U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

Promoting Stakeholder Action Against Botnets and Other Automated Threats	))))))	Docket No. 180103005–8005–01

COMMENTS OF THE NCTA – THE INTERNET TELEVISION ASSOCIATION

William A. Check, Ph. D.
Senior Vice President, Technology
and Chief Technology Officer

Matthew J. Tooley
Vice President, Broadband Technology

Rick Chessen
Loretta Polk
NCTA – The Internet & Television Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

February 12, 2018

Table of Contents

U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

Promoting Stakeholder Action Against Botnets and Other Automated Threats	)	Docket No. 180103005–8005–01

COMMENTS OF NCTA –
THE INTERNET AND TELEVISION ASSOCIATION

NCTA – The Internet and Television Association[1/] hereby submits its comments in response to the Request for Comments (RFC)[2/] on the Draft Report issued by the Department of Commerce and the Department of Homeland Security (DHS) on bolstering resilience against botnets, DDoS attacks, and other automated and distributed threats.[3/] The Draft Report identifies opportunities and challenges associated with preventing automated and distributed attacks and discusses a series of goals that, if achieved, will improve the resilience of the Internet and Communications ecosystem.

INTRODUCTION AND SUMMARY

NCTA appreciates the responsiveness of the National Telecommunications and Information Administration (NTIA), the National Institute of Standards and Technology (NIST), and DHS to the input received from a range of entities in the Internet and Communications ecosystem in developing the Draft Report. The report sets forth a comprehensive analysis of the

---

1/ NCTA is the principal trade association for the U.S. cable industry, , representing cable operators serving approximately 85 percent of the nation's cable television households and more than 200 cable program networks. The cable industry is the nation's largest provider of broadband service after investing more than $250 billion over the last two decades to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to more than 30 million customers.

2/ Department of Commerce, National Telecommunications and Information Administration; Department of Homeland Security, *Promoting Stakeholder Action Against Botnets and Other Automated Threats*, Docket No. 180103005–8005–01, 83 Fed. Reg. 1342 (Jan. 11, 2018) ("RFC").

3/ REPORT TO THE PRESIDENT ON ENHANCING THE RESILIENCE OF THE INTERNET AND COMMUNICATIONS ECOSYSTEM AGAINST BOTNETS AND OTHER AUTOMATED, DISTRIBUTED THREATS, DEPARTMENT OF COMMERCE & DEPARTMENT OF HOMELAND SECURITY (Jan. 5, 2018), https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf ("Draft Report").

key issues and objectives that need to be addressed to strengthen the resilience of the ecosystem against botnets and other automated and distributed attacks. On behalf of its member companies, NCTA provides the following recommendations to clarify and improve the Final Report.

As the nation's largest providers of broadband Internet access service, cable companies have devoted considerable efforts and resources toward detecting, preventing. and mitigating automated and distributed attacks to protect their customers and their networks from service disruptions and malicious activity threats. NCTA's members have been leaders in deploying a diverse set of network capabilities, security tools and measures, and customer support services aimed at preventing, detecting, and mitigating botnet threats and Distributed Denial of Service (DDoS) attacks. Cable companies have invested heavily to develop and deploy leading edge products and services, such as tools to bolster network defenses against botnets and DDoS attacks. NCTA members also have deployed IPv6, Domain Name System Security Extensions (DNSSEC), network filtering and partitioning to isolate malicious traffic, the Border Gateway Protocol's (BGP) Flow specification to help scrub DDoS traffic, Software Defined Network (SDN) network features, and other anti-botnet capabilities.[4/] In addition, NCTA member companies offer a wide range of customer-facing tools and services to deter and remediate endpoint infections.[5/] Cable companies also play leading roles in several key collaborative industry-based and public-private initiatives to bolster anti-botnet efforts, and are actively involved on a daily basis in extensive information sharing activities through a variety of venues and exchanges.[6/]

4/ *See* Comments of NCTA – The Internet & Television Association, Docket No. 170602536-7536-01, at 7-11 (filed July 28, 2017)("Comments of NCTA").

5/ *Id.* at 11-12.

6/ *Id.* at 12-16.

As the Draft Report correctly recognizes, however, cable broadband providers and other Internet service providers (ISPs) are only one part of a diverse and interdependent Internet and Communications ecosystem. The Draft Report fully embraces the fundamental principle that anti-botnet efforts are – and must be – a shared responsibility among all entities across the full Internet ecosystem. It asserts that automated and distributed attacks are an ecosystem-wide problem, and that, most importantly, no single segment alone can prevent and protect against attacks. The causes and consequences of botnet and DDoS attack propagation and amplification implicate not just ISPs, but also network hardware and software companies, application developers, cloud providers and hosting platforms, edge providers, security specialists and tools providers, device makers, and business, enterprise, and residential end users, as well as many others. Holistic solutions that span the full breadth of the ecosystem are essential, because they reduce the likelihood that anti-botnet measures successfully implemented in some segments of the ecosystem will be negated by gaps and unaddressed vulnerabilities in others.[7/]

While the Draft Report helpfully recognizes that success in combatting botnets requires activating the full breadth of entities and actors within the Internet and Communications Ecosystem, there are portions of its findings and recommendations that should be revised in order to ensure consistency with that critical insight.[8/] The Final Report also would benefit from a forward-looking analysis of how the botnets of the future are expected to behave, and the strategies for detecting, deterring, and mitigating automated and distributed attacks that devise

---

[7/] For example, an ISP can put in place many tools to reduce the impact of DDoS attacks, which often rely on spoofing source network addresses. But the tools are not unlimited in their capacity and capability. If a hosting provider or other network fails to take diligent steps to prevent their platform from being used as a source of such spoofing, then they will make efforts by others in the ecosystem to combat DDoS attacks more difficult and expensive to combat.

[8/] *See infra* at 8-9.

new techniques to propagate and amplify attacks through exploitation of cloud computing, the Internet of Things (IoT), artificial intelligence, and machine learning capabilities.[9/]

As the Draft Report recognizes, automated and distributed attacks are a global problem, affecting the entire Internet and Communications ecosystem. As such, the attacks must be met with collective and coordinated action domestically and abroad. The overwhelming majority of botnet attacks originate from outside the United States and are located beyond our borders, meaning that effective action to reduce such threats requires government leadership to foster globally-scaled solutions and international cooperation. While the Draft Report adequately captures the scope of the problem, the Final Report should include concrete initiatives for collective action that can be implemented across the Internet and Communications ecosystem and in international venues.

In an effort to address existing gaps and vulnerabilities, the Draft Report provides important recommendations for key segments of the ecosystem.[10/] The Draft Report endorses the establishment of baseline security profiles for IoT devices that eventually could be adopted as international standards. It also promotes efforts to ensure that software developers implement more robust security design and updates. In addition, the Draft Report seeks to spur enterprise networks toward greater utilization of existing services, tools, and capabilities that are on the market today for detecting, deterring, and mitigating DDoS attacks and botnet threats. These recommendations should materially bolster the ecosystem's overall resilience against botnets. The Final Report would benefit from a similar analysis focused on measures to strengthen the resilience of cloud platforms, which are increasingly being exploited as launch and amplification points for botnet attacks.

9/ *Id.* at 10.

10/ Draft Report at 23-27; *see infra* at Section III.

The Draft Report also validates several security-related offerings and capabilities provided by ISPs, such as ingress and egress filtering, DDoS mitigation services, anti-spoofing and fast flux deterrence techniques, IPv6, and other offerings and tools highlighted in the Communications Sector Coordinating Council's (CSCC) Technical White Paper and NCTA's comments.[11/] At the same time, some ISP-related findings and recommendations warrant further elaboration or revision to reflect additional relevant factors, as well as limitations imposed by ecosystem interdependencies.[12/] Likewise, the Draft Report's discussion of ISP information sharing activities would benefit from additional discussion of promising ongoing activities as well as the critical importance of improving the capacity of sharing venues to identify and target actionable information. In addition, while the Draft Report correctly flags the potential for prescriptive regulation to handicap security innovation and thereby hamper the objective of strengthening resilience,[13/] select portions that could be read to favor traditional regulation should be revised.[14/]

In short, while the Draft Report offers a thorough analysis of key botnet prevention issues facing the ecosystem today and delineates a number of effective recommendations for addressing those issues, we recommend that NTIA, NIST, and DHS should implement the following improvements in the Final Report:

- In discussing network-related findings and recommendations, consistently articulate the expansive and accurate conception of "infrastructure providers" set forth in Section II;[15/]

11/ Draft Report at 9-12; Comments of NCTA at 7-11; *Industry Technical White Paper*, COMMUNICATIONS SECTOR COORDINATING COUNCIL, Docket No. 170602536-7536-01, at 14-21, 29-30 (filed July 28, 2017).

12/ *See infra* at Section IV.

13/ *See e.g.*, Draft Report at 24 ("Due to the complexity and diversity across the IoT landscape, it is difficult to envision a set of one-size-fits-all rules that could ensure security while keeping pace with the rate of change and the dynamic nature of the threat environment"). *See also id.* at 20.

14/ *See infra* at Section V.

15/ *See infra* at 8-9.

- Include a forward-looking analysis of how the next generation of botnets are expected to behave, strategies for addressing them, and an analysis of gaps, unknowns, and open questions requiring further study;[16/]

- Set forth a prioritization of anti-botnet initiatives that should be addressed on a global scale and provide concrete ideas of specific international venues and vehicles for advancing those initiatives;[17/]

- Include specific recommendations for cloud providers, Content Delivery Networks (CDNs), and related platform providers, given their increasingly prominent roles as mechanisms for botnet operation, propagation, and amplification;[18/]

- Reframe passages suggesting that end users could be relieved from responsibility for preventing and addressing device infection;[19/]

- Enrich the discussion of ISP-related issues involving use of network filtering and slicing capabilities, DDoS mitigation services, and information sharing activities; [20/] and

- Modify language that could be read to support greater regulatory involvement in network traffic management practices and IoT device certification and marketing to reinforce the goal of promoting market-driven security innovation.[21/]

Soon after release of the Final Report, NTIA, NIST, and DHS should effectuate its recommendations by convening a series of workshops that draw upon the resources and expertise of the relevant Sector Coordinating Councils, Information Sharing and Analysis Centers (ISACs), and Information Sharing Analysis Organizations (ISAOs) to focus on implementing key actions proposed in the Report. Stakeholders participating in the workshops should develop the structure and timetable for implementing the Final Report's most significant recommendations, which would include concrete plans with specific commitments by relevant stakeholders for implementing the following action items:

16/ *See infra* at 10-11.
17/ *See infra* at 11-12.
18/ *See infra* at 17-18.
19/ *See infra* at 18-19.
20/ *See infra* at 20-25.
21/ *See infra* at 25-27.

- NTIA, NIST, device makers, and other interested parties should set forth the process and timetable to forge baseline security profiles for IoT devices based on consensus industry standards;[22/]

- NTIA, NIST, software providers, and other interested parties should work together to set forth the process and timetable for a multi-stakeholder process establishing software development protocols for IoT products that address vulnerability detection and reporting and software patching and upgrading;[23/]

- NTIA, NIST, the retail industry, leading trade associations representing enterprise users, and other interested parties should set forth the structure and timetable for a process aimed at providing guidance to enterprise networks on using the NIST Cybersecurity Framework to address botnet and DDoS attack prevention and mitigation;[24/]

- DHS, in conjunction with all 16 critical infrastructure sectors, should work with the National Council of Information Sharing and Analysis Centers to examine, and develop guidelines for, identifying, what constitutes "actionable" information in various critical infrastructure sectors; [25/] and

- The Communications and Information Technology (IT) sectors, in consultation with DHS (their sector-specific agency), NTIA, NIST, and industry associations and standard-setting organizations, will continue to work together on developing network traffic management practices, tools, and capabilities designed to detect, deter, and mitigate automated and distributed attacks.[26/]

The foregoing modifications and action items should go a long way to achieving the goal of dramatically reducing threats perpetrated by automated and distributed attacks on the nation's infrastructure underlying the digital ecosystem.

22/ *See infra* at 13-15.
23/ *See infra* at 15-16.
24/ *See infra* at 16-17.
25/ *See infra* at 23-24.
26/ *See infra* at 25-26.

I. THE DRAFT REPORT SHOULD CONSISTENTLY ADHERE TO ITS ECOSYSTEM-WIDE CONCEPTION OF "INFRASTRUCTURE PROVIDERS" AND ANALYZE HOW BOTNETS WILL EVOLVE IN THE ECOSYSTEM

The Draft Report constructively finds that strengthening resilience against automated and distributed attacks is a shared responsibility among a diverse set of interdependent entities and business segments.[27/] Consistent with this core insight, the Draft Report defines the "infrastructure" of the Internet and Communications ecosystem broadly, encompassing the "technology and organizations that enable connectivity, interoperability, and stability, going beyond the physical wires, wireless transmitters and receivers, and satellite links to include the hardware, software tools, standards, and practices on which the ecosystem depends."[28/] Infrastructure includes "routers, switches, Internet service providers, DNS providers, software, device makers, content delivery networks, hosting and cloud service providers."[29/] The Draft Report emphasizes that because of "the complexity of modern infrastructure, with key tools and players interspersed through the ecosystem, no single tool can secure the infrastructure."[30/]

The Draft Report further acknowledges that ISPs alone cannot address botnet threats, finding that "no single actor or sector is responsible for single-handedly addressing" botnet risks.[31/] It notes that while many solutions "involve active coordination with ISPs, putting sole responsibility at the network level would make all traffic dependent on this connective layer to determine what 'good' traffic looks like."[32/] Not only would such an approach impose an undue – and impracticable – burden on ISPs, it also would be ineffective. Botnets exploit and impact all parts of the ecosystem and hence all those elements must be part of the solution.

27/ Draft Report at 9.
28/ *Id.*
29/ *Id.* at 10.
30/ *Id.*
31/ *Id.* at 20.
32/ *Id.*

Having appropriately scoped the breadth of entities and actors that comprise the Internet and Communications Ecosystem, the Draft Report's discussion of recommended actions in several places appears to conflate ISPs with all infrastructure providers. For example, the Draft Report states that "[Enterprises] may not understand the limitations of their contracts with Internet service providers, or the availability of products and services to mitigate DDoS attacks."[33/] In fact, however, DDoS mitigation services are available from a wide range of infrastructure providers besides ISPs, and enterprise take rates may simply reflect an incomplete understanding of the value of these offerings or a flawed cost-benefit analysis.

Similarly, the Draft Report states that "[t]he impact of past botnets has been mitigated by actions taken by ISPs—mainly absorbing excess traffic and cease and desist actions—but past mitigations were mainly reactive by nature, and the increase in IoT devices indicates diminishing returns for these traditional mitigation strategies."[34/] But these past actions were not limited to ISPs, and neither will future actions be limited to ISPs. While ISPs may engage in cease and desist actions as part of providing their services, most takedowns are often achieved through coordinated action among those that operate and provide domain name servers, such as Google DNS, Open DNS, UltraDNS, DYN, and Regional Internet Registrars (RIRs). Other parts of the Draft Report that reference only ISPs, instead of infrastructure providers more broadly, likewise should be revised.[35/] Consistent adherence to the broad model of the cybersecurity "ecosystem" identified in the Draft Report will help facilitate the collective action and cross-sector coordination necessary to combat botnets and other automated and distributed threats. The Final

---

33/ *Id.* at 12.

34/ *Id.* at 24.

35/ *See e.g., id.* at 13 (reference to "ISP-based detection services" rather than "detection services from infrastructure providers); *see also id.*31, Action 3.1 (reference to "networking industry" traffic management offerings for enterprise networks rather than "infrastructure provider"); *id.* at 33, Action 4.1.

Report should ensure that its findings and recommendations in the Final Report more closely conform to that conception.

The emergence of the cloud as a key platform for launching and amplifying botnet attacks underscores the importance of ensuring fidelity to the broad conception of infrastructure articulated at the beginning of the Draft Report.[36/] Cloud service providers are correctly defined as part of the infrastructure of the Internet and Communications Ecosystem, but then are implicitly excluded from recommendations applicable to ISPs only. Indeed, the Draft Report contains few recommendations for cloud providers, even though they are an increasing target for exploitation by bot masters and play a growing role in botnet mitigation. The emergence of global cloud platforms has made the Internet as much a network of clouds as it is a network of networks. Further, the cloud platforms are the backend hosts for IoT data processing and commands, integrated Big Data analytics, artificial intelligence, and digital assistants – all of which have (or will) become ripe targets for botnet exploitation.

More rigorous analysis of the role of cloud providers, CDNs, and other components of Internet infrastructure in bolstering resilience also will help make the Final Report more forward-looking, examining not only how botnets are behaving today but also how they will evolve in the future. While the Draft Report describes how recent botnets have behaved in the past,[37/] the Final Report must examine how botnet propagation and amplification techniques will function on an Internet being reshaped by the prevalence of cloud computing, artificial intelligence (AI), machine learning, and other advancements. The Final Report should address the prospect of

---

[36/] *See* Comments of NCTA at 17; Danny Palmer, *Cloud Computing: Why a Major Cyber-Attack Could Be as Costly as a Hurricane*, ZDNET (Jan. 17, 2018), http://www.zdnet.com/article/cloud-computing-why-a-major-cyber-attack-could-be-as-costly-as-a-hurricane/ Andy Greenberg, *How Hackers Hid a Money-Mining Botnet in the Clouds of Amazon and Others*, WIRED (July 24, 2014), https://www.wired.com/2014/07/how-hackers-hid-a-money-mining-botnet-in-amazons-cloud/.

[37/] *See, e.g.*, Draft Report at 7.

botnets integrating with AI, infiltrating the cloud, infecting digital assistants, and/or harnessing the power of the cloud. AI-powered bots can pollute social media or engage in other malicious activities, such as stealing sensitive information or manipulating public opinion for financial or political advantage. In order to proactively meet the future challenges posed by botnets and other malware, the Final Report should initiate a review to identify the next generation of automated and distributed threats and strategies for mitigating and deterring them on a global scale. Because the botnet landscape continues to evolve, this review also should capture gaps in our current understanding of how attack surfaces and propagation techniques will change and compile questions and issues that will warrant further study.

II. WHILE THE DRAFT REPORT RECOGNIZES THE GLOBAL SCALE OF THE BOTNET PROBLEM, THE FINAL REPORT SHOULD OFFER MORE SPECIFIC AND CONCRETE GLOBALLY-BASED SOLUTIONS

The Draft Report appropriately frames the global scope of the problem of automated and distributed attacks. It acknowledges that "broad advances in the Edge Device technical domain" must take place on a global scale, because the majority of compromised devices in recent botnet attacks have been located outside the U.S.[38/] Because the problem is worldwide in nature, bolstering the resilience of the Internet and Communications ecosystem necessitates considerable coordination with international partners.[39/]

While the Draft Report acknowledges that effective action against botnets requires greater international coordination, the Final Report should set forth a concrete vision of venues and activities that can help achieve such a result. Moreover, the Draft Report's recommendations are almost exclusively domestically focused, notwithstanding the fact that the vast majority of botnets – and compromised devices – are from outside the U.S, thereby

---

38/ Draft Report at 3, 7, 16.

39/ *Id.* at 7, 20.

highlighting the relative effectiveness of botnet deterrence and mitigation practices and tools here at home compared to other parts of the world.[40/] Global connectivity, however, ultimately will corrode the success and impact of purely domestic solutions that are far from the source of most malicious activity and most infected devices. Meaningful progress toward bolstering resilience requires the establishment and enforcement of international norms and standards.

The Final Report should contain more concrete suggestions for global initiatives and recommended venues for deeper international engagement. At a global level, bolstering resilience will depend upon more than just international adoption of best practices. It requires broader adoption of a common set of cybersecurity norms that can be incorporated in trade treaties. For example, the global nature of cybersecurity can hamper botnet investigation and takedown activity, often requiring the cooperation and coordination of multiple law enforcement agencies across the globe to neutralize a botnet. The Final Report should recommend processes for streamlining botnet takedowns on an international scale so that law enforcement across the globe will be in alignment.[41/] This same set of norms would give law enforcement more tools to use in mitigating botnets, such as requesting that Autonomous System Networks (ASNs) habitually hosting bad actors should be removed from the Internet routing table. Thus, the suggestion that the Federal government should make efforts to deepen coordination on enlisting regional registrars to assist with attribution of bad actors in order to facilitate botnet

---

40/ Draft Report at 3, 7; Comments of NCTA at 4, 42. *See also* ITU-D, *Global Cybersecurity Index (GCI) 2017*, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (finding that the U.S. demonstrates a high commitment to cybersecurity).

41/ Comments of the ACT | The App Association Comments, Docket No. 170602536-7536-01, at 4 (July 28, 2017) ("The App Association recommends that the U.S. government provide law enforcement new and sustained resources to combat botnet attacks, and work to streamline international processes for botnet takedown. NTIA is well-positioned to lead, coordinate, and facilitate U.S. government agencies in accomplishing these goals.").

investigations is useful,[42/] and the delineation of more such specific undertakings and initiatives on an international scale would be helpful.

III. THE DRAFT REPORT CONTAINS A NUMBER OF CONSTRUCTIVE RECOMMENDATIONS, BUT SHOULD REVISE ITS DISCUSSION OF SOME PARTS OF THE ECOSYSTEM

The Draft Report endorses a variety of leading-edge security capabilities offered by ISPs and other infrastructure providers, such as ingress and egress filtering, DDoS mitigation services, anti-spoofing and fast flux deterrence techniques, and IPv6.[43/] It notes that the tools, processes, and practices to boost resilience against botnets "are widely available," but their adoption lags due to a lack of awareness, cost avoidance, and insufficient market incentives.[44/] ISPs, however, have ample incentive to invest in state-of-the-art security tools and capabilities to protect their customers against botnet threats and DDoS attacks because their business success is tied directly to maximizing their customers' network usage and preserving and strengthening their relationships with end users – both of which hinge on providing a safe, trusted, and secure network environment.[45/] Other parts of the ecosystem, however, may not be in direct privity with end users or may have only one-time interactions with them, and greater effort should be made to align their incentives with the goals of strengthening security and resilience.[46/]

IoT Device Security Profiles. The Draft Report recognizes that IoT device security and upgradability constraints are key issues that must be vigorously addressed in order to boost

---

42/ Draft Report at 33.

43/ *See id.* at 10-11, 32, 34.

44/ *Id.* at 16.

45/ Comments of NCTA at 5-12. These investments often prove to be cost-effective, not only because they strengthen customer engagement and trust but also because they reduce call volumes and technician visits arising from malicious activity.

46/ *See* Comments of Google Inc. and Nest Labs, Inc., Docket No. 170602536-7536-01, at 6 (filed July 28, 2017) ("Rather than impose new legal mandates, government can and should encourage the marketplace to do more to reward those who invest in good security practices and punish those that do not.").

resilience.[47/] Security issues for IoT devices will arise over the entire life-cycle of the product,[48/] and some IoT devices may operate for long periods of time without any user interaction or oversight. Importantly, the Draft Report highlights as its first recommended action the need to "establish broadly accepted baseline security profiles for IoT devices in home and industrial applications, and promote international adoption through bilateral arrangements and the use of international standards."[49/] The Draft Report correctly recognizes that a considerable portion of these baseline security profiles can be culled from the "existing suite of standards and practices."[50/] There are a plethora of organizations whose work in this area can be drawn upon, including DHS,[51/] NIST,[52/] the Internet Engineering Task Force (IETF),[53/] the Broadband Internet Access Technical Advisory Group (BITAG),[54/] the Open Connectivity Foundation

47/ *See, e.g.*, Draft Report at 14, 16-17, 23-25.

48/ *See* Comments of Symantec Corporation, Docket No. 170602536-7536-01, at 2-3 (filed July 27, 2017) ("Attacks using IoT devices also greatly lower the barrier of entry for cyber criminals, as there is little or no security on many of them. Unlike a desktop computer, or laptop, which often have security software installed and receive automatic security updates, IoT devices are often only protected by a user name and password. Analysis of the passwords used by IoT malware to attempt to log into devices revealed that user names and passwords are often never changed from their factory default settings.").

49/ Draft Report at 23

50/ *Id.* at 25.

51/ *See* DEPARTMENT OF HOMELAND SECURITY, STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (2016), https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf.

52/ *See NIST Special Publication 800-183, Networks of 'Things'*, National Institute of Standards and Technology (2016), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf; Ron Ross, *et al.*, *NIST Special Publication 800-160: Systems Security Engineering,* National Institute of Standards and Technology (2016) (updated January 3, 2017), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf.

53/ *See Software Updates for Internet of Things* (November 2017), https://datatracker.ietf.org/wg/suit/about/.

54/ *See* BROADBAND INTERNET TECHNICAL ADVISORY GROUP, INTERNET OF THINGS (IOT) SECURITY AND PRIVACY RECOMMENDATIONS (2016), https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf.

(OCF),[55/] the National Security Telecommunications and Advisory Council (NSTAC),[56/] the Federal Trade Commission (FTC),[57/] and the Communications Sector Coordinating Council.[58/]

IoT security is a matter of significant interest to cable broadband service providers given their investment, deployment, and management of Internet facilities and technologies over several decades. For example, CableLabs is working with OCF on standards-setting activities relating to several key IoT security issues identified in the Draft Report, including authentication, authorization, delivery of software updates, hardware roots of trust and managing device life cycles.[59/] While continuing to promote this type of private sector leadership in IoT technology and standards development, NTIA and NIST also should convene a focused process, involving device makers and other interested stakeholders to accelerate and consolidate IoT device standards development work to benefit the ecosystem as a whole.

IoT Product Software Development and Updating. As the Draft Report correctly finds, addressing vulnerabilities in the software development, patching, and upgrading processes for IoT devices also is critical to preventing and mitigating software vulnerabilities that affect the volume, velocity, and scale of automated and distributed attacks.[60/] IoT devices frequently ship

---

55/ *See* OPEN CONNECTIVITY FOUNDATION, https://openconnectivity.org/ (last accessed Feb. 2, 2018). OCF's membership is broad-based with roughly 400 members, including leading companies at all levels of the IoT space---- silicon (e.g., Intel, Qualcomm), software (e.g., Microsoft), platform and finished-goods (e.g., Cisco, Samsung, LG), and network operators.[55] It is an open, industry-led effort to develop a specification to enable connected devices to *securely* communicate with one another regardless of manufacturer, operating system, chipset, or physical transport.

56/ *See* DRAFT NSTAC REPORT TO THE PRESIDENT ON INTERNET AND COMMUNICATIONS RESILIENCE, NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE (Jan. 5, 2018), https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20DRAFT%20-%20508%20compliant.pdf.

57/ FEDERAL TRADE COMMISSION, THE INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD (2015) https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

58/ COMMUNICATIONS SECTOR COORDINATING COUNCIL, INDUSTRY TECHNICAL WHITE PAPER (2017), https://docs.wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf.

59/ CABLELABS, A VISION FOR SECURE IOT (2017), http://www.cablelabs.com/vision-secure-iot/.

60/ Draft Report at 25-26.

with outdated software containing known flaws and often lack a mechanism for updating software or alerting consumers of the need for a patch or upgrade.[61/] The Draft Report notes that "common software development techniques result in, optimistically, a flaw every 2,000 lines of code," and that many of these bugs create exploitable security vulnerabilities.[62/] A recent study on the state of software security noted that while "there are a number of maturing programs that are making steady progress on their vulnerability flaw density," such programs "are still in the minority of organizations both small and large and even the most mature programs still have plenty of room to improve their application risk posture."[63/] The President's National Security Telecommunications Advisory Committee (NSTAC) recent report on Internet and Communications resilience found that the "ecosystem requires increased use of secure software development and management practices."[64/] NTIA and NIST – in conjunction with the IT sector, software makers, and other interested parties – are well-suited to lead an effort to improve software development and updating tools and processes, particularly given NTIA's experience with the software vulnerability disclosure and software updating and patching multi-stakeholder initiatives.

Enterprise Network Issues. The Draft Report also finds that enterprise customers are taking insufficient advantage of current offerings and capabilities that could boost security against automated and distributed attacks.[65/] Despite the fact that they are highly attractive targets for botnets seeking to harvest or exploit valuable commercial data, enterprise customers often forego elementary security tools and capabilities that could lower their exposure to cyber

---

61/ *Id.* at 18.
62/ *Id.* at 15.
63/ Veracode, STATE OF SOFTWARE SECURITY 2017, AT 6.
64/ National Security Telecommunications Advisory Committee, NSTAC REPORT TO THE PRESIDENT ON INTERNET AND COMMUNICATIONS RESILIENCE, at 11.
65/ *See, e.g.*, Draft Report at 10-11.

risks. NTIA and NIST should explore programs and incentives that would encourage enterprise customers to invest in and commit to offerings, tools, and capabilities on the market today that help detect, disrupt, and mitigate automated and distributed attacks.[66/] They also should encourage enterprise customers to address network security and cyber hygiene as they approach workplace safety – through training on anti-botnet prevention measures, awareness programs, and built-in job functions. Further, NTIA should convene a focused process, that would include NIST, the retail industry, leading trade associations representing enterprise users, and other interested parties, designed to formulate specific guidance and recommendations that would help enterprise networks use the Cybersecurity Framework risk management process and informative references to strengthen their defenses against automated and distributed networks. This undertaking could be patterned after efforts by several sectors, following publication of Version 1.0 of the Framework, to provide guidance on tailoring use of the Framework to the specific characteristics and attributes of particular industry segments.[67/]

Cloud Providers, CDNs, and Other Platform Providers. As discussed previously, the Draft Report does not discuss any specific actions for cloud providers notwithstanding their key position in the ecosystem. Akamai notes that it has "unmatched visibility into Internet activity and active attacks" due to the global scale of its platform, and can employ big data analytics on the aggregate traffic flow across its platform to identify new attack vectors, pro-actively warn at-risk endpoints, and provide actionable advice on defensive measures and mitigation tools.[68/] Cloudfare notes that the presence of its data centers on the edge of the network "allows the use of

---

66/ *Id.* at 32; Comments of NCTA at 7-8, 24.

67/ For example, the communications developed specific guidance for use of the NIST Framework to bolster communications network cyber defenses undertaken by the FCC Communications Security, Reliability, and Interoperability Council (CSRIC) IV Working Group 4. CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES, WORKING GROUP 4: FINAL REPORT (Mar. 2015), http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf

68/ Comments of Akamai, Docket No. 170602536-7536-01, at 26-27 (filed July 28, 2017).

the collective intelligence of an entire network to identify and block new threats."[69/] Further, there is a variety of work and innovation taking place around augmenting the security of links between cloud servers and IoT devices in order to reduce device vulnerability and strengthen server defenses against ingesting and retransmitting malware from infected client devices that are being used for attacks.[70/] Indeed, Microsoft highlights the importance of cloud providers utilizing tools and capabilities that not only withstand attacks from external sources, but also provide protection against other infected tenants on the platform.[71/] The Final Report should integrate these insights, measures, and capabilities into a set of recommended actions for cloud providers, CDNs, and other components of Internet infrastructure.

End Users. The Final Report should reframe its discussion of end user responsibilities, particularly regarding language suggesting that it is impractical to hold end users responsible for infected devices and of limited utility to seek to change consumer behavior.[72/] Cable providers have significant experience working with our customers to address security challenges, and end users have an important role to play. End users often can be the target of malicious attacks, as well as the vehicle by which botnets are propagated and amplified. Technology should allow for end-users to take some responsiblity for security on their local area networks (LANs) but at present they have limited capacity to address or take control over remediation of remote attacks on them. To help meet this challenge, the Federal government should consider enlisting the FTC, along with other agencies such as DHS, the Small Business Administration (SBA), and NIST, to develop a program that assists the small business sector in obtaining resources and services to prevent and remediate botnets. Further, the ecosystem as a whole would benefit from

69/ Comments of Cloudfare, Docket No. 170602536-7536-01, at 3 (filed July 28, 2017).
70/ *Id.*; Comments of NCTA at 26-27.
71/ Comments of Microsoft, Docket No. 170602536-7536-01, at 8 (filed July 28, 2017).
72/ Draft Report at 18.

greater efforts to promote education and awareness around good cyber hygiene by all end users – regardless of the network they may be on.

The "human element" is a significant factor in the spread of botnets and DDoS attacks, often because of the failure of end users to take rudimentary steps to protect themselves against attacks.[73/] While IoT devices and products should be engineered based upon how consumers actually behave – rather than how the might ideally behave – more education regarding the basics of good cyber hygiene can help secure Internet endpoints against botnet threats and DDoS attacks. Indeed, the Draft Report elsewhere acknowledges the need for – and benefits of – greater education and awareness efforts directed toward end users.[74/] Boosting the collective knowledge and vigilance of all end users with regard to botnet risks and key preventive measures would benefit the entire ecosystem. The Final Report should reframe language from the Draft Report that could be read as relieving consumers from any role in helping to defend against botnets and DDoS attacks.

IV. THE FINAL REPORT SHOULD REFINE SOME OF THE DRAFT REPORT'S ISP-RELATED FINDINGS AND RECOMMENDATIONS

While reinforcing the value of a number of the security-related offerings and capabilities from ISPs, the Draft Report does not take full account of some of the interdependencies and countervailing considerations that may limit the accuracy or efficacy of some of its ISP-related findings and recommendations.

Filtering Capabilities. The Final Report should make clear that its recommendations for greater deployment and procurement of filtering capabilities apply across the ecosystem, and not just to ISPs. In its current form, the Draft Report could be read to suggest that ingress and egress

---

73/ *See* Comments of Consumer Technology Association, Docket No. 170602536-7536-01, at 9-10 (filed July 28, 2017); Comments of NCTA at 28-30.

74/ Draft Report at 8, 16, 17, 19, 37.

traffic filtering is only a capability for carriers and ISPs, when in fact it can and should be incorporated into networks of all sizes including those operated by enterprises, small businesses, and even home networks. As NCTA noted in its initial comments, enterprises have been slow to implement proven defensive measures such as BCP-38, IETF's best practices recommendation for using ingress filtering to deter DDoS attacks.[75/] BCP-38 applies to any network that has been assigned an autonomous system number by a RIR. Autonomous system numbers can be assigned to networks of all sizes from large ISP networks down to small business networks. Even for enterprise customers that may not have an autonomous system number, ISPs cannot unilaterally filter traffic. Instead, they provide that capability in the context of the service provider/customer relationship and in accordance with the level of service selected by the customer.

DDoS Mitigation Services. The Draft Report observes that DDoS mitigation services are not purchased "due to the expense" or because of the failure of enterprises to understand the limits of their contracts with ISPs.[76/] This analysis, on its own, is incomplete. Anti-DDoS services are offered by a large number of companies in the infrastructure space, including carriers, ISPs, cloud providers, and specialized anti-DDoS companies, so the notion that ISP service contracts or pricing constitute an impediment is misleading given the competitiveness of the market. The market for anti-DDoS services is highly competitive and the companies serving that market provide a large menu of capabilities to choose from, allowing enterprises to customize the service as needed to match their network requirements. Further, the fact that some

---

[75/] Filtering techniques other than BCP-38/84 are also used. ISPs and other network infrastructure providers do forms of filtering at the routing layer. The cable industry is actively participating in the National Cybersecurity Center of Excellence (NCCoE) project to demonstrate the Route Origin Validation (ROV) feature that has been added to BGP.

[76/] *Id.* at 10.

enterprise end users may opt against purchasing a service level that includes the capability to integrate anti-DDoS products with their existing network is not necessarily a function of contract limits, but may simply reflect a failure to appreciate the value of that offering or a business decision predicated upon an incomplete cost-benefit analysis.

The burden of protecting enterprises against automated and distributed threats and alerting them about ongoing attacks and deterrence, detection, and remediation solutions should not fall on the shoulders of the infrastructure providers alone. Enterprises of all sizes should be accountable for the tools and capabilities they choose – or do not choose – in conjunction with obtaining Internet connectivity, and they should have response plans in place for a botnet or DDoS attack so that they can address such situations in a timely manner. The under-consumption of anti-DDoS services suggests that they would benefit from the development of incentives (*e.g.*, favorable tax treatment for both suppliers and purchasers). NTIA should work in concert with the SBA to develop programs and policies that encourage greater adoption of these products and services, in order to overcome what may be the default impulse among many enterprises to refrain from spending capital on such items until they are in the throes of an attack.

Information Sharing. The Draft Report understates the robust state of information sharing among ISPs and fails to take account of key factors that should be addressed to enhance sharing and exchange activities across sectors. In discussing information sharing by ISPs, the Draft Report opines that current sharing arrangements "are often driven by personal relationships and are not comprehensive."[77/] It notes that while "the information technology and communications sectors do actively work to understand security risks, sectors are unable to coordinate well with other sectors."[78/] The Draft Report states that collaboration between ISPs

---

77/ *Id.* at 28.

78/ *Id.* at 20.

and peering partners "should include sharing of detection, notification, and planned or utilized mitigation methods within the network,"[79/] suggesting that the current level of such activity is inadequate. It also expresses concern that sharing may be "encumbered by commercial concerns" that could be addressed in their peering and transit agreements.[80/]

This analysis significantly understates the level and efficacy of current ISP sharing arrangements.[81/] ISPs are involved with a wide variety of information sharing organizations, including the Communications ISAC, the National Cybersecurity and Communications Integration Center (NCCIC), the National Council of ISACs, DHS' Cyber Storm exercises, the North American Electric Reliability Corporation Gridex exercises, and the Department of Defense's Cyber Gard exercises. On a daily basis, these organizations actively exchange threat data, strategic intelligence, and deterrence measures among a broad range of entities, both within and outside the communications sector. Assertions that cross-sector coordination is not functioning effectively are overstated. Whatever friction that may exist is anomalous, largely attributable to differences in how to distinguish between "signal" and "noise" with regard to threat information, and those differences will be resolved over time as coordination evolves. The public-private partnership with DHS, administered primarily through the NCCIC, which includes several resident ISPs, provides an effective forum for coordinating among sectors and resolving issues as needed.

The Draft Report does not take account of factors that currently inhibit both the volume and quality of information sharing. For example, mandated top-down information sharing protocols such as STIX/TAXII have impeded information sharing by creating obstacles for

---

79/ *Id.* at 28.

80/ *Id.*

81/ Comments of NCTA at 15-16; WORKING GROUP 5: CYBER SECURITY INFORMATION SHARING, COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL (March 2017).

participation in exchange venues by organizations that lack the resources to upgrade their threat management platforms to support STIX/TAXII. The choice of protocol/format for information sharing should be use case driven. For example, the cable industry has found that JSON is a much better format for sharing indicators of compromise (IOCs) because it is more adaptable, as evidenced by the fact that STIX/TAXII – previously compatible only with XML– itself has been updated to support JSON. The Final Report should address the handicaps to sharing, including, for instance, by recommending that the choice of protocol/format for information sharing should be use case driven, and that STIX/TAXII should accommodate all such use cases.

The Draft Report also pays insufficient attention to the need for sharing platforms to function less as venues for exchanging raw data and more as mechanisms for sharing reliable, actionable intelligence tailored to the needs of recipients.[82/] Indeed, the DHS Inspector General recently released a report on information sharing platforms highlighting this issue.[83/] Actionable information can vary by sector. It is critical for all members of the information sharing community to understand what is "actionable" and that the definition of "actionable" varies by sector. Therefore, it would be beneficial for DHS, in conjunction with the information sharing community (e.g., the National Council of ISACs) and the 16 critical infrastructure sectors, to develop guidelines for the "actionable" attributes for indicator of compromise (IOCs) for each sector.

82/ *See e.g.*, Comments of NCTA at 19 (Noted limited utility of sharing suspect IP address information without a time stamp, due to prevalence of dynamic IP addresses and use of fast flux techniques by malicious actors).

83/ DEPARTMENT OF HOMELAND SECURITY, OFFICE OF INSPECTOR GENERAL, BIENNIAL REPORT ON DHS' IMPLEMENTATION OF THE CYBERSECURITY ACT OF 2015, AT 4 (2018) ("[T]he system DHS currently uses does not provide the quality, contextual data needed to effectively defend against ever-evolving threats"); *id.* at 12 (Because the AIS feed is produced through an automated process, with pre-determined data fields, the information many not provide sufficient details to be actionable").

Additionally, ISPs do actively share information with law enforcement.[84/] The bottleneck with large law enforcement led botnet takedowns is not the lack of information; but rather the lack of adequate resources within law enforcement to address the scale and velocity needed to rapidly takedown botnets. The Final Report should reflect this shortfall. Lastly, as the Draft Report itself acknowledges,[85/] there remain concerns across the ecosystem that legal uncertainties and liability concerns continue to serve as an obstacle to achieving optimal levels of information sharing.[86/] The Final Report should call for DHS, in conjunction with the information sharing community (e.g. National Council of ISACs) and the 16 critical infrastructure sectors, to address this ongoing challenge.

Other ISP-Related Findings and Recommendations. The Draft Report asserts that ISPs should do more to observe device-specific misbehavior.[87/] There are, however, regulatory and customer goodwill considerations associated with having ISPs unilaterally assert greater control over securing customer devices – particularly those that are not furnished or leased by the ISP itself – against botnets, viruses, and other malware. The Draft Report also erroneously suggests that ISPs are "less likely to diligently follow-up" on botnet/malware notifications.[88/] NCTA's members, however, offer their customers – both residential and enterprise – services and resources that deter botnet threats, alert them to botnet attacks that occur, provide notifications to customers with infected devices, and offer assistance with remediation.[89/] In

---

84/ *Cf.* Draft Report at 33.

85/ *Id.* at 22-23.

86/ *See e.g.*, Comments of CTIA at 16-17; Comments of U.S. Telecom at 15; Comments of U.S. Chamber of Commerce at 5.

87/ Draft Report at 32.

88/ *Id.* at 11.

89/ Comments of NCTA at 11. One tool worth exploring that is being developed at the State and local level is the Cybercrime Support Network, a public-private, nonprofit collaboration designed to meet the particular challenges of cybercrime. Rather than over-burden already-strained E911 services, and reflecting the specialized expertise attendant to addressing cybercrime, CSN (https://cybercrimesupport.org/) envisions enabling cybercrime

addition, with the growth of cloud-based services, notifying end-users should not be viewed as the sole province of ISPs, but should include large edge platforms as well, as they are often in a better position to identify a given threat and alert their end users.[90/]

Lastly, the Draft Report should temper its assessment of the impact of the transition to IPv6.[91/] While ISPs are well underway in transitioning their backbone and customer networks to IPv6, reaping the full benefits of the transition requires autonomous system operators at the edge of the ecosystem to make that transition as well. Further, while completing the IPv6 migration will facilitate identifying end-points that send malicious traffic, it is not a panacea due to the prevalence of IP address spoofing and fast flux techniques. These ongoing challenges, however, underscore the value of the Draft Report's recommendation that the cybersecurity community take concrete steps to limit fast flux hosting.[92/]

V. THE DRAFT REPORT SHOULD REVISE PORTIONS OF ITS RECOMMENDATIONS THAT COULD BE READ AS SUPPORTING INCREASED REGULATION

While the Draft Report in most instances embraces voluntary mechanisms for coordinated action and industry-driven solutions to the issues it identifies and downplays the utility of prescriptive rules,[93/] there are a handful of sections that could be read to support traditional prescriptive regulation. For example, the Draft Report calls for the Federal government to "work with network providers to expand best practices on network traffic management across the ecosystem."[94/] NCTA shares the goal of advancing and expanding best

---

victims throughout the U.S. to call one number, 211, to reach support and connect to resources, including assistance from law enforcement and consumer protection officials.

90/ For example, many end users' primary email account is with an email provider other than their ISP.

91/ Draft Report at 19, 32.

92/ *Id.* at 34.

93/ *Id.* at 20 ("[R]egulations that are overly specific quickly become obsolete and can hinder innovation and limit consumer/user benefit. Compliance requirements or mandating specific regulations may address some risks, but often carry with them a greater burden while still leaving the broader ecosystem insecure").

94/ *Id.* at 30.

practices on network traffic management issues, and is actively engaged in such efforts. We caution, however, that direct Federal government involvement in the development and evolution of network traffic management best practices could have unintended adverse consequences for broader Internet governance and be counterproductive to Internet security and resilience. Network traffic management issues have been effectively addressed by private, inter-industry groups and standards-setting organizations for decades, even as network architecture, capabilities, and security issues have changed dramatically. Existing inter-industry venues addressing issues related to traffic management and automated and distributed attacks mechanisms include the IETF, BITAG, North American Network Operators Group (NANOG), the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), and the Society of Cable and Telecommunications Engineers (SCTE). In addition, private industry works closely with NIST and the NCCOE on many initiatives related to traffic management and cybersecurity. The IT and Communications Sectors should continue to work in a coordinated fashion with these entities, and consult on an ongoing basis with their sector-specific agency, DHS, to identify and implement innovative and continuously-evolving network traffic management best practices – driven primarily by stakeholders' operational experience in the dynamic Internet ecosystem – that bolster resilience against automated and distributed attacks.

Finally, the Draft Report also should revise language that could be read as endorsing sector-specific prescriptive security requirements related to marketing of, and security certification requirements for, IoT products.[95/] Prescriptive rules are ill-suited for bolstering resilience against botnets, because they are generally backward-looking and static in a circumstance in which delivering security requires companies to be agile, flexible and forward-

95/ *See id.* at 34

looking. Notably, the FTC data security regime lauded in the Draft Report eschews prescriptive rules in favor of a more agile and adaptable case-by-case assessment of the reasonableness of a company's data security measures based upon a range of criteria. Likewise, the Draft Report's suggestion that IoT device marketing concerns could be dealt with via sector-specific regulation is at odds with its later recommendations that a multi-stakeholder process be convened to develop voluntary measures for addressing IoT marketing and labeling issues that are based on market drivers.[96/] We strongly recommend that the Final Report unequivocally endorse the latter approach. The Draft Report correctly recognizes that the "private sector is best suited to the creation and maintenance of lightweight and agile mechanisms" to address IoT policy concerns, "but can often benefit from government's convening power."[97] The Final Report should drop or revise language conflicting with this important insight.

CONCLUSION

NCTA and its member companies appreciate the depth and scope of the Department of Commerce and the Department of Homeland Security's work on the complex problem of combatting botnets pursuant to the White House Executive Order. We urge the federal agencies to revise the Final Report in accordance with the recommendations discussed above. NTIA, NIST, and DHS also should move forward with efforts to address IoT device security profiles, IoT software development and updating issues, and enterprise network utilization of anti-botnet and DDoS threat tools and offerings. In addition, DHS should work with all 16 critical infrastructure sectors to enhance the value of shared threat information by identifying and targeting actionable data for each sector. Further, the Communications and IT sectors should

96/ *Compare* Draft Report at 34 and *id.* at 35-36.

97 Draft Report at 36.

continue to work with standards-setting bodies, industry organizations, and DHS on identifying and implementing network traffic management best practices for bolstering resilience.

Respectfully submitted,

/s/ Rick Chessen

Rick Chessen
Loretta Polk
NCTA – The Internet & Television Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

William A. Check, Ph. D.
Senior Vice President, Technology
and Chief Technology Officer

Matthew J. Tooley
Vice President, Broadband Technology

February 12, 2018