August 4, 2014

The Honorable Patrick J. Leahy
Chairman
United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Mr. Chairman:

Thank you again for inviting me to testify at the Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism hearing entitled "Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks" on July 15, 2014, and also for your letter of July 23 requesting additional written testimony. My answers (also representing the M^3AAWG position) to your written questions are as follows:

1. "As we discussed, the Subcommittee is exploring possible legislation to address the botnet threat. What specific proposals would you recommend we include in such legislation?"

First, I have a concern regarding the standards for *ex parte* injunctive relief when used as a tool for botnet takedowns. F.R.C.P. § 65(b)(1)(A) assumes that the court will be able to judge the clarity of the movant's claim of irreparable injury, loss, or damage. The Internet is a complex system, with an exquisite interdependence among its component parts, and the full framing of the issues at stake in a takedown provided by opposing technical experts will not (by definition) be explored at an *ex parte* proceeding. Effectively, the court currently has to take the movant's word for the clarity of their claims. I argue that a stronger standard is needed, noting that injunctive relief in support of a botnet takedown can have a wide-ranging impact on innocent third parties whose identities and Internet interdependencies literally cannot be foreseen by a movant.

Second, I note that in all botnet takedowns, private information belonging to affected parties, including botnet victims as well as third parties who are users of shared Internet components impacted by the takedown, may be placed into the hands of takedown operators. In any instance where a statutory duty or a specific contractual relationship such as employer-employee or provider-customer does not govern the handling of such information, the Subcommittee should ensure that a legal framework governing botnet takedowns appropriately balances the need to facilitate effective and expedient mitigation and remediation measures with the need to protect botnet victims and affected third parties against disclosure, retention, or use of such information.

2. "Do you have any comments on the legislative proposals that Assistant Attorney General Caldwell discussed in her testimony?"

Assistant Attorney General Caldwell's described amendments to the Computer Fraud and Abuse Act (CFAA) that would cover trafficking in access to botnets and would loosen the specification of a botmaster's intent; these are both well researched and they are borne out by my own recent experiences in the Internet security industry. Similarly, A.A.G. Caldwell's proposal to criminalize the overseas sale of stolen U.S. financial information will close a gaping loophole and help the letter of the law meet with its clear intent.

With regard to A.A.G. Caldwell's description of the DOJ's request for enhanced resources to combat botnets and other cyber threats, I am reminded of Attorney General Robert F. Kennedy's crusade against organized crime five decades ago. The United States is the richest target in the world for both individual and organized cybercrime and all of our lives are as affected by cybercrime today as we were by pre-cyber organized crime in 1960. We must do no less than RFK, and make the fight against this threat a top priority for our nation's law enforcement agencies. I support A.A.G. Caldwell's well-reasoned request for enhanced resources to combat botnets and other cyber threats and I expect that even more resources will be needed in the years ahead.

3. "How do we ensure that our laws give the public and private sectors the tools they need to respond to the botnet threat, while at the same time recognizing that the threat itself – and therefore the most effective responses to it – are constantly evolving?"

There is a bright middle ground where the best tradition of law exists: broad enough to accomplish our intended purposes, yet also narrow enough to resist misapplication, abuse, and overreach. Congress should strive for legislation to support the fight against botnets and cybercrime that first and foremost protects due process and individual rights, since any tradeoff of our nation's fundamental principles for temporary and targeted success against this or any threat would be a bad bargain. Within this envelope, I support the specific initiatives described by A.A.G. Caldwell in her testimony, noting that future wisdom as to cybercrime related legislative priorities is likely to come, as A.A.G. Caldwell's has come, from the women and men "in the trenches."

I would like to repeat my remark made during the July 15 subcommittee hearing: the Internet is borderless; the botnet problem is borderless; and any solution to the botnet problem will also be borderless. I also went on record describing the U.S. DOJ as the envy of the world in its approach to botnet takedowns and its awareness of the technical and social subtleties involved. The international law enforcement outreach and cooperation shown by the FBI and by the NCFTA perfectly demonstrates what I mean by "borderless solutions." We, the people of the United States, can only address this worldwide threat by efficiently and effectively cooperating with our peers around the world and by treating this as the world's problem, not merely a U.S. problem.

Mr. Chairman, thank you again for this opportunity to address your questions. I remain, as before, at your service.

Paul Vixie, CEO
Farsight Security, Inc.
August 4, 2014