CENTER FOR DEMOCRACY & TECHNOLOGY

12 February 2018

National Telecommunications and Information Administration (NTIA)
U.S. Department of Commerce
1401 Constitution Avenue NW., Room 4725,
Washington, DC 20230

Via email: Counter_Botnet@list.commerce.gov

Attn: Evelyn L. Remaley, Deputy Associate Administrator
David J. Redl, Assistant Secretary for Communication and Information

Re: Request for Comment on Promoting Stakeholder Action Against Botnets and Other Automated Threats

Dear Ms. Remaley and Mr. Redl,

The Center for Democracy and Technology (CDT) is a nonprofit advocacy organization that works to promote democratic values by shaping technology policy and architecture, with a focus on the rights of the individual. CDT supports laws, corporate policies, and technological tools that protect privacy and security and enable free speech online. Based in Washington, D.C., and with a presence in Brussels, CDT works inclusively across sectors to find tangible solutions to today's most pressing technology policy challenges.

CDT appreciates this opportunity to comment on the Department of Commerce's draft Report on enhance resilience against botnets and other automated, distributed threats. We have previously provided comments to the NTIA in July on botnets,[1] as well as in response to the Department's "Internet of Things" (IoT) green paper.[2] We additionally participated in the NTIA summer convening and briefed the National Security Telecommunications Advisory Committee.

Generally, we commend the agencies for endorsing a botnet mitigation regime that assigns responsibility to those who have the access and ability to make systemic changes -- device manufacturers and service providers. We also appreciate that the report still calls for educating and empowering end users so that they may make informed decisions. Because there is an explicit tension between allowing companies to take voluntary but automated action against devices and accounts, and permitting consumers to control their digital footprint, we propose that the National Institute of Standards and Technology (NIST) convene a dedicated process for discussing the implications for

[1] Ctr. for Democracy & Tech., Comments to the NTIA on Executive Order 13800 (July 28, 2017), https://cdt.org/insight/request-for-comment-re-strengthening-federal-cybersecurity-and-addressing-botnets/.
[2] Ctr. for Democracy & Tech., Comments to the NTIA on Fostering the Advancement of the Internet of Things (Mar. 10, 2017), https://cdt.org/insight/cdt-comments-to-the-ntia-on-fostering-theadvancement-of-the-internet-of-things/.

privacy and freedom of expression. Ideally and with your convening function, industry and civil society representatives could more fully flesh out best practices for more systematically evaluating privacy and free speech effects of botnet responses.

1. The Ecosystem: Is the Report's characterization of risks and the state of the current internet and communications ecosystem accurate and/or complete? Are there technical details, innovations, policy approaches, or implementation barriers that warrant new or further consideration?

The report is appropriately oriented toward technical solutions and action from IT and information security professionals, but botnet takedowns present an array of ethical concerns.[3] The implications of certain offensive and defensive mitigation strategies under the Fourth Amendment and existing criminal law have received attention,[4] but it is also important to acknowledge that voluntary corporate actions taken against botnets may have adverse effects on users' privacy online, their property interests in the IoT, and users' ability to consume content and express themselves.

As noted in your report, common techniques for botnet mitigation include ingress and egress filtering, re-routing and shaping internet traffic, and isolating devices or other entities.[5] However, automating these actions to respond to an increasing number of compromised devices risks letting certain private actors "decide what fundamentally is and is not allowed on the Internet," which will likely lead to unintentionally "block[ing] traffic that is 'good.'"[6] This calls for a very specific conversation about avoiding these pitfalls and it would benefit from involvement by civil society and the public in crafting appropriate responses.

Your report also acknowledges the broad array of risks involved in botnet mitigation. It points to a number of voluntary codes of conduct that recognize privacy or freedom of expression must be protected in responsible mitigation efforts. For example, the Industry Botnet Group includes protecting privacy as one of its nine principles for voluntary botnet responses,[7] and reports from the Federal Communication Commission note that even the *appearance* of a privacy infringement can deter consumers from taking actions to protect their devices.[8] However, despite the repeated recognition of

---

[3] David Dittrich et al., A Case Study in Ethical Decision Making Regarding Remote Mitigation of Botnets (2010), https://staff.washington.edu/dittrich/papers/wecsr2010-botethics-dlw.pdf.

[4] *See, e.g.*, Gabe Rottman & Ian Williams, *All Bots Must Die: How a New Senate Bill to Combat Botnets Could Put Privacy at Risk*, CDT (Aug. 08, 2016), https://cdt.org/blog/all-bots-must-die-how-a-new-senate-bill-to-combat-botnets-could-put-privacy-at-risk/; *see also* Sam Zeitlin, *Botnet Takedowns and the Fourth Amendment*, 90 N.Y.U. L. Rev. 746 (2015).

[5] Secretary of Commerce and Secretary of Homeland Security, A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats, (DRAFT FOR PUBLIC COMMENT, Jan. 5, 2018) at 10-11.

[6] *Id.* at 20.

[7] Industry Botnet Group, Principles for Voluntary Efforts to Reduce the Impact of Botnets in Cyberspace, https://archive.is/20131015084520/www.industrybotnetgroup.org/principles/ (stating only that participants should address "privacy and security in appropriate manner" and follow existing law, as well as existing practices).

[8] Further, one report notes public understanding about "the magnitude of the problem is critical to sizing up what might be necessary, and metrics also provide programmatic transparency." Communications Security, Reliability and Interoperability

the rights implications of these programs, there has been no intentional and thorough discussion of how these private actors can protect the larger internet ecosystem while minimizing the impact on these rights.

While we do not presume to know the full range of issues or policy considerations that would come from such a discussion, we expect that topics like notice, attribution, and remediation will be relevant as well as instituting processes like privacy impact assessments (PIA).[9] The final product could be a list of best practices, a botnet-specific model PIA, or even a list of considerations that could be used by companies in their botnet takedown practices.

3. Stakeholder Roles: How can specific actions be refined for efficacy and achievability? What actors, inside the Federal government, in the private sector, and across the global community, can be instrumental in the successful accomplishment of these activities? Who should play a leadership role; and where and how? What stakeholders are key to particular successes?

We recommend that the Departments of Commerce and Homeland Security convene and participate in this discussion, as well as the other agencies that consulted on the draft report. We recognize that such a discussion will only be productive with input and buy in from companies with experience in botnet takedowns or those who expect to play an integral role in the future. There appears to be wide recognition that effective cybersecurity relies on public-private partnerships, and companies and governments have become comfortable with the notion of collaborating on botnet takedowns.[10] We were also pleased to see the report acknowledge the need for participation by civil society, and we believe it is essential that digital liberties and consumer protection advocates, academics, and security researchers participate in this specific conversation.

4. Road map: What information can help the government and stakeholders delineate a road map for achieving these goals? How should implementation be phased to optimize resources and commitments? Which actions are of highest priority, or offer opportunities for near term progress? Which actions depend on the completion of other actions? Are there known barriers that may inhibit progress on specific actions?

Internal corporate practices with respect to botnet takedowns are unclear and a meaningful conversation about the effect they have on user rights must spring from an understanding of current

---

Council III Working Group 7, Final Report on U.S. Anti-Bot Code of Conduct (ABC) for Internet Services Providers (ISPs) 64, (Mar. 2013), *available at* https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf. Other CSRIC reports have called for the need for best practices around privacy considerations.

[9] Privacy Impact Assessment, IAPP Resource Center, https://iapp.org/resources/topics/privacy-impact-assessment-2/ (last visited Feb. 9, 2018).

[10] Press Release, Microsoft, Microsoft, the FBI, Europol, and Industry Partners Disrupt the Notorious ZeroAccess Botnet (Dec. 5, 2013), http://news.microsoft.com/2013/12/05/microsoftthe-fbi-europol-and-industry-partners-disrupt-the-notorious-zeroaccess-botnet/.

practice. To be clear, inappropriate behavior by the companies who have been engaging in botnet mitigation is rare. Yet the government and private sector's renewed commitment to timely and automated botnet responses makes this conversation important now. Absent more information, civil society and other industry stakeholders have little common understanding of how to evaluate the risks associated with internal practices to deter, prevent, or mitigate botnets and distributed threats.

Sincerely,

Michelle Richardson
Deputy Director, Freedom, Security, and Technology Project

Joseph Jerome
Policy Counsel, Privacy and Data Project