Network Abuse BoF
APNIC 34
Phnom Penh, Cambodia

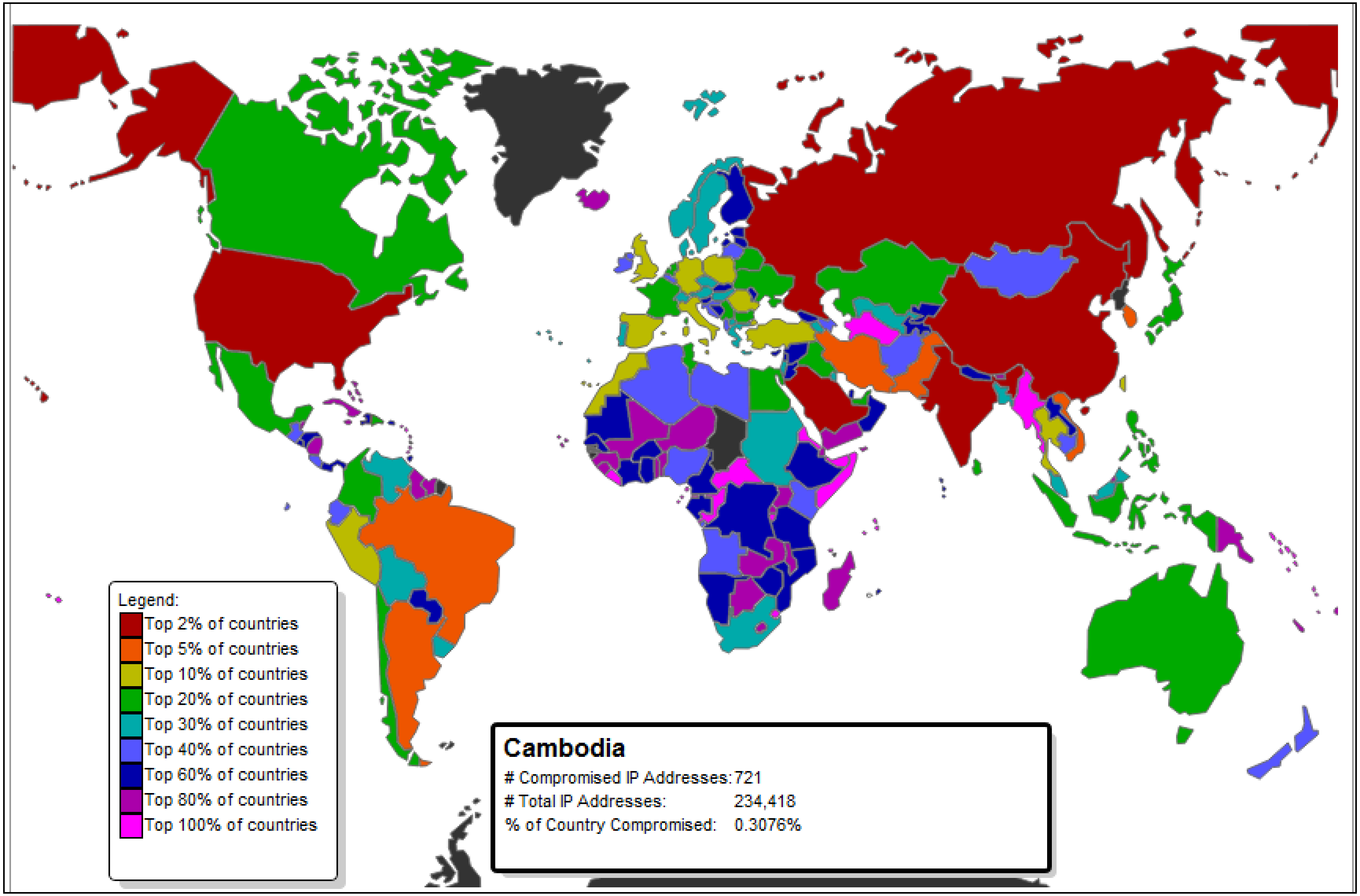
Aftab A. Siddiqui
aftabs@cyber.net.pk

CYBERNET

Introduction - Reasoning

- Network related abuse is on the rise all around the world.
- For SP it’s a night mare in terms of OPEX to deal with network abuse:
  - Internal threats
  - External threats
- Now deal with Abuse reports on top of that.
- How organizations are handling network based attacks
- How organizations handle abuse complaints from within their networks
- Significance of having a valid IRT object

TC No. of IPs Compromised



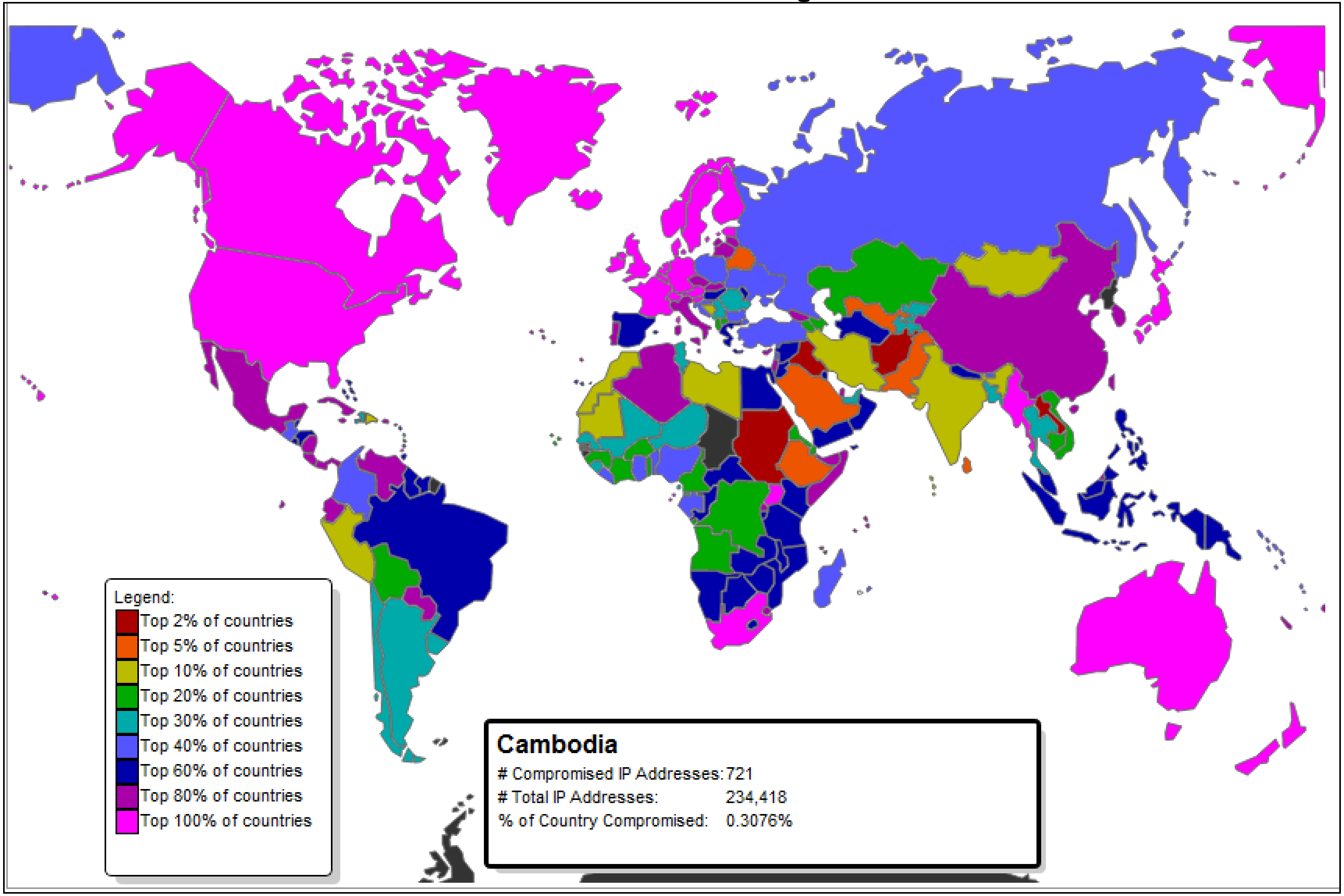
Cambodia

Compromised IP Addresses: 721

Total IP Addresses: 234,418

% of Country Compromised: 0.3076%

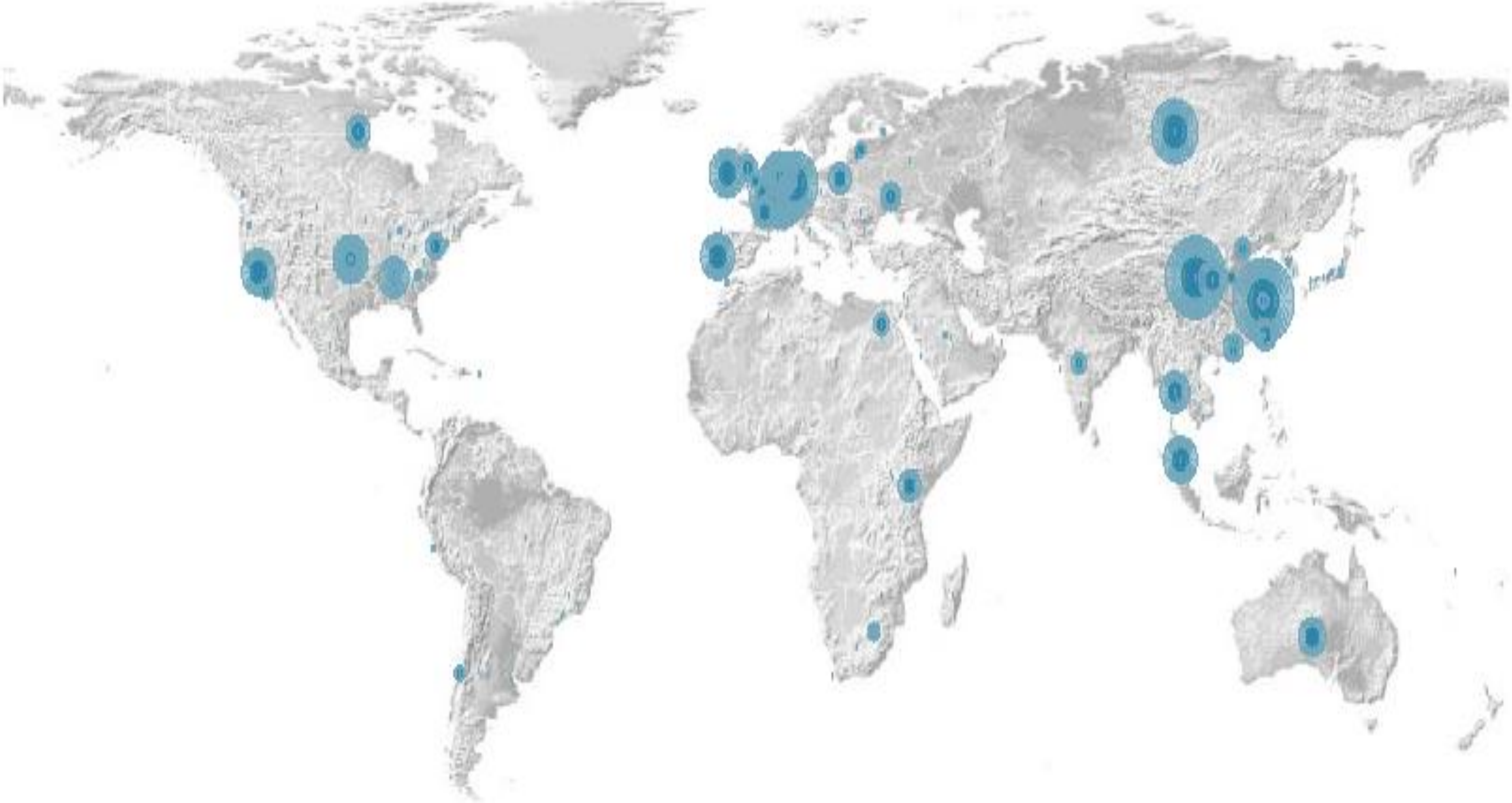
TC % of IPs Compromised



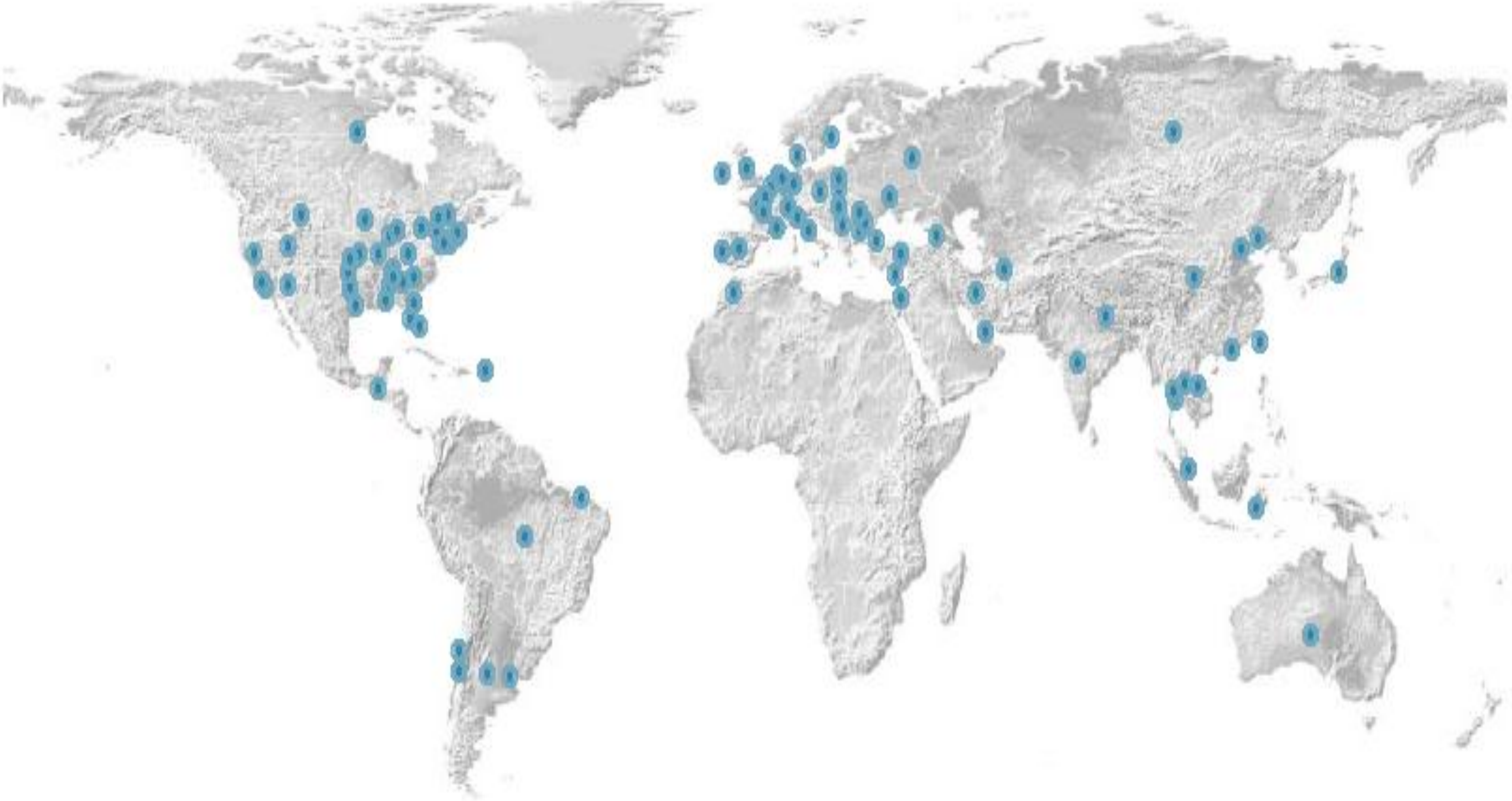
Cambodia

# Compromised IP Addresses:	721
# Total IP Addresses:	234,418
% of Country Compromised:	0.3076%

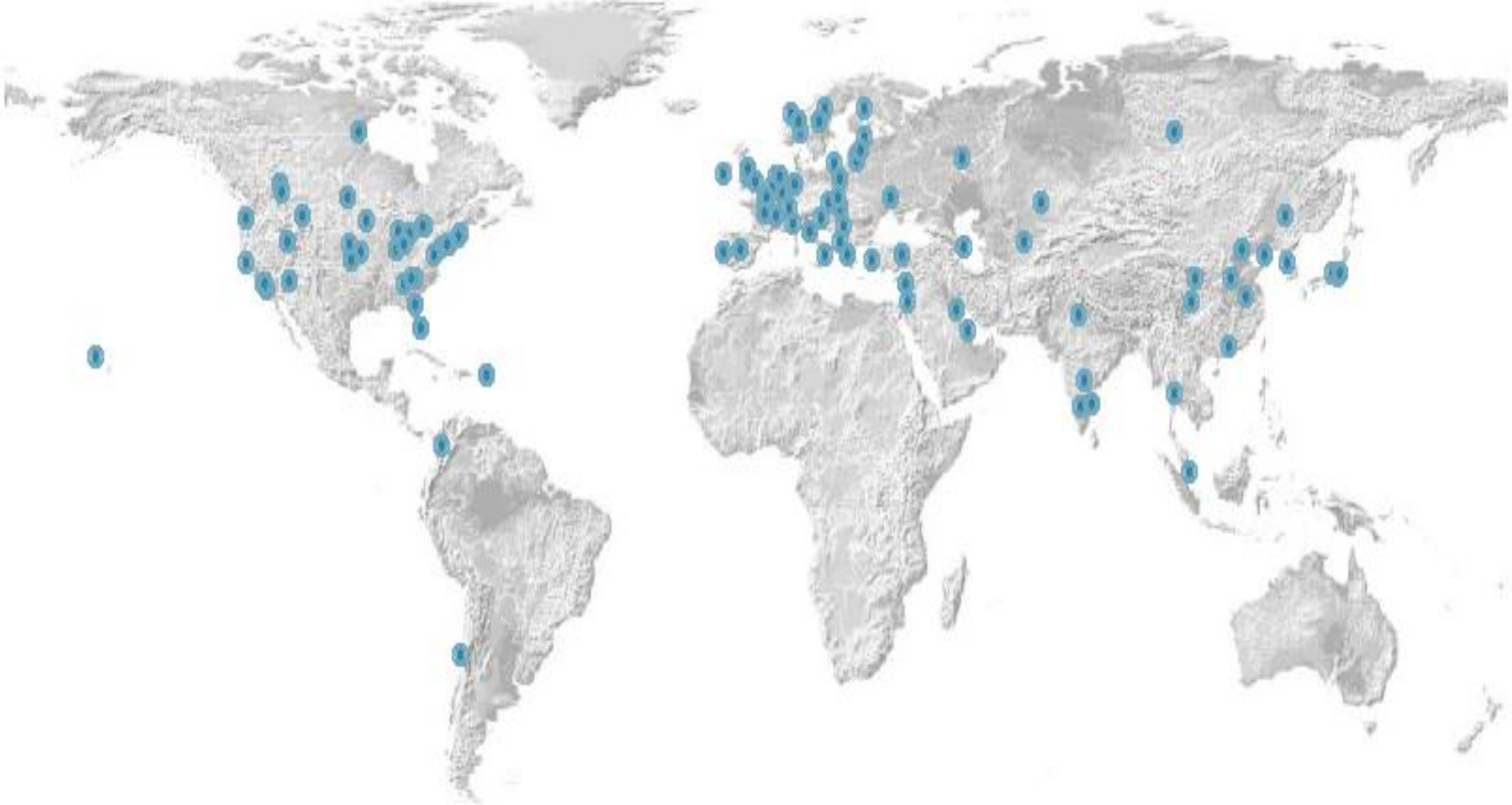
Arbor Atlas: Attack Sources



Arbor Atlas: Phishing Websites



Arbor Atlas: Botnet IRC Servers



IRT-CYBERNET-PK

- APNIC implemented mandatory IRT references on 8 November 2010
- In response to that Cybernet formed a specialized team with capability and authority to handle any sort of network abuse.
- noc-abuse@cyber.net.pk
- We receive approx 100 reports per month

IRT-CYBERNET-PK

- 70% complaints are of Email Spamming
- 20% complaints are of network scanning or IRC Botnets.
- 5% complaints are of Phishing
- 5% are miscellaneous complaints that include Copyright Infringements and SPAM.

IRT-CYBERNET-PK

- Our Response
  - We cater 95% of the reports and act as per the designed processes.
  - Suggest to implement RIPE-409 to downstream customers to minimize spam generating from the network.
  - Update end users via email with possible remedy.
  - Frequently update the Frequent Abuser List which may leads to service suspension.

Reporting Abuse

- We report approx 100 network abuse per month which crosses our threshold.
- Not productive to report spam generating from hotmail, yahoo and esp google.
- We only report to SPs and Enterprises.
- Issues in AP Region:
  - No response from email addresses mentioned as abuse contact.
  - Email box full or doesn't exist messages.
  - No abuse email box exist.
  - Usually no issues while reporting within Pakistan as we know people who can fix the issue.

Bottom Line

- Find the people who can fix it.
- IRT object holds the key, but people behind it knows how to open the lock.
- APNIC should keep a check if IRT objects are updated and working.
- NO this is not operational stuff for RIR, its like keep a clean and working resource database.

APNIC – About Us

- APNIC (Asia Pacific Network Information Centre) is an open, membership-based, not-for-profit organization. It is one of five Regional Internet Registries (RIRs) charged with ensuring the fair distribution **and responsible management of IP addresses** and related resources. These resources are required for the stable and reliable operation of the global Internet.
- Source : http://www.apnic.net/about-APNIC/organization

Thankyou

and

I hope you have an updated and working IRT Object?