

## IGF Workshop report

Session title: WS6:

Can Law enforcement catch bad actors online anymore ?

Proposal details: [https://www.intgovforum.org/cms/igf2016/index.php/proposal/view\\_public/6](https://www.intgovforum.org/cms/igf2016/index.php/proposal/view_public/6)

**Date:** December 8th, 2016 (Day 3)

**Time :** 10:15 - 12:00

**Location:** Workshop room #4

Session Organizers:

- Robert Guerra, SSAC, ICANN
- Jeff Bedser, SSAC / ICANN, Private Sector, iThreat Cyber Group

Chairperson/Moderator:

- Robert Guerra, SSAC / ICANN, Technical Community

List of Speakers and their institutional affiliations:

3. Jeffrey R. Bedser

Jeffrey R. Bedser is the founder and CEO of iThreat Cyber Group [www.ithreat.com](http://www.ithreat.com). Jeff presented an overview of the current challenges being faced by cyber investigators as IPv4 addresses are exhausted and the transition to a wider deployment of IPv6 takes place. As well Jeff presented several case studies for the speakers and audience to discuss.

4. Ben Butler

Ben Butler is the Director of the Digital Crimes Unit at GoDaddy. Ben brought a registrar and hosting company perspective to the conversation and dialogue.

5. John Curran

John Curran is the current President and Chief Executive Officer of the American Registry for Internet Numbers (ARIN), the Regional Internet Registry (RIR). John gave a 10 minute overview of the history of IPv4, IPv6 and implications for law enforcement agencies in investigating online crimes. As well, John also brought a North American Regional Internet Registry perspective to the conversation.

6. Laura DeNardis

Laura DeNardis is a tenured Professor and Associate Dean in the School of Communication at American University. She was unable to attend the session, however did share questions and topics for the panelists to consider and discuss.

7. Athina Fragkouli

Athina Fragkouli is the Legal Counsel at the RIPE Network Coordination Centre (NCC). Athina shared her views on the policy issues that she and her team at RIPE deal with. She stressed that her organization co-operates with law enforcement, however there is no legal mandate to share non-public information unless there is an appropriate duly authorized judicial order from the Netherlands.

8. Merike Kaeo

Merike Kaeo is the CTO at Farsight Security. Merike collaborated with and developed the workshop proposal together with Ben Butler, Jeff Bedser and Robert Guerra. She was unable to attend the session; however she did share questions and issues for the panel and audience to discuss.

9. Iranga Kahangama

Iranga Kahangama is a Policy Advisor for the Federal Bureau of Investigation. Iranga brought a US and international law enforcement perspective to the conversation and dialogue. He spoke to the many challenges that exist for governments, especially at the local and state level to adopt to new technologies such as IPv6.

10. Dick Leaning

Dick Leaning is an external relations consultant at RIPE NCC. Dick brought an Internet Registry, Law Enforcement and International Cyber Investigation perspective to the conversation and dialogue.

11. Carlos M. Martinez

Carlos Martinez-Cagnazzo is the Chief Technical Officer of LACNIC, the Latin American and Caribbean Internet Address Registry. Carlos brought a Latin American, Internet Registry, and developing country perspective to the conversation and dialogue.

Key Issues raised:

- IPv4 depletion is a reality and IPv6 adoption is substantially rising every year.
- It is important for RIRs to work closely with LEAs and international justice organizations such as INTERPOL.
- Well trained Law Enforcement that has a technical understanding of domain names, IP address allocation and CGNs will get far better results when they engage with ISPs, content hosts and domain name registrars.
- Robust logging and data retention makes investigations by LEA's easier, however there are big data and privacy issues that need to be resolved.

- Investigations are helped by having highly trained technical experts that know how to access public (whois) databases and have access to commercial investigation products and services.
- Information kept by the RIR's about IP address blocks may not always be accurate, which in turn is making it more challenging for LEAs to perform their investigations.
- Governments can be slow to improve investigative methods to adopt to new technologies such as IPv6 and the Internet of Things.
- Scalability does not matter as long as we can keep up with who has what resource.
- The challenges to adopt to a IPv6 environment is possible as long as there is a sharing of best practices and sharing of information at fora such as the IETF, ICANN, the ITU and the Internet Governance Forum.
- A decision will need to be made on what the future Internet looks like, will it be fully anonymous or be a mediated reality where no privacy exists at all.

### Summary of presentations made during the session:

John Curran started the conversation by giving a presentation and overview of IPv4 depletion and presenting the challenges being faced by law enforcement.

### Description of the discussion that took place during the workshop session:

The workshop was organized as a facilitated dialogue. Led by the moderator, subject experts debated and discuss the key questions and issues.

John Curran started the conversation by giving a presentation and overview of IPv4 depletion and presenting the challenges being faced by law enforcement. After the presentation, the expert panelists give short 2-3 min opening comments where they shared their role in their organization and how they are involved in cyber investigations.

After the round of introductions, the moderator turned to those attending the session for questions and facilitated a discussion and dialogue with the panelist.

Jeff Bedser then presented several case studies and scenarios to provide a historical context on the complexities involved in cyber investigations in the 1990s, 2000's, and current day. The case studies painted an evolution in the complexity of investigation and many challenges that are being faced by IPv6 adoption.

After the case studies were presented, a second round of facilitated discussion took place between the issue experts and the audience.

### Potential next steps / takeaways:

- Feedback and comments will be feed into ICANN Security and Stability (SSAC) so that it gets incorporated into existing and future board advisories.
- Several attendees proposed that it would be valuable to have a similar session at upcoming ICANN meeting in Copenhagen (March 2017), and at national level IGF in USA & Europe.

- Civil society participants expressed an interest to learn more about open source cyber investigation techniques for journalism. Specifically, investigative journalists expressed an interest to participating in training workshops in Latin America.
- Incorrect information is making it more challenging for LEAs to perform their investigations, as such need to have policy dialogue at ICANN, RIRs and related to accuracy of Information kept by the RIR's about IP address blocks.
- Ongoing training and education efforts in regards to IP addresses need to be organized by RIRs for law enforcement agencies and cyber investigators.
- Policies, investigative techniques and are needed to keep Governments and investigators a step ahead of the bad actors online that are committing crimes.
- Adam Peake (ICANN staff) proposed idea of including SSAC members in civil society outreach efforts being planned for Copenhagen (ICANN 58) and Johannesburg (ICANN 59).

### Gender reporting information:

- 1 Estimate of # of participants present at session: - Room was full – Estimated # 150
- 2 Estimate # of women present at the session:
  - Speakers: 1/3 female, 2/3 male
  - Participants: 40%
  - Remote speakers: 50%
- 3 To what extent did the session discuss gender equality and/or women's empowerment:
  - The session did not discuss the issue of gender quality or women's empowerment
  - The related issue of online cyber stalking and online harassment was discussed as a case study.