July 28, 2017

National Telecommunications and Information Administration
US Department of Commerce
1401 Constitution Avenue, NW #4725
Washington, DC 20230

Attn: Evelyn L. Remaley, Deputy Associate Administrator

Re: Request for Comment, Executive Order 13800, ''Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" and the Government's Role in Addressing Automated Distributed Attacks

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 DC, and with a presence in Brussels, CDT works inclusively across sectors to find tangible solutions to todays' most pressing technology policy challenges.

We appreciate the opportunity to comment on automated distributed attacks (hereinafter botnets) both in these comments and through participation in NIST's July Workshop on Enhancing Resilience of the Internet and Communications Ecosystem. Because CDT recently discussed privacy at length in comments on your Internet of Things (IoT) green paper,[1] these comments will highlight additional principles that are crucial to the government's response to botnets.

[1]CDT Comments to the NTIA on Fostering the Advancement of the Internet of Things, Mar. 10, 2017, available at https://cdt.org/insight/cdt-comments-to-the-ntia-on-fostering-the-advancement-of-the-internet-of-things/.

Question 8: Policy and the Role of Government:
What specific roles should the Federal government play?
What incentives or other public policies can drive change?

New government investigative powers or shut down authorities.

Because the government already has extensive compulsory powers to respond to botnets, the government should not consider amending current law unless it can explicitly and precisely explain what authorities are missing and how new ones will be used. Any proposed legislation should be narrowly tailored to botnet mitigation and not affect the larger legal system. As CDT's has commented before, botnet bills introduced over the last several years would have made the Computer Fraud and Abuse Act broader and vaguer and would only discourage the types of independent research that could fight botnets in its own right.[2] So far, there is also little evidence that the government can justify more undefined civil takedown authorities beyond the ones they already have.[3]

In fact, the government just obtained new investigative authorities that can be used against botnets. Just eight months ago, an amendment to Federal Rules of Criminal Procedure granted the government the authority to remotely search multiple computers when they are spread across more than five judicial districts or when their locations are obscured by technological means.[4] Although CDT opposed this change at the time,[5] the tool is now in the government's tool box and already has been used in the investigation and takedown of the Kelihos botnet, for example. According to the Department of Justice, a combination of trap and trace orders and warrants allowed law enforcement to reroute internet traffic, identify infected computers, and prevent the spread of the malware that was spamming and scamming people across the world.[6]

---

[2] Harley Geiger, Despite Improvements, Whitehouse Computer Crimes Amendment to CISA Needs More Work, Oct. 21, 2015, available at https://cdt.org/blog/despite-improvements-whitehouse-cisa-amendment-needs-more-work/; Harley Geiger, Graham/Whitehouse Draft Bill Would Make CFAA Worse, July 17, 2015 available at https://cdt.org/blog/grahamwhitehouse-draft-bill-would-make-cfaa-worse/.

[3] Id.

[4] Federal Rules of Criminal Procedure, Rule 41(b)(6).

[5] Written Statement of The Center for Democracy & Technology Before the Judicial Conference Advisory Committee on Criminal Rules, Oct. 24, 2014, available at https://cdt.org/files/2014/10/CDT-Rule41-Written-Statement-final-20141024.pdf.

[6] DOCUMENTS AND RESOURCES RELATED TO U.S. V PETER YURYEVICH LEVASHOV, available at https://www.justice.gov/opa/documents-and-resources-related-us-v-peter-yuryevich-levashov.

Proportional use of existing authorities and collateral damage to unrelated computers/users.

It is crucial that the government's extensive criminal and civil authorities are used carefully to address botnets, and in fact the Departments of Justice and Homeland security should host a public and transparent discussion of how botnet investigations and takedowns occur. Because hundreds of thousands of computers can be impacted with a single investigative technique, even a good faith mistake can cause damage exponentially more serious than computer crime investigations targeted at a specific device and/or individual.

With so much at stake, the government should think through in advance how existing guidelines map onto network investigative techniques. The Attorney General's Guidelines, the FBI's Domestic Investigations and Operations Guide, the US Attorney's Manual and the Computer Crimes and Intellectual Property Section Manual all contain important principles of proportionality and risk. For example, these policies call for using the least intrusive means possible to conduct an investigation, permitting an escalation through more intrusive tactics as necessary. How does that apply to network investigative techniques? Will the administration draw different lines around identifying information, records and content, and how will those lines be defined? These policies also refer to proportional techniques based on the seriousness of the crime or risk to national security. How will the government judge seriousness in a botnet ecosystem that can range from annoying to a serious critical infrastructure threat?

These considerations are only more important when the government seeks to go beyond collecting information and interferes with the operation of a computer or system. If the government is seeking to reroute traffic, take down a server or remove malware from a device, collateral damage to innocent users or innocent mistakes can have serious implications. For example, in 2011 the Department of Homeland security took down a domain name that not only cut off a child exploitation site, but over 80,000 others. It reportedly took three days to restore innocent users' websites, which is certainly long enough to impede business, stifle discussion on breaking news, and otherwise interfere with important and lawful activities. The government should develop techniques that do not create this sort of collateral damage in non-emergency situations.

Reasonable attempts to provide notice and redress.

While the government is obligated to give notice to criminal defendants in botnet prosecutions, notice to victims is a largely discretionary. The government should standardize how it provides notice to device or account holders and always make a good faith effort to inform them that their computer is infected, has been accessed by government, or even recorded as a compromised entity in government investigations.

Even further, the government needs to create a redress mechanism for those situations where it does in fact make a mistake or causes collateral damage to innocent users or devices. A most egregious example happened in the U.K. in 2011 where a typo in an IP address led to a man

being wrongfully arrested for possessing child pornography.[7] While he was eventually cleared, it took years for the record to be corrected and only after the individual lost his job and access to his own children. This story rides on a human error-not an automated one—but underscores the stakes in these cases.

Voluntary cooperation with the private sector.

Beyond compulsory powers, the government will be engaging in voluntary relationships with corporate entities. In many ways, some sort of coordinated, automated response to botnets and the Internet of Things will be necessary to fight bad actors at scale, and doing so will advance cybersecurity across the system. The onus of securing devices should not fall solely or even primarily with lay consumers --this will not work as a practical matter and shifts responsibilities to those in the worst position to make change. We know from a recent Pew study that a majority of internet users do not follow long-recommended cyber hygiene practices.[8] While estimates vary, most industry commenters expect 10s of billions of devices to be connected to the internet in the coming years, making a device-by-device approach even more unrealistic as time goes on.

However, we recommend that these voluntary relationships operate in the open so that the public may be informed and congress may conduct oversight of the activities. One upside to compulsory powers is that they presumptively become public eventually, and are usually overseen by judges or the legislative branch. Voluntary efforts run the risk of operating in the dark and obscuring a level of coordination that would be offensive to the general public. It is imperative that private actors do not evolve into state actors without all the attendant oversight and accountability that comes with the latter.

Because voluntary relationships will likely only increase in number and complexity going forward, the government should commit to 1) publicly naming its partners, 2) publicly listing at the type of arrangements that it enters into and the actions either party agrees to take, 3) sharing statistics or estimates wherever possible about the number of devices, accounts or individuals affected by the actions, and 4) the legal authority authorizing the monitoring, routing, sharing or other activities pursuant to the agreements. While we expect that some classified information must be withheld from the public, the general contours of these cyber programs should never be kept secret considering the affect they potentially have on privacy, expression and security.

---

[7] Matthew Champion, This is What It's Like to Be Wrongly Accused of Being a Paedophile Because of a Typo by Police, Mar. 10, 2017, at https://www.buzzfeed.com/matthewchampion/this-mans-life-was-destroyed-by-a-police-typo?utm_term=.nyzKvNR66#.iyVP1qmYY.

[8] Americans and Cybersecurity, Pew Research Center, Jan. 2017, available at http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.