Thank you for the opportunity to give you some additional comments on the Draft report. I've addressed this email to the counter_botnet email that you mentioned below.

Here are some of our thoughts and findings on this subject -

Possible addition of a paragraph/section about "Aggressive SIP based global Voice BotNet attacks on US voice critical infrastructure":

We would like to add that we're seeing SIP based global BotNets specifically targeting the Voice portions of the carrier's networks. As legacy and large carriers who make up the foundation of the US voice infrastructure migrate their networks from traditional TDM and SS7 networks to a more IP centric SIP and RTP based networks, they are more prone to attacks from external actors whose aim is to cause harm to the United States.

Also as voice traffic has been evolving from traditional legacy networks to smartphones, soft clients, Click to call applications, OTT based voice communications (Facebook/Google etc) to voice enabled OTT devices, the attack surface for a hacker has grown exponentially.

With every network moving towards commonly used protocols like SIP and WebRTC - the bad actors have created "standard tools" that can now target all these networks.

As you know our company, RedShift Networks, has been in the forefront of VOIP cyber Security in the last few years and we have collected a rich data set that includes information of how these attackers are trying to penetrate the Tier 1 Carrier (and other) infrastructure. At the edge of these SIP based networks are public facing Session Border Controllers (SBCs). Based on global SIP scans conducted by these hackers (mafias and state sponsored bad actors), they have a clear understanding of the edge (IP addresses) of most major and minor carriers in the US. Unfortunately the US carriers are responding to these scans that typically come from well known Hosting Cloud Servers located in the US or Western Europe. Typically these bad actors are hijacking these servers or even legitimately 'renting' the servers to intimate their SIP BotNet attacks. As the US carrier responds to these SIP Scans, the attackers starts to probe the weaknesses of the edge of these SIP based networks (SBCs).

The major of the attacks are financially and fraud related as we've seen that they send SIP messages and try to Register into the network using legitimate credentials and fool the network to allow them to make calls all over the world. This according to the CFCA (Communications Fraud Control Association) is a $29B problem for carriers globally.

They are also aggressively sending Robocalls, Telephony DOS, SIP malformed packets, and a myriad of other SIP based attack vectors against traditional US based carriers. We can detect up to 40,000 different SIP attack vectors. They are also exploiting end point based security SIP vulnerabilities. We have also collected information on these SIP based attack tools.

Our customer base includes Tier 1, Tier 2 and Tier 3 carriers in the US both fixed line, cable, Mobile, VOIP/UC and other OTT carriers - 30+ carriers and we have our products installed in another 10 carriers around the world.

We’ve seen this behavior across all of these networks and the attacks are coordinated in nature.

We would love to share some of our findings with the FCC and we would encourage an open discussion with US carriers to elevate the importance of future securing their networks from this new attack vector via SIP and on voice based products/technology.

Hope this information is helpful and appreciate an opportunity to tell you a little more about this problem set. It would be great if this new vector of attack (SIP Botnets) can be included into the report to the president.

Thank you and many regards,

Amitava
[Phone number redacted—NTIA]

CEO & Co-Founder
RedShift Networks