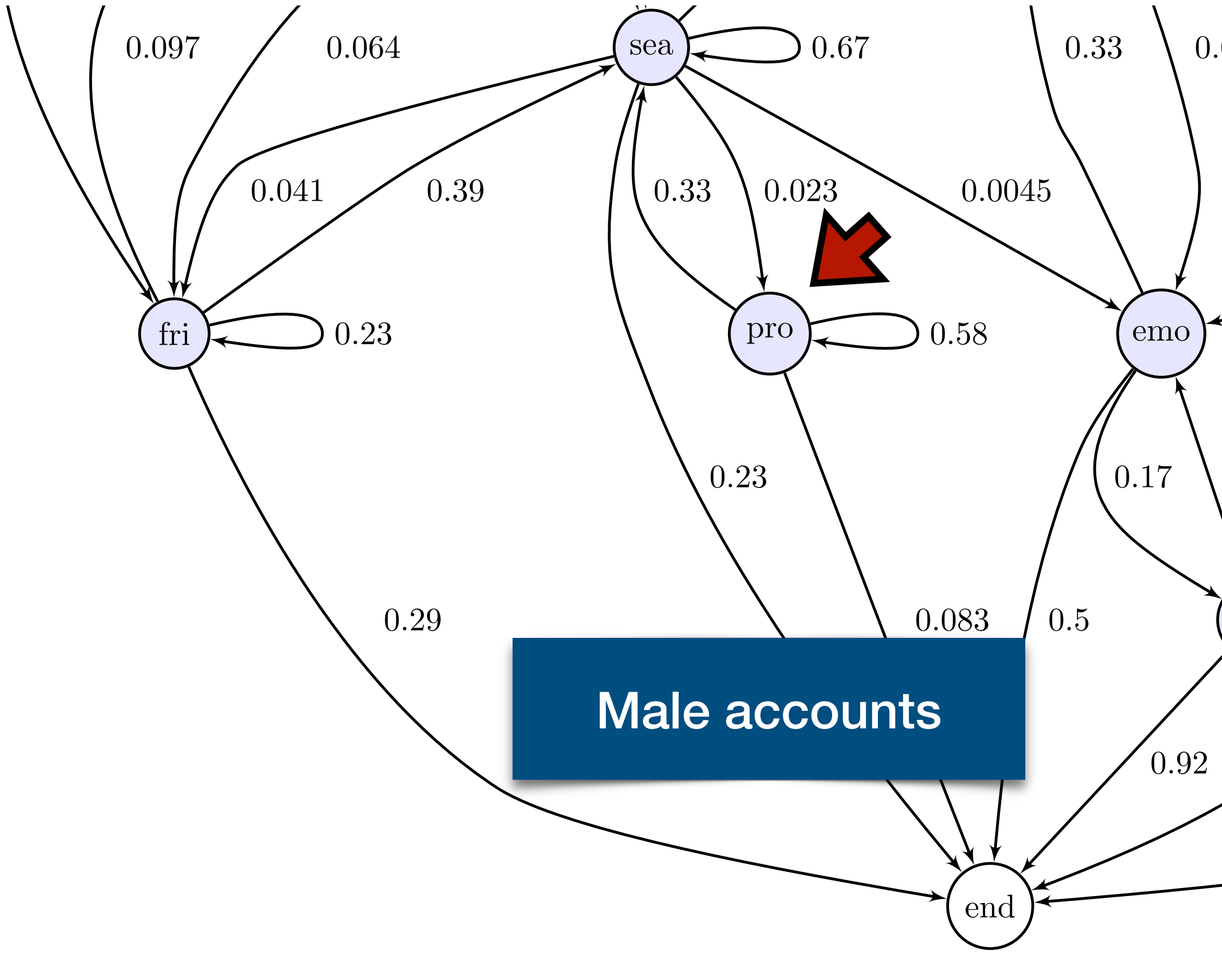

sta
pro
0.041
0.77
0.53
0.012
0.083
0.047
cur
emo
Female accounts
0.083
0.25
0.11
hij
0.042

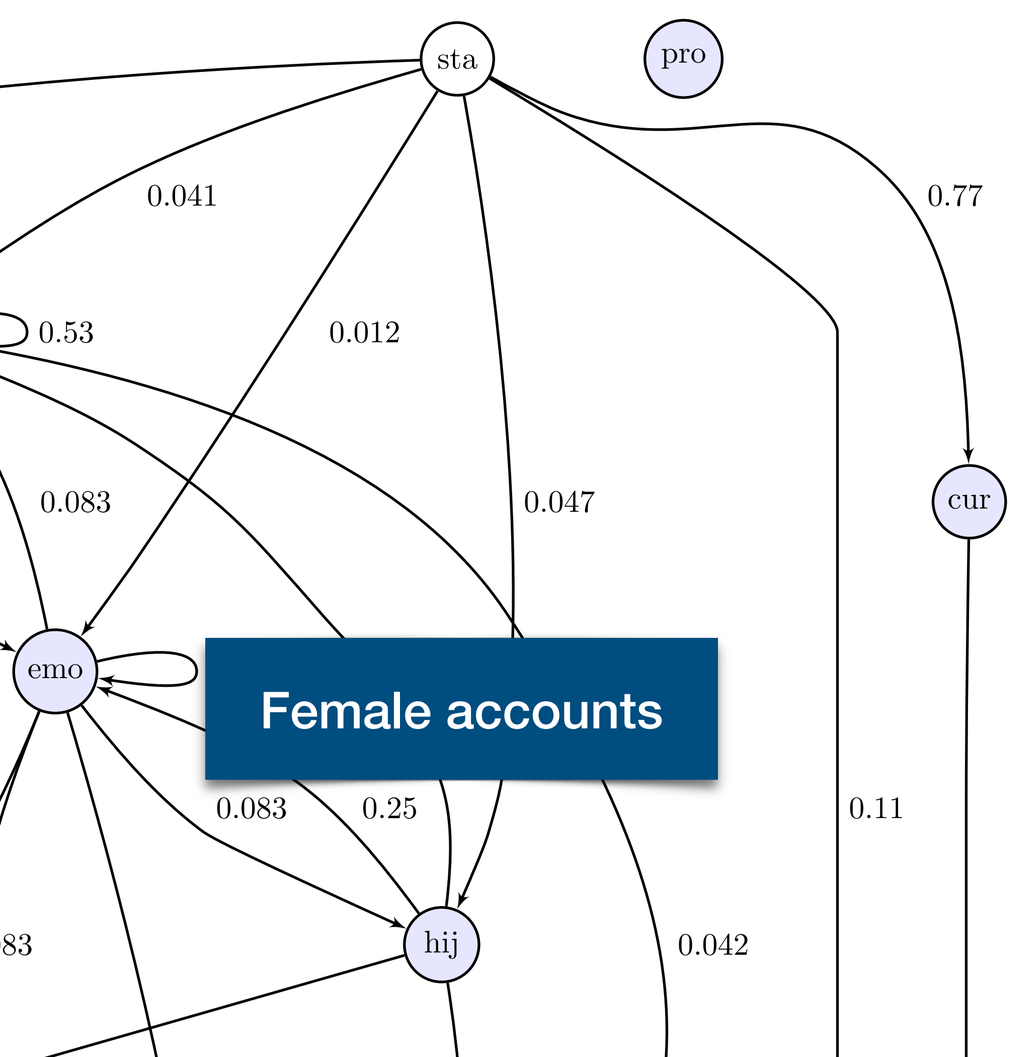

0.097
0.064
sea
0.67
0.33
0.041
0.39
0.33
0.023
0.0045
fri
0.23
pro
0.58
emo
0.23
0.17
0.29
0.083
0.5
Male accounts
0.92
end

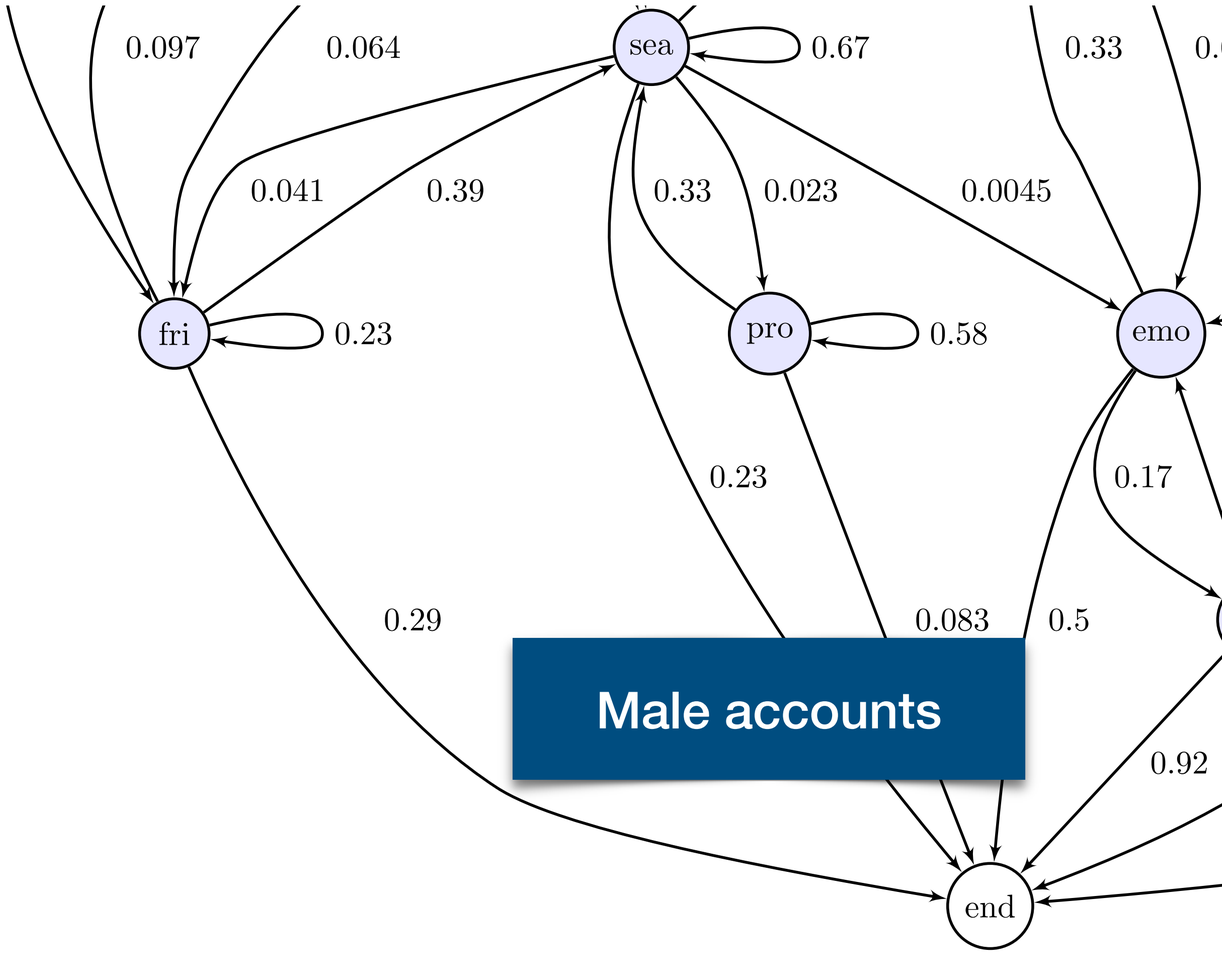

sta
pro
0.041
0.77
0.53
0.012
0.083
0.047
cur
emo
Female accounts
0.083
0.25
0.11
hij
0.042


0.097
0.064
sea
0.67
0.33
0.041
0.39
0.33
0.023
0.0045
fri
0.23
pro
0.58
emo
0.23
0.17
0.29
0.083
0.5
Male accounts
0.92
end


sta
pro
cur
emo
hij
0.041
0.77
0.53
0.012
0.083
0.047
0.083
0.25
0.11
0.042
Female accounts


sea
fri
pro
emo
end
0.097
0.064
0.67
0.33
0.041
0.39
0.33
0.023
0.0045
0.23
0.58
0.23
0.17
0.29
0.083
0.5
0.92
Male accounts


sta
pro
0.041
0.77
0.53
0.012
0.083
0.047
cur
emo
Female accounts
0.083
0.25
0.11
hij
0.042

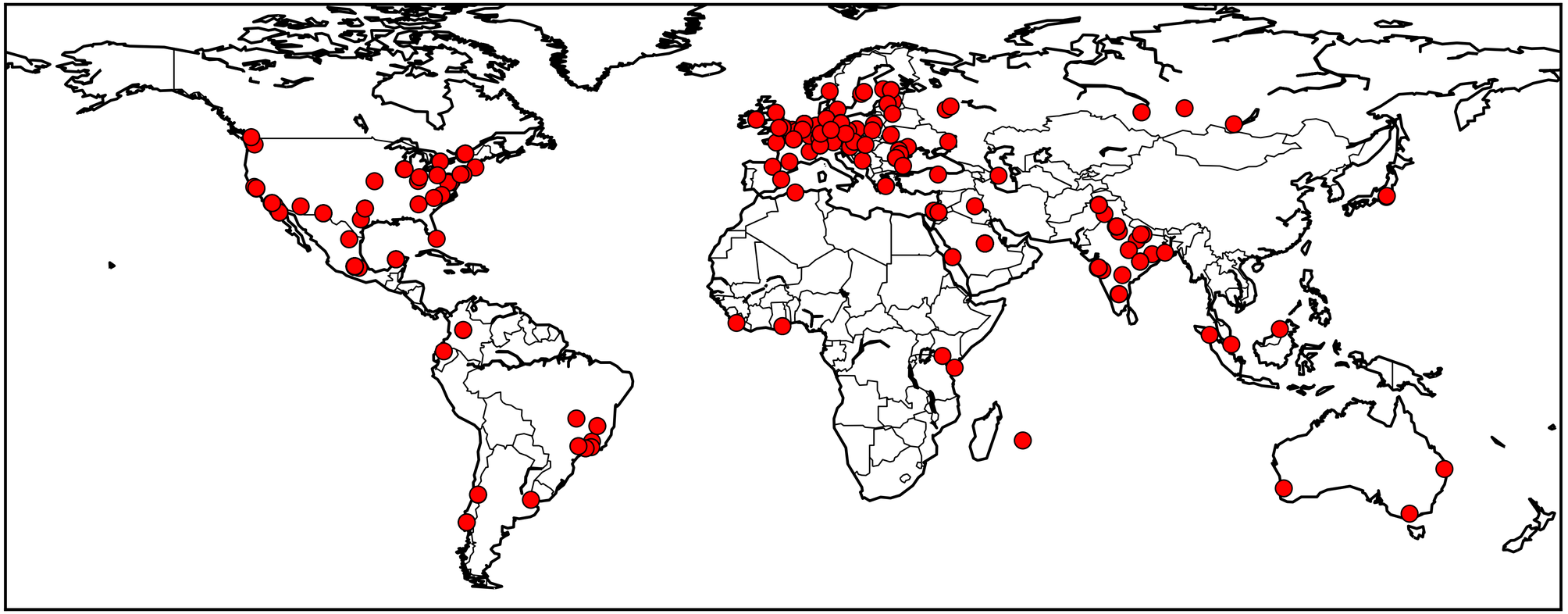

0.097
0.064
sea
0.67
0.33
0.041
0.39
0.33
0.023
0.0045
fri
0.23
pro
0.58
emo
0.23
0.17
0.29
0.083
0.5
Male accounts
0.92
end

Origins of Accesses

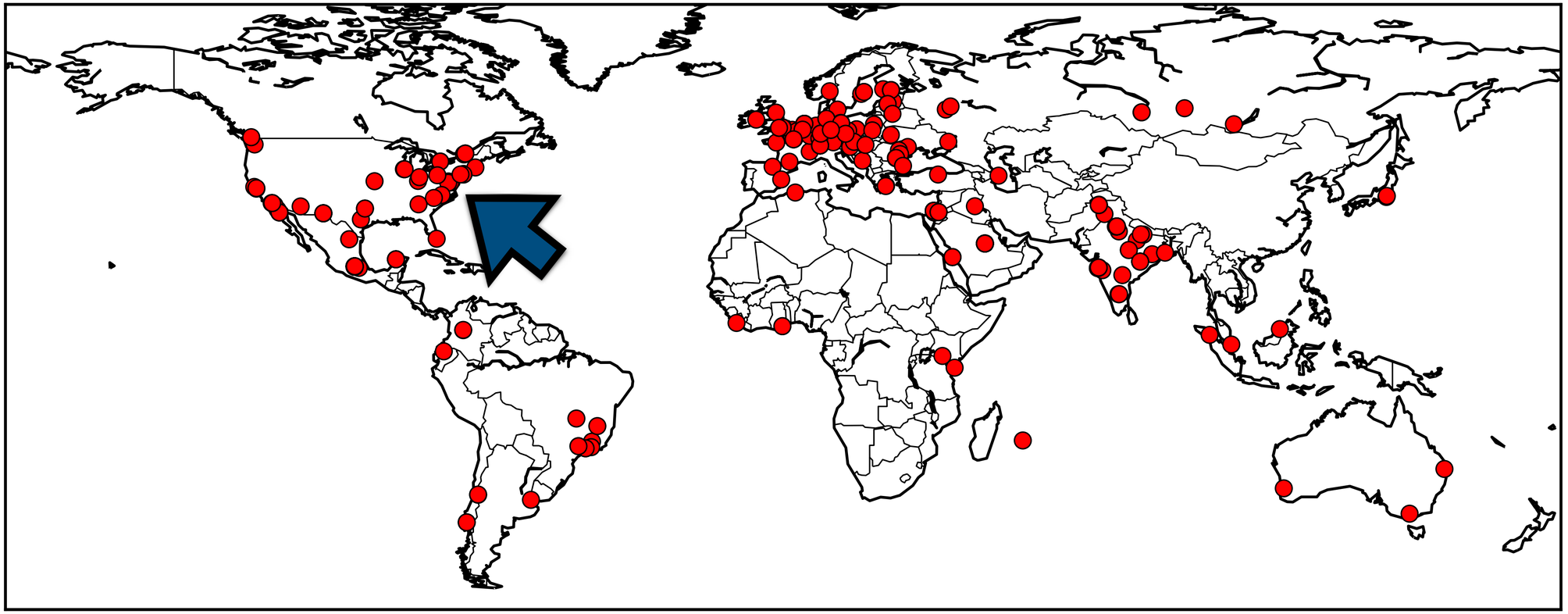
- 415 IP addresses (a mix of IPv4 and IPv6)
- 53 countries
- 39 TOR exit nodes

Caveat: Some may be VPNs and proxies

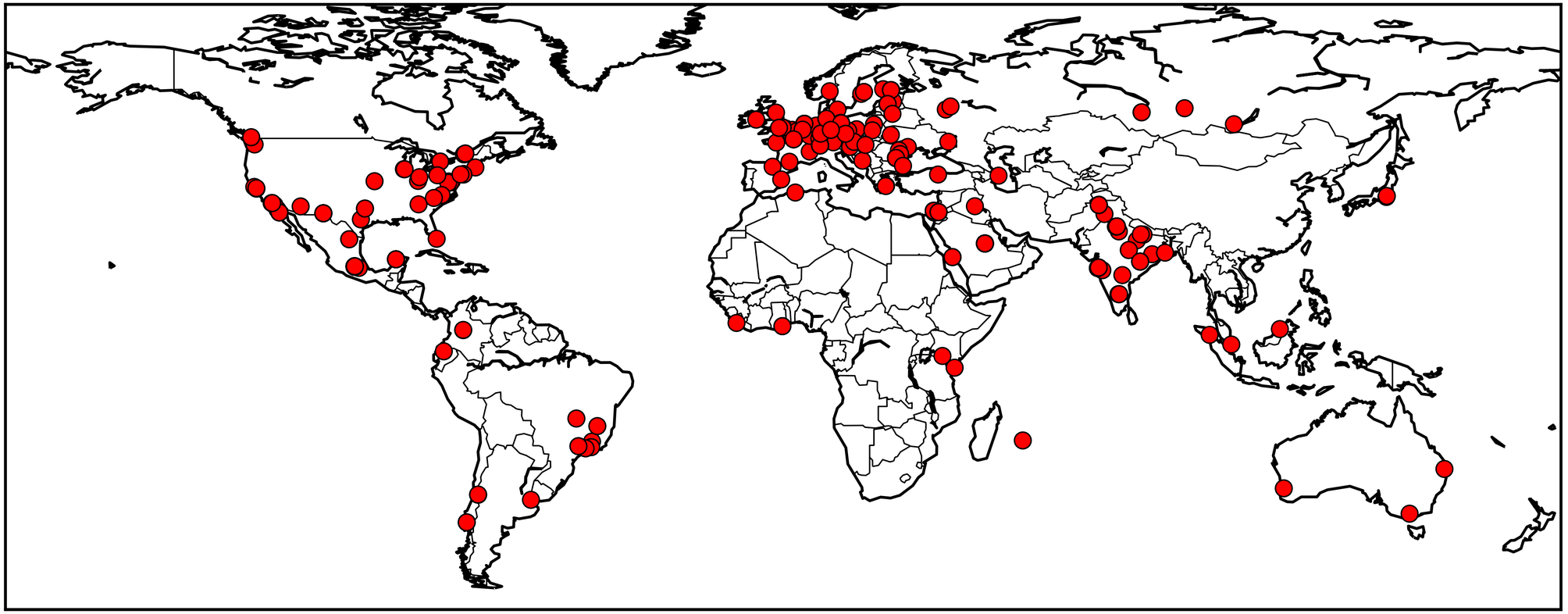
Origins of Accesses



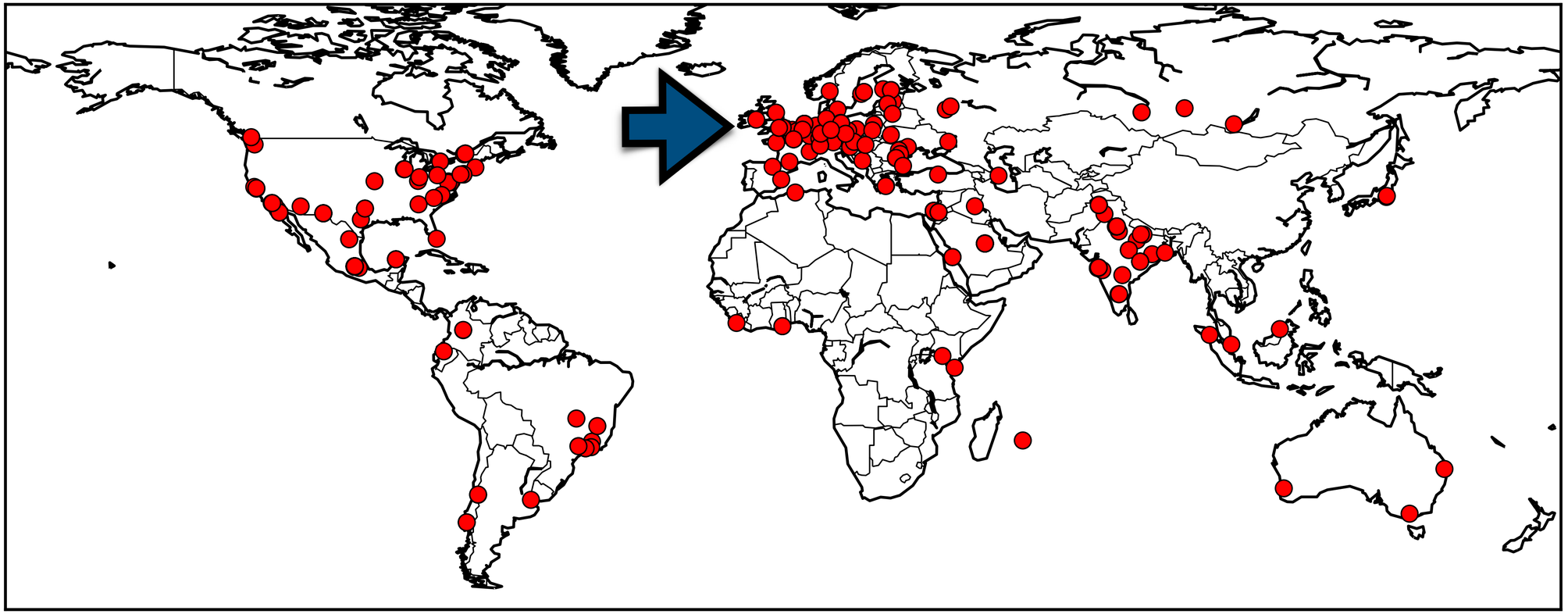
Origins of Accesses



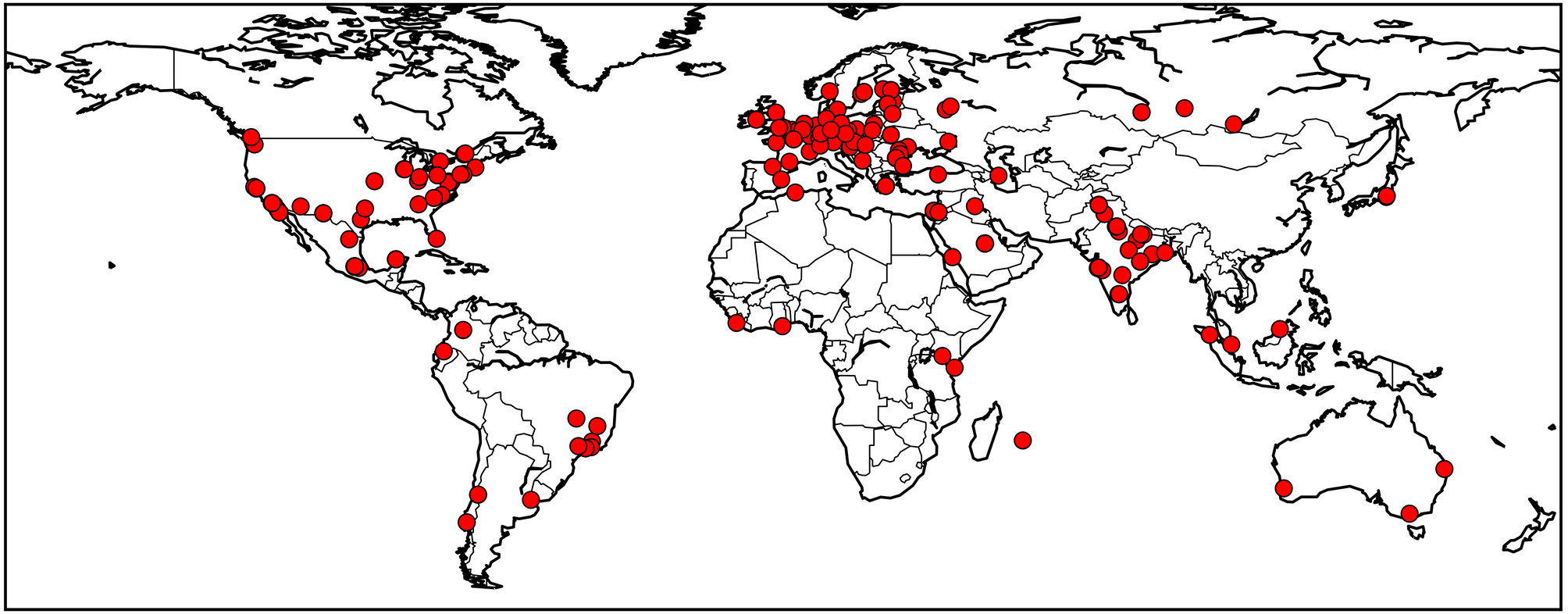
Origins of Accesses



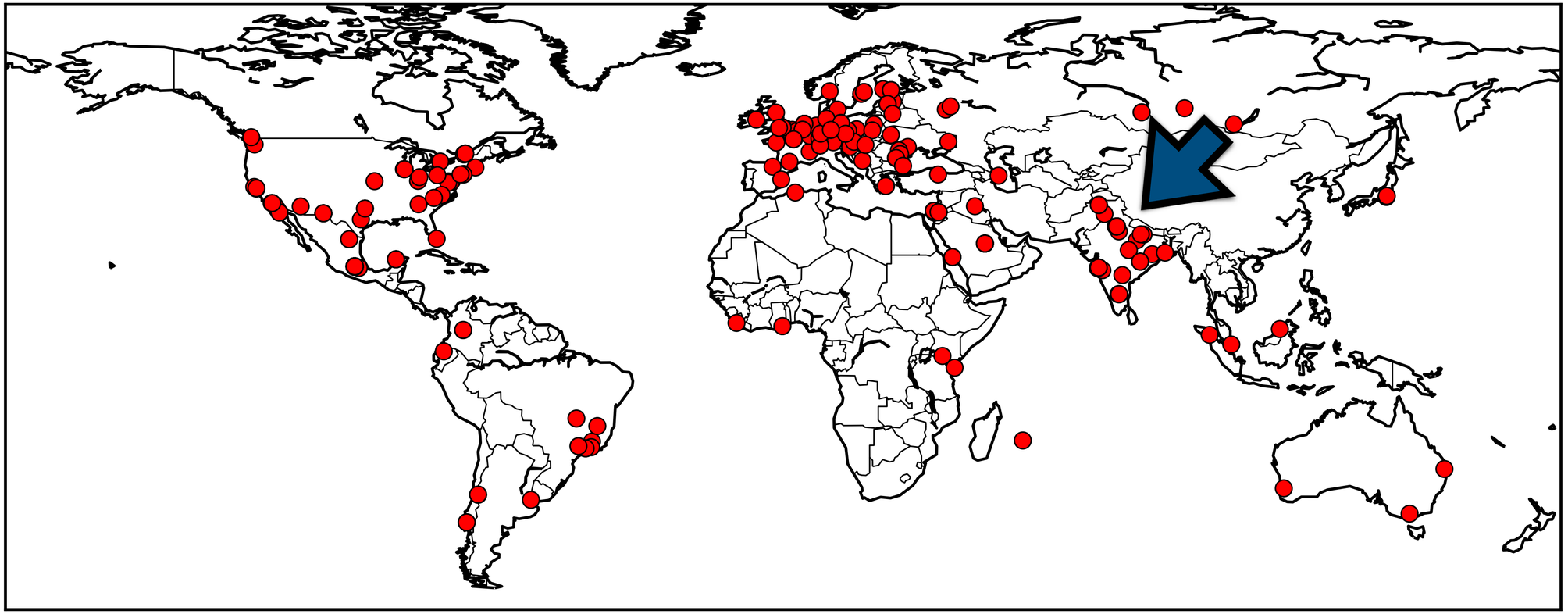
Origins of Accesses



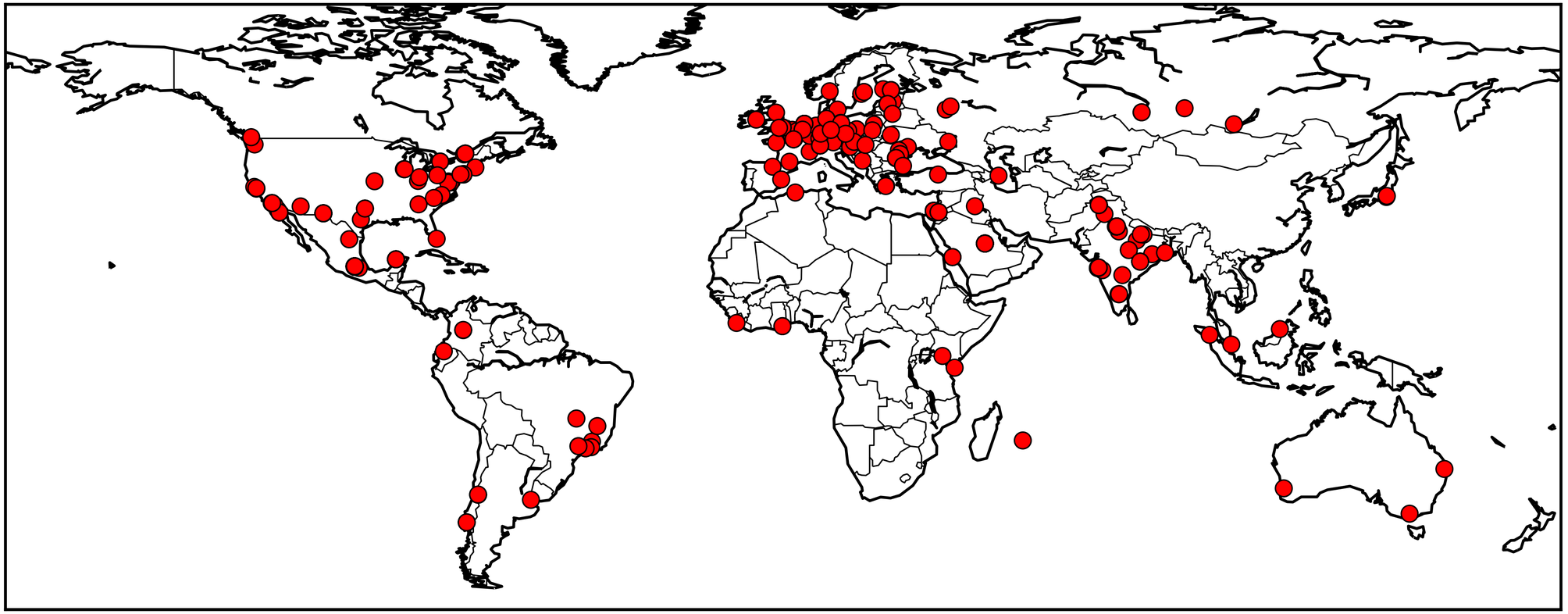
Origins of Accesses



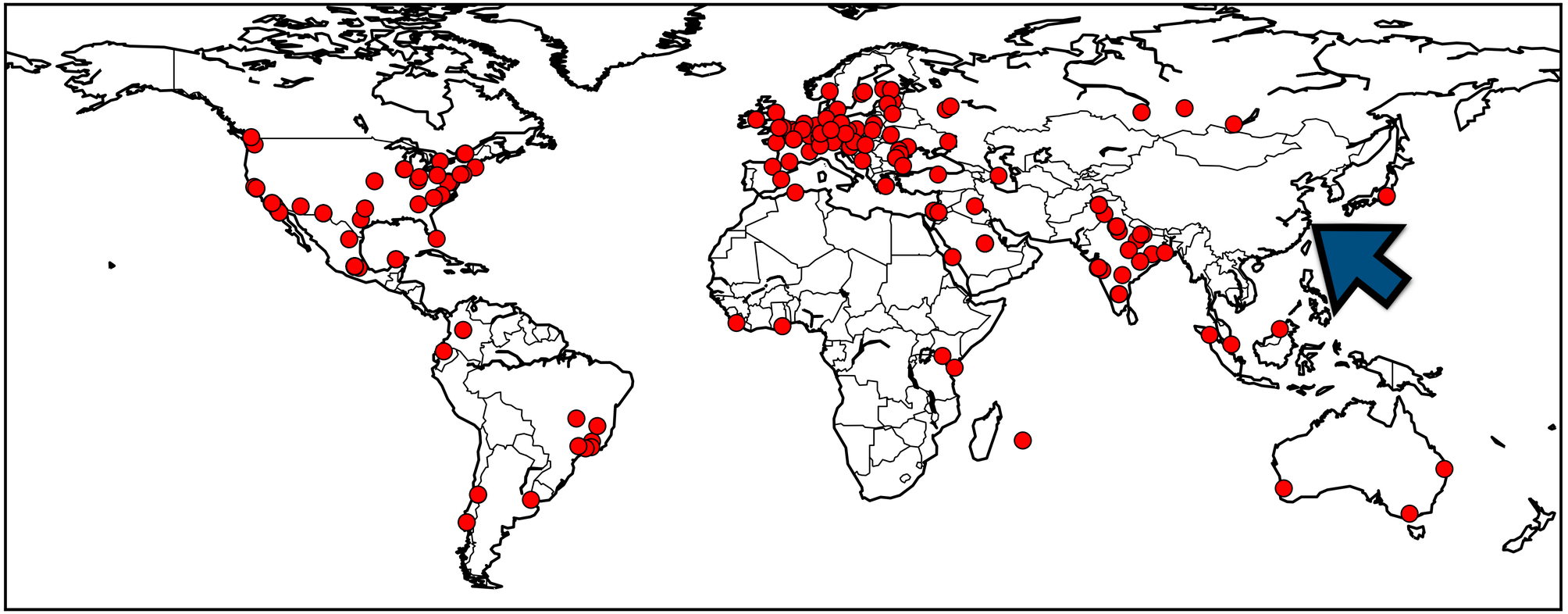
Origins of Accesses



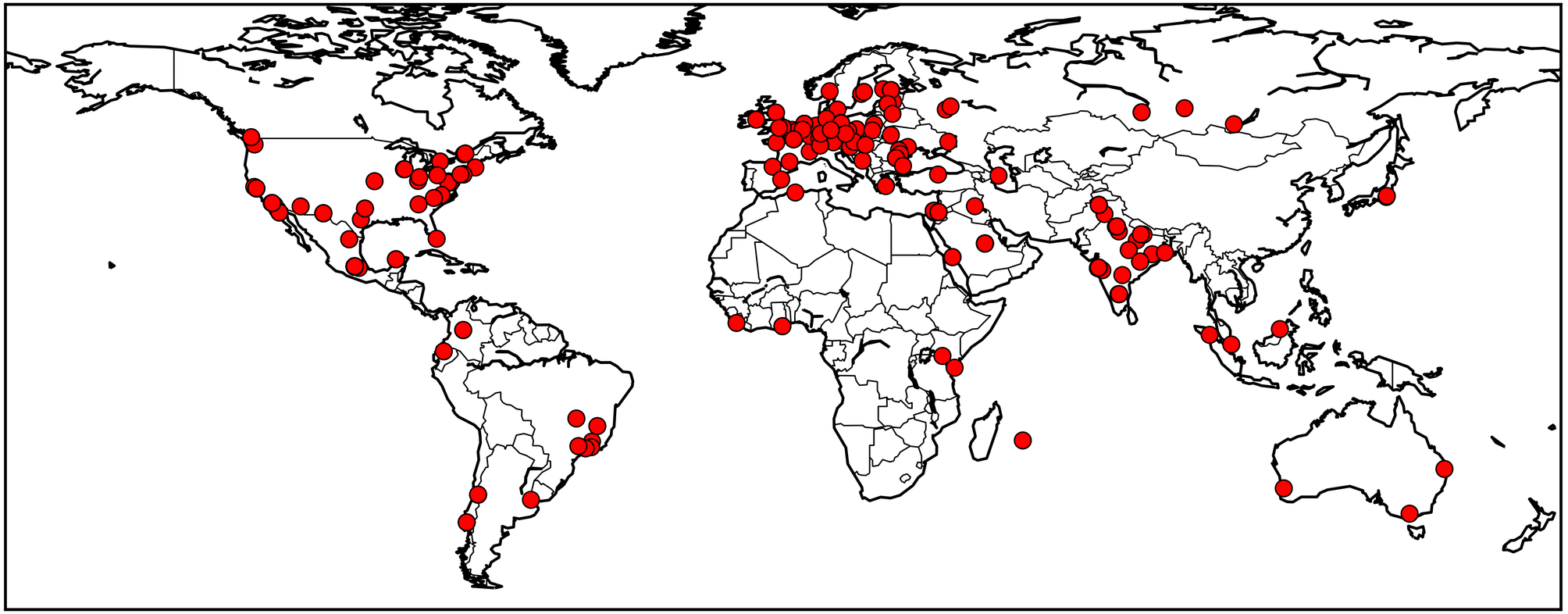
Origins of Accesses



Origins of Accesses



Origins of Accesses



Summing Up

Implications

- Need to rethink detection and mitigation systems
- Along demographic (and other?) attributes
- More work needs to be done in this area

Ethics

- Used test accounts; isolated from regular Facebook social graph
- Used publicly available stock photos and social posts
- Facebook contacts kept an eye on the accounts
- Obtained IRB ethics approval

Thanks!

- Jeremiah Onaolapo, *University of Vermont*
  - jeremiah.onaolapo { at } uvm.edu
  - www.uvm.edu/~jonaolap
- Nektarios Leontiadis, *Facebook*
- Despoina Magka, *Facebook*
- Gianluca Stringhini, *Boston University*