

# M<sup>3</sup>AAWG @ APNIC Cooperation SIG: Anti-Abuse Community Development

Jesse Sowell, PhD

Special Advisor to M<sup>3</sup>AAWG; Vice-Chair of Growth and Develop Directing Outreach  
NANOG Program Committee  
Cybersecurity Fellow at Stanford Center for International Security and Cooperation

APNIC 44  
Taichung, Taiwan  
12 September 2017

# Introduction

# Anti-Abuse and Attribution

## Prescriptive Ethos

“all information exchanges on the Internet *should be consensual*, and unless you choose to receive [traffic] from a third party, you should not *have to accept it*”<sup>1</sup>

Just because there is a *legitimate route* to a destination doesn't mean all traffic *using that route* is legitimate

Provides a ***prescriptive ethos***, but doesn't help with ***practical application***



<sup>1</sup> Adapted from an early definition by MAPS

# Anti-Abuse and Attribution

## Prescriptive Ethos

“abuse is what customers complain about”<sup>2</sup>

“all information exchanges on the Internet *should be consensual*, and unless you choose to receive [traffic] from a third party, you should not *have to accept it*”<sup>1</sup>

Just because there is a *legitimate route* to a destination doesn't mean all traffic *using that route* is legitimate

Provides a *prescriptive ethos*, but doesn't help with *practical application*



<sup>1</sup> Adapted from an early definition by MAPS

<sup>2</sup> Definition offered by Dave Crocker

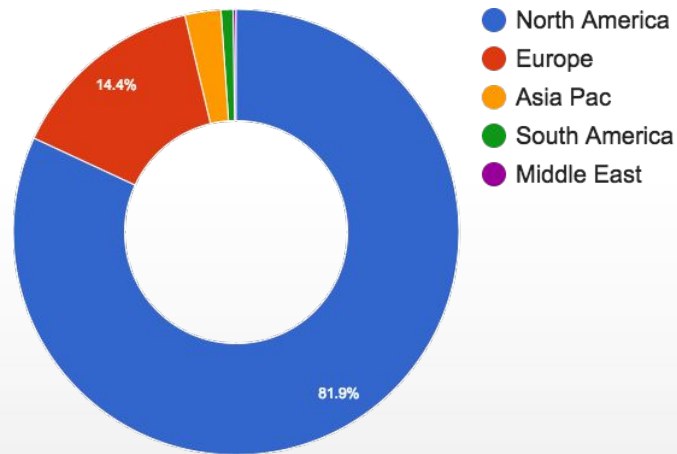
# M<sup>3</sup>AAWG and Anti-Abuse Overview

# Who is M<sup>3</sup>AAWG?

## Constituencies and Demographics

“The Messaging, Malware and Mobile Anti-Abuse Working Group (M<sup>3</sup>AAWG) is where the industry comes together to work against botnets, malware, spam, viruses, DoS attacks and other online exploitation”

- 200 member orgs “worldwide”
- 300-400 conference participants
- technology-neutral, *non-political* working body focusing on operational issues of Internet abuse
  - Supporting technologies
  - Industry collaboration
  - Informing Public Policy

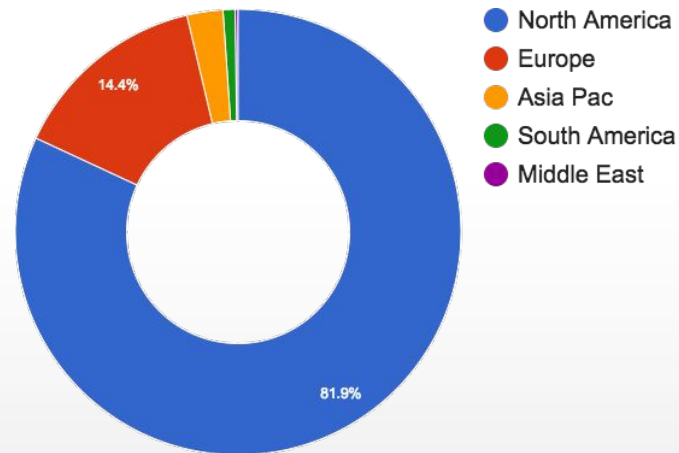


# Who is M<sup>3</sup>AAWG?

## We Need AP Contributions

“The Messaging, Malware and Mobile Anti-Abuse Working Group (M<sup>3</sup>AAWG) is where the industry comes together to work against botnets, malware, spam, viruses, DoS attacks and other online exploitation”

- 200 member orgs “worldwide”
- 300-400 conference participants
- technology-neutral, *non-political* working body focusing on operational issues of Internet abuse
  - Supporting technologies
  - Industry collaboration
  - Informing Public Policy



Too many US voices

# Who is M<sup>3</sup>AAWG?

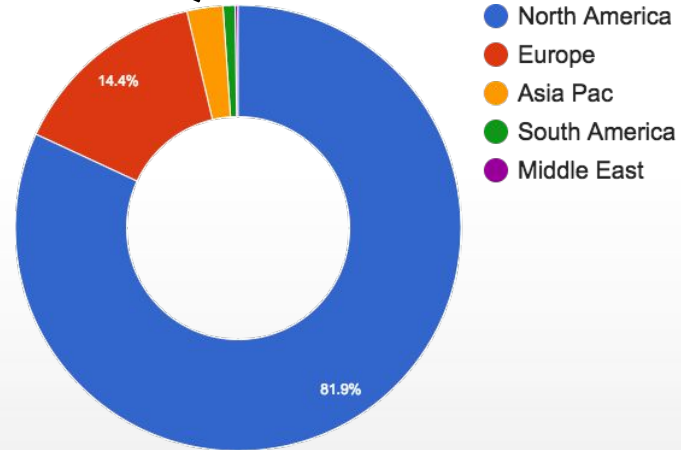
## We Need AP Contributions



“The Messaging, Malware and Mobile Anti-Abuse Working Group (M<sup>3</sup>AAWG) is where the industry comes together to work against botnets, malware, spam, viruses, DoS attacks and other online exploitation”

- 200 member orgs “worldwide”
- 300-400 conference participants
- technology-neutral, *non-political* working body focusing on operational issues of Internet abuse
  - Supporting technologies
  - Industry collaboration
  - Informing Public Policy

Not enough global voices,  
not enough **AP voices!**



Too many US voices



# What Does M<sup>3</sup>AAWG Do? Distill Industry Knowledge into BCPs



## The “M” cubed:

- **Messaging:** abuse on any messaging platform, from e-mail to SMS texting
- **Malware:** abuse is often just a symptom and vector for viruses and malicious code
- **Mobile:** addressing messaging and malware issues emerging on mobile as an increasingly ubiquitous platform

## Develop and Publish:

- Best practice papers
- Position statements
- Training and educational videos

## Public Policy and Industry Guidelines

<https://www.m3aawg.org/for-the-industry/published-comments>

## The Anti-Bot Code of Conduct for Internet Service Providers

<https://www.m3aawg.org/abcs-for-ISP-code>

# What Does M<sup>3</sup>AAWG Do?

## Distill Industry Knowledge into BCPs

### Latest BCPs

- [M<sup>3</sup>AAWG Best Practices for Implementing DKIM to Avoid Key Length Vulnerability](#)
- [M<sup>3</sup>AAWG Best Practices Introduction to Reflective DDOS Attacks](#)
- [M<sup>3</sup>AAWG Initial Best Practices: Arming Businesses Against DDOS Attacks](#)
- [M<sup>3</sup>AAWG Best Current Practices For Building and Operating a Spamtrap, Ver. 1.2.0](#)
- [Using Generic Top Level Domain Registration Information \(WHOIS Data\) in Anti-Abuse Operations](#)
- [M<sup>3</sup>AAWG Introduction to Traffic Analysis](#)



**M<sup>3</sup>AAWG**  
MESSAGING MALWARE MOBILE

**M<sup>3</sup>AAWG Best Practices for Implementing DKIM To Avoid Key Length Vulnerability**  
October 2012, December 2013  
Revised: July 2017  
URL to Reference this Document: [www.m3awg.org/Implement-DKIM-BP](http://www.m3awg.org/Implement-DKIM-BP)

The Message arrives thru IP short DKIM

The recipient

1) K  
2) R  
3) E  
4) H

**M<sup>3</sup>AAWG** MESSAGING MALWARE MOBILE  
Anti-Abuse Working Group

**Messaging, Malware and Mobile Anti-Abuse Working Group**  
**M<sup>3</sup>AAWG Initial Recommendations: Arming Businesses Against DDOS Attacks**  
March 2017  
The reference URL for this document: [www.m3awg.org/DDoS-Recommendations-Business](http://www.m3awg.org/DDoS-Recommendations-Business)

**Table of Contents**  
Introduction ..... 1

**M<sup>3</sup>AAWG** MESSAGING MALWARE MOBILE  
Anti-Abuse Working Group

**Messaging, Malware and Mobile Anti-Abuse Working Group**  
**M<sup>3</sup>AAWG Introduction to Reflective DDOS Attacks**  
May 2017  
The reference URL for this document: [www.m3awg.org/Reflective-DDoS-Introduction](http://www.m3awg.org/Reflective-DDoS-Introduction)

**Introduction**  
Disrupted Denial of Service (DDoS) attacks are a critical concern for many businesses today. Many thousands of individual DDoS attacks take place each day, and though most are relatively small (5-10 gbps per second), they are still more than sufficient to take important sites offline. Moreover, attacks of even relatively modest means can create attacks in the hundreds of gigabits per second range. These attacks concentrate over large regions of the internet. It is everyone's interest to take all possible precautions to limit these damaging attacks.

There are several types of DDoS attacks. This document includes just one: the **reflective amplification attack**. This paper is not a best practice document as such, its main purpose is to provide an overview of how this very common form of attack works and what measures can be taken to help eliminate it. It also provides pointers to some of the many related documents that can provide the detail this overview leaves out.

**Reflective Amplification Defined**  
A reflective amplification attack can be compared to a hijacked conference call. The first person, Alice, purposefully misidentifies herself as her intended victim, Vera. Also directs a short question to a second person, Bob, that requires a long answer, such as a list of relatives' names and addresses. Bob responds to Vera (who did not ask the question) with a very long answer. Alice's short message has been amplified and the reply is being relayed to Vera. Repeated many times, with Alice impersonating multiple people (Charlie, Deborah, Edna, and so on), these communications will completely swamp Vera with large amounts of unwanted noise.

In the case of a DDoS attack, the message is amplified when compromised devices send a short message to a system that responds with a much larger payload in the answer. It is often because the IP address of these requests are forged so that all the responses are sent to a targeted victim rather than the originating device.

**M<sup>3</sup>AAWG**  
Messaging, Malware and Mobile Anti-Abuse Working Group  
781 Beach Street, Suite 302 • San Francisco, California 94109 U.S.A. • [www.m3awg.org](http://www.m3awg.org)

**M<sup>3</sup>AAWG**  
MESSAGING MALWARE MOBILE

**Messaging, Malware and Mobile Anti-Abuse Working Group**  
**M<sup>3</sup>AAWG Best Current Practices For Building and Operating a Spamtrap**  
Version 1.2.0  
Updated August 2016

**Table of Contents**

**M<sup>3</sup>AAWG** MESSAGING MALWARE MOBILE  
Anti-Abuse Working Group

**Messaging, Malware and Mobile Anti-Abuse Working Group**  
**Using Generic Top Level Domain Registration Information (WHOIS Data) in Anti-Abuse Operations**  
July 2016

**Introduction**  
The purpose of this document is to provide an overview of how this very common form of attack works and what measures can be taken to help eliminate it. It also provides pointers to some of the many related documents that can provide the detail this overview leaves out.

**Reflective Amplification Defined**  
A reflective amplification attack can be compared to a hijacked conference call. The first person, Alice, purposefully misidentifies herself as her intended victim, Vera. Also directs a short question to a second person, Bob, that requires a long answer, such as a list of relatives' names and addresses. Bob responds to Vera (who did not ask the question) with a very long answer. Alice's short message has been amplified and the reply is being relayed to Vera. Repeated many times, with Alice impersonating multiple people (Charlie, Deborah, Edna, and so on), these communications will completely swamp Vera with large amounts of unwanted noise.

In the case of a DDoS attack, the message is amplified when compromised devices send a short message to a system that responds with a much larger payload in the answer. It is often because the IP address of these requests are forged so that all the responses are sent to a targeted victim rather than the originating device.

**M<sup>3</sup>AAWG** MESSAGING MALWARE MOBILE  
Anti-Abuse Working Group

**Messaging, Malware and Mobile Anti-Abuse Working Group**  
**M<sup>3</sup>AAWG Introduction to Traffic Analysis**  
June 2016

**Introduction**  
Postering against pervasive monitoring and the use of encryption continues to be a major focus for the messaging industry. M<sup>3</sup>AAWG has already published initial recommendations for deploying TLS mitigating Man-in-the-Middle attacks, and using forward secrecy to secure data, to help the messaging community understand how to better secure email in transit. Now M<sup>3</sup>AAWG would like to bring awareness to a different type of risk - a form of attack called traffic analysis. In this paper, we outline the key characteristics of traffic analysis, discuss potential ways to avoid it, and consider the advantages and disadvantages of deploying preventive measures.

**Understanding Traffic Analysis with Respect to Messaging and Network Traffic**  
The content of messages encrypted with PGP/GPG, GSN, PGPsec, GnuPG, or S/MIME is generally highly resistant to eavesdropping. Even if a third party manages to get a copy of a PGP/GPG encrypted email (or an S/MIME encrypted email), they are not likely to be able to decrypt and read it. However, even messages that are perfectly protected with end-to-end encryption remain potentially subject to traffic analysis attacks.

To understand the difference, consider the following summary table of email message elements visible to an intermediary SMTP server utilizing TLS for transmitting messages and their availability for traffic analysis purposes:

Email message elements	Vulnerable to traffic analysis?
Return-path header	Yes
Return headers	Yes
From header	Yes
To header	Yes
CC header	Yes
Date header	Yes
Subject header	Yes
Mailing-List header	Yes
Any/all other headers	Yes
Body of the message	Yes
Line message was received	Yes
Apparent encryption used by message	Yes
Message content (passworded to be possibly or actually encrypted)	No

In a traffic analysis attack, the focus is not on the content, but on the message headers and other externally-observable artifacts associated with the message or the communication process itself. The summary table

**M<sup>3</sup>AAWG**  
Messaging, Malware and Mobile Anti-Abuse Working Group  
P.O. Box 19027 • San Francisco, CA 94119-0020 • [www.m3awg.org](http://www.m3awg.org)

# What Does M<sup>3</sup>AAWG Do?

## Who Do We Work With?

Unsolicited Commercial Enforcement Net

- Operation Safety Net

Internet Society

- Provided training material

i<sup>2</sup>Coalition

- Hosting BCP

EastWest Institute

- 2013 Cyber Security Award for China & India Work

Anti-Phishing Working Group (APWG)

- Anti-Phishing Best Practices for ISPs and Mailbox Providers

**LAC-AAWG**

- Updating and developing BCPs to reflect LAC dynamics

**AF-AAWG**

- In progress with AfricaCERT



# What Does M<sup>3</sup>AAWG Do? Who Do We Work With?

Unsolicited Commercial Enforcement Net

- Operation Safety Net

Internet Society

- Provided training material

i<sup>2</sup>Coalition

- Hosting BCP

EastWest Institute

- 2013 Cyber Security Award for China & India Work

Anti-Phishing Working Group (APWG)

- Anti-Phishing Best Practices for ISPs and Mailbox Providers

LAC-AAWG

- Updating and developing BCPs to reflect LAC dynamics

AF-AAWG

- In progress with AfricaCERT

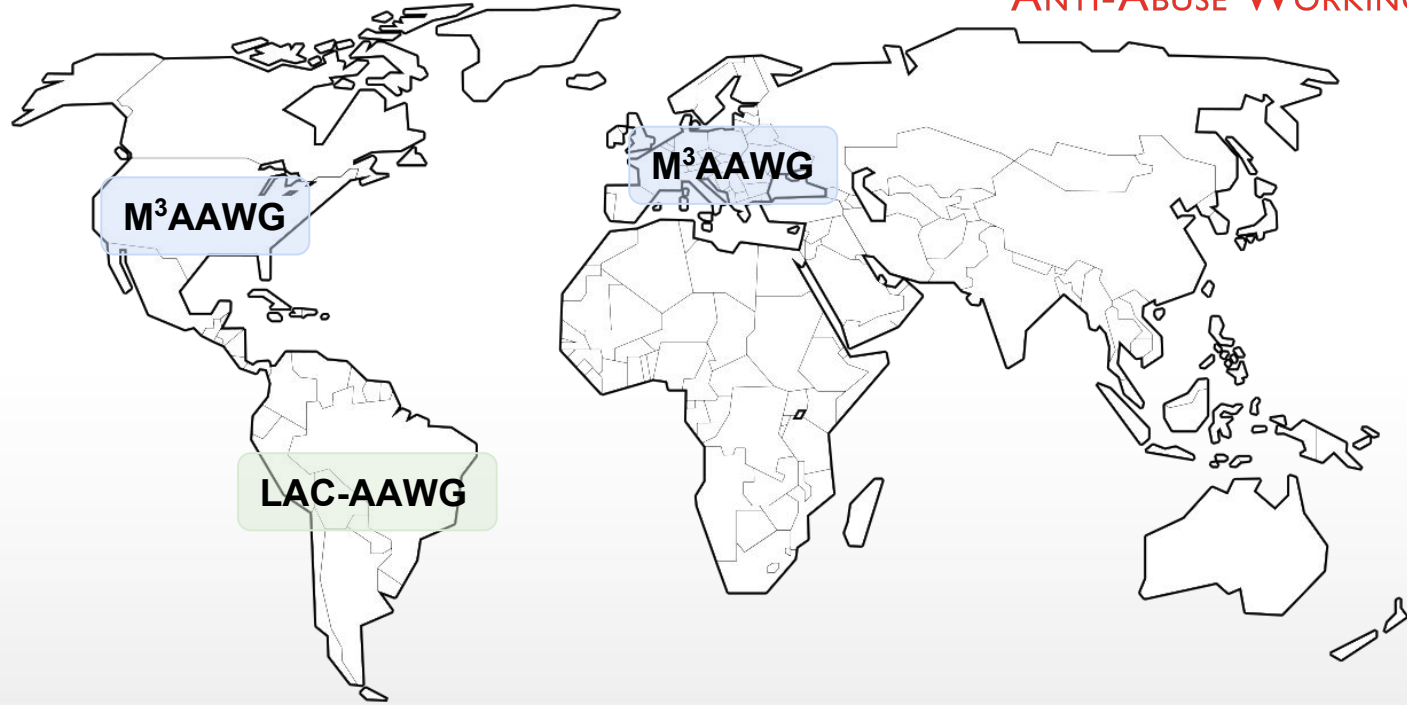


# Outreach: Anti-Abuse Working Group (AAWG) Development

# Regional AAWG Development Contributing to *Peer Working Groups*



# Regional AAWGs Development Contributing to *Peer Working Groups*



# Regional AAWGs Development Peer Working Group in LAC



## Comunicado de prensa Para publicación inmediata

### LACNIC y la comunidad latinoamericana de seguridad operacional se unen a M<sup>3</sup>AAWG para combatir las amenazas en línea

*San Francisco, 31 de marzo de 2016* – LACNIC, el Registro Regional de Internet para América Latina y el Caribe, se ha unido al Grupo de Trabajo Antiabuso de Mensajes, Malware y Móvil para colaborar en temas globales de ciberseguridad. LACNIC es también el foro que convoca al Grupo de Operadores de Red de LAC; LACSEC, el Foro de Seguridad de Redes de la región; y LAC-CSIRT, un foro regional de respuesta a incidentes de seguridad. Como parte de una asociación mutua para luchar contra las amenazas en línea, M<sup>3</sup>AAWG también se ha unido a LACNIC para interactuar con estos proveedores de servicios y comunidades de seguridad en línea.

[Esta interacción continua](#) permitirá que el M<sup>3</sup>AAWG tenga acceso a expertos regionales en tendencias operacionales y antiabuso y les dará la oportunidad de desarrollar soluciones conjuntas relevantes que aborden las tendencias actuales en el área de la ciberseguridad y la ciberdelincuencia. LACNIC, el Registro de Direcciones de Internet para América Latina y el Caribe, tendrá acceso a la variada experiencia de los miembros del M<sup>3</sup>AAWG y su permanente trabajo en el



# Regional AAWGs Development

## Peer Working Group in LAC



## LACNOG Anti-Abuse Working Group

### Introduction:

In March of 2016 LACNIC and M<sup>3</sup>AAWG established a memorandum of understanding (MOU) to collaboratively combat “global cybersecurity issues” and “online threats” (reference). As part of this MOU, M<sup>3</sup>AAWG established its LAC Initiative to help develop a self-sustaining anti-abuse community in the LAC region. Strategically, this effort balances M<sup>3</sup>AAWG’s historical expertise in anti-abuse efforts in North America and Europe with the nuanced difference in abuse dynamics in the LAC region. As part of this effort, M<sup>3</sup>AAWG is collaborating with LACNIC and LACNOG to develop the LACNOG Anti-Abuse Working Group, or LAC-AAWG.

### LAC-AAWG Charter

LAC-AAWG will serve as a convening forum for operators in the LAC region that want to develop anti-abuse recommendations and best common practices (BCP) and global members

# Regional AAWGs Development

## Peer Working Group in LAC



## AAWG Principles and Objectives

Promulgate anti-abuse norms and principles  
Further develop regional anti-abuse expertise

- Anti-abuse research
- BCPs within and across regions

Convene anti-abuse actors

- operators
- public policy
- LE

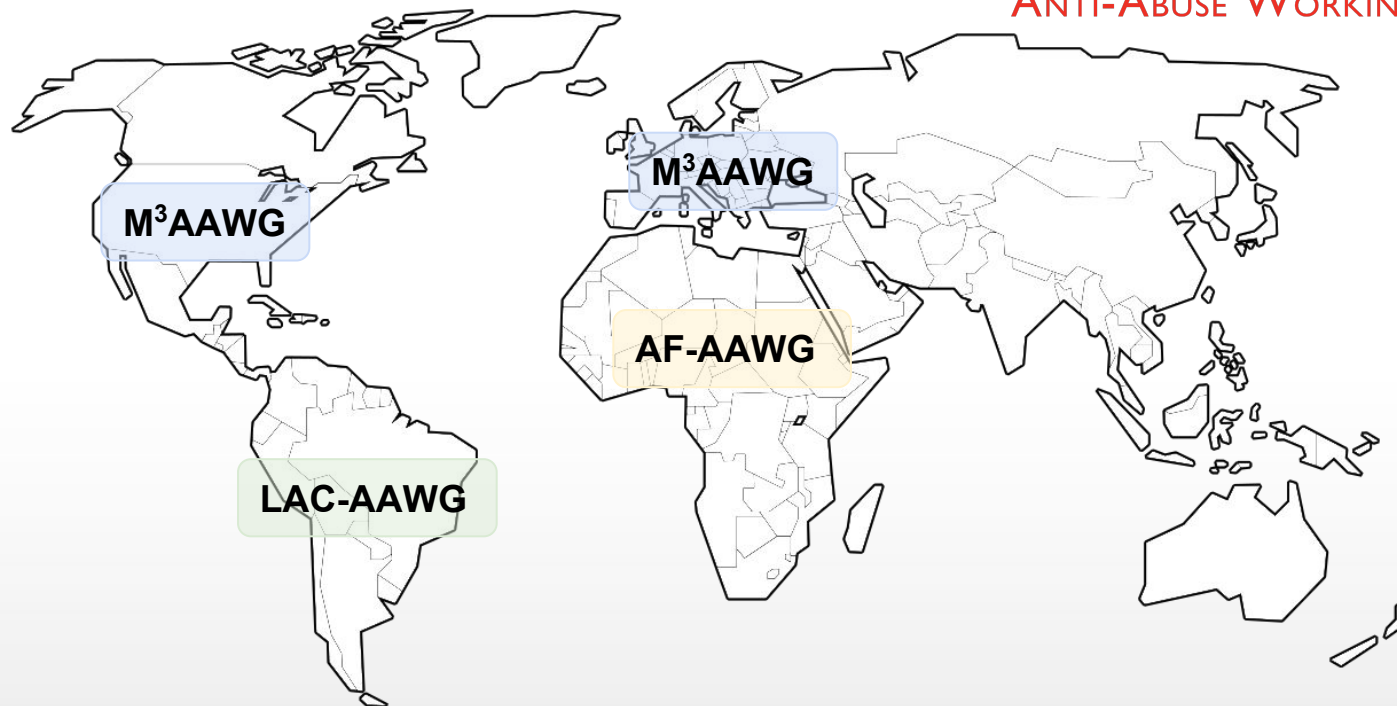
Represent regional anti-abuse expertise

Exchange expertise

- among operators within the regions
- globally, among peer regions

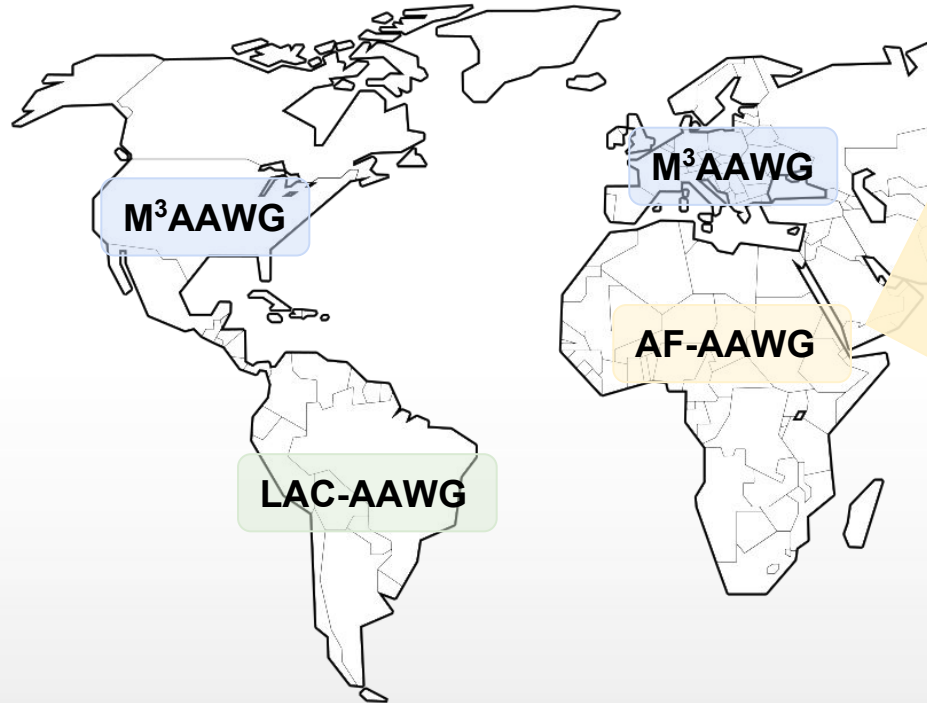
# Regional AAWGs Development

## Peer Working Group in AF



# Regional AAWGs Development

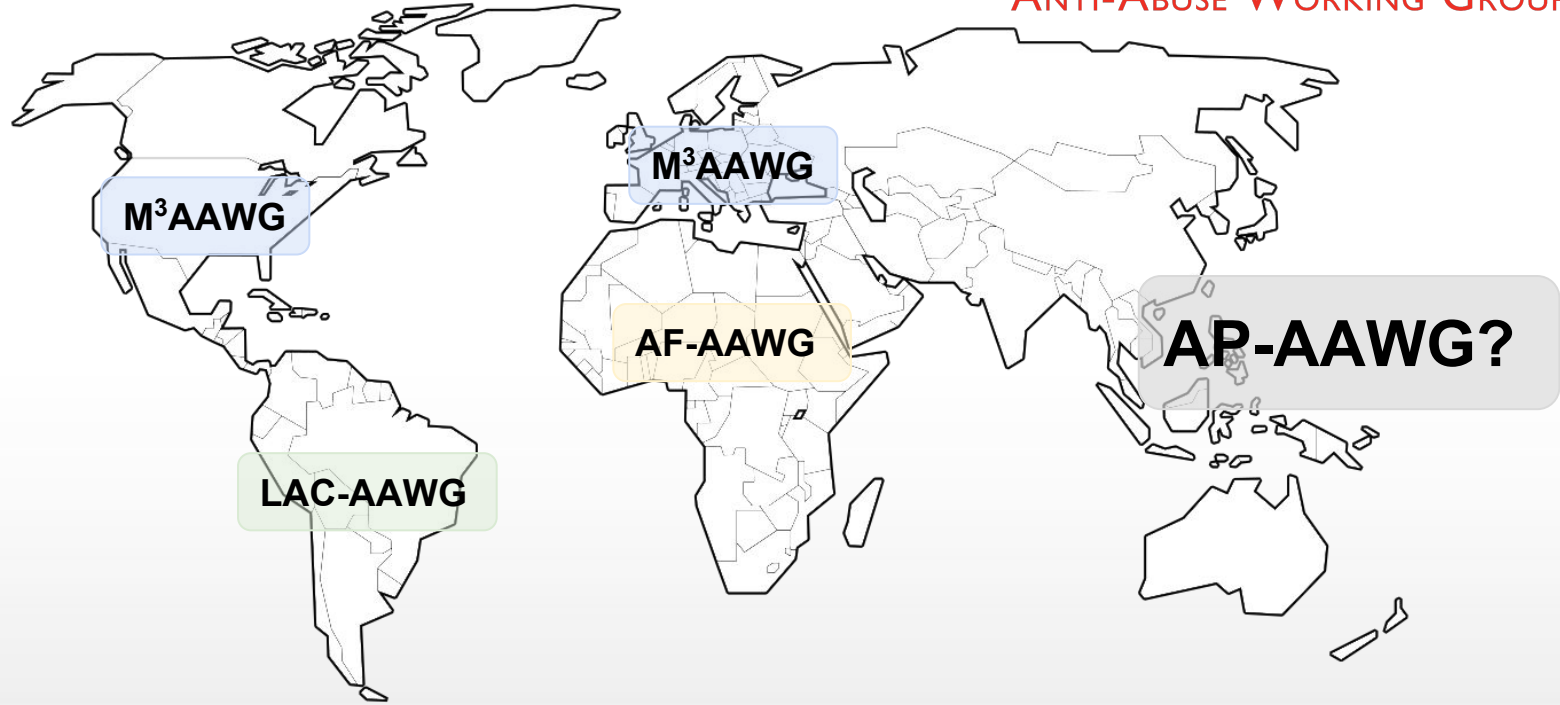
## Peer Working Group in AF



### Progress

- AF-AAWG charter drafted
- AfricaCERT is the home
- Jean-Robert Hountomy is driving engagement
- Partnering with a variety of organizations including
  - ◆ AfriNIC
  - ◆ AFIX
  - ◆ ISOC
  - ◆ Cybergreen
  - ◆ ICANN
  - ◆ ....

# Regional AAWGs Development *Peer Working Group in AP?*



**Questions?  
Comments?  
Volunteers?!??**

**[jesse.sowell@gmail.com](mailto:jesse.sowell@gmail.com)**