Before the
National Telecommunications and Information Administration
Washington, DC

In re

Promoting Stakeholder Action Against
Botnets and Other Automated Threats

Docket No. 180103005-8005-01

COMMENTS OF COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

Pursuant to the request for comments[1] (RFC) issued by the National Telecommunications and Information Administration (NTIA), the Computer & Communications Industry Association (CCIA) submits the following comments on the draft Report on "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats" prepared by the Departments of Commerce and Homeland Security.

CCIA represents large, medium, and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications, and Internet products and services. Our members employ more than 750,000 workers and generate annual revenues in excess of $540 billion.[2]

I. Introduction

CCIA commends the Department of Commerce for seeking stakeholder input through its request for comments on botnets and other automated, distributed threats for the security and

[1] *Notice, Request for Comment on Promoting Stakeholder Action Against Botnets and Other Automated Threats*, 83 Fed. Reg. 1342 (Jan. 11, 2018).

[2] A list of CCIA members is available at http://www.ccianet.org/members.

vitality of the digital ecosystem. Botnets, DDoS attacks, and other automated malicious activities pose substantial risk to the stability of the Internet and its continued viability as a platform for communication and commerce.

The draft Report prepared by the Departments of Commerce and Homeland Security offers a sober and comprehensive look at the digital ecosystem, its vulnerabilities, and the risks posed by automated distributed threats, accompanied by sound recommendations for improving system-wide resiliency and preventing future harms to users. While there are areas of the ecosystem and threat landscape that merit further examination, the Report is largely a successful blueprint for addressing automated, distributed attacks.

II. Ecosystem and Governance

The draft Report does a commendable job of cataloguing and evaluating the extensive components and domains of the digital ecosystem—from infrastructure and enterprise networks, to edge devices and home and small business networks—and the degree to which each can be both source and victim of distributed threats. However, within these domains, there are areas where further details as to the roles of policy bodies, consumers, and device-makers are necessary to shape a more secure future.

A. Infrastructure

The draft Report defines "infrastructure" as "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—for example, routers, switches, Internet service providers, DNS providers, content delivery networks, hosting and cloud-service providers . . . ."[3] Within that definition, there is a great deal to unpack. ISPs, CDNs, and cloud-service providers each deserve a more in-depth treatment than they currently receive, as significant contributors to botnet mitigation efforts with high levels of visibility into the wider ecosystem.

In assessing the current state of play of Internet infrastructure, the Report also describes the array of overlapping frameworks, techniques, and services that help to protect infrastructure-scale ecosystem participants from distributed threats, but makes little mention of the organizations and standards developed therein, beyond the definitional statement. The same is true in the Report's description of the future of Internet infrastructure, where only a single mention is given to "new infrastructure standards and practices,"[4] and not even one to the bodies that will define and disseminate them.

Given the transnational, borderless nature of the Internet and automated distributed threats, the convening and coordination capacities of international technical bodies will be essential to bring together the range of relevant ecosystem stakeholders to evaluate existing technical standards and practices, and develop new ones to respond to rapidly evolving threats. The Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN), Internet Governance Forum, and Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG) will be essential fora for these international multistakeholder conversations. Action 4.2 sketches out an outline of necessary activities in international engagement and standards development, but these organizations and their capabilities merit a more fulsome evaluation in this Report.

[3] Department of Commerce & Department 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 9-10 (Jan. 5, 2018).
[4] *Id* at 11.

B. Edge Devices and Home and Small Business Networks

Among the technical domains detailed, edge devices and home and small business networks receive the most attention in the draft Report. This is appropriate, given the frequency with which edge devices and small networks are used to create and serve distributed threats, and the degree to which their end users are targeted by malicious actors.

A significant portion of the Report's assessment of the current state of edge devices and home and small business networks focuses on the Internet of Things (IoT).[5] The report describes the relative unsophistication of security practices in IoT device manufacture and a lack of security expertise in the enterprise customers and consumers who use them.[6] Combined with their increasing proliferation in consumer and enterprise networks, IoT devices are highlighted as the primary present and future targets and sources of automated, distributed threats.

In drawing a path to a secure vision for edge devices and consumer networks, the draft Report wisely pinpoints consumer and manufacturer education, device lifecycle security, and secure product design practices as essential to improving reducing the attractiveness of IoT products and their installed networks for malicious automated code.

Central to effectuating lifecycle security and improved product design is a better understanding among consumers and manufacturers of the "things" that actually make up the Internet of Things. CCIA previously highlighted this in our comments in response to NTIA's 2016 RFC on fostering the advancement of the Internet of Things:

> "When consumers purchase a 'connected device,' they are getting both a good and a service—the physical device's connection often comes paired with a service operated remotely, often without a separate monthly service fee. True, the consumer may also see an application interface used to control or view data from a connected device, but that app is just an aspect of the services associated with that particular purchased 'thing.' It is

[5] *Id* at 15, 17-18.
[6] *Id.*

> important to ensure that the inherent duality found in IoT products is reflected in the context of any consumer protective best practices going forward."[7]

This is the chief educational burden that policymakers, regulators, and cybersecurity professionals face with respect to the security of edge devices and small networks. As consumers more regularly recognize that the IoT products they purchase are both goods and connected software services—with embedded applications no different than traditional software—they will begin to expect those devices to be secure at purchase and updated regularly once deployed. In response to these marketplace expectations, manufacturers will be more likely to disclose their patching and update lifecycles, maintain their IoT software and services, and design more secure products in the first place.

III. Goals and Actions

The draft Report's most important contribution is the series of concrete Goals and Actions it presents, which, if implemented, would improve resilience of the digital ecosystem to botnets and other automated threats. Each of the five Goals presented are laudable and achievable, but certain Actions are worth prioritizing because of the relative ease with which they may be accomplished, outsized impact, or both.

Industry and government should prioritize Actions that entail near-term changes in software development practices, government and industry collaboration, or consumer awareness-building, as they are low-hanging fruit that require comparatively less effort and build on proven, existing results. These include:

Action	Description
1.2	Industry adoption of software development tools and processes to reduce the incidence of vulnerabilities

[7] Comments of CCIA, Docket No. 160331306-6306-01, NTIA at 2 (2016), *available at* http://www.ccianet.org/wp-content/uploads/2016/06/CCIA-Comments-NTIA-IoT-RFC-FINAL.pdf.

1.4	Government and industry collaboration to ensure existing best practices, frameworks, and guidelines relevant to IoT are more widely adopted
2.2	Stakeholders, experts, and NIST should develop a Cybersecurity Framework Profile for Enterprise DDoS Prevention and Mitigation
3.2	User interface design for home IT and IoT should maximize security while reducing knowledge requirements for administration
4.3	Regulatory agencies should work with industry to ensure non-deceptive marketing
5.1	Private sector developed and provided voluntary informational tools for home IoT devices that focus on security and usability

In particular, Action 2.2, which recommends that stakeholders, experts, and NIST should develop a Cybersecurity Framework Profile for enterprise DDoS prevention and mitigation, might have the most impact if designed and implemented successfully. NIST's experience in convening experts to develop voluntary, best practices-based cybersecurity risk management frameworks will prove vital in helping enterprises of all sizes develop the capacity to combat DDoS attacks. A successful profile will be flexible and adaptable for enterprise networks in different sectors with varying risk profiles, rather than a compliance checklist focused on specific tools or solutions.

Certain Actions require new technology to be developed, shifts in network architecture, or international collaboration. These are more difficult to achieve, but some ought to be prioritized because of the significant improvement in ecosystem resiliency that might result from accomplishing these tasks. These include:

Action	Description
1.3	Industry should expedite the development and deployment of innovative technologies for prevention and mitigation of distributed threats
3.1	The networking industry should expand current product development and standardization efforts for effective and secure traffic management in home and enterprise environments

3.3	Enterprises should migrate to network architectures that facilitate detection, disruption, and mitigation of automated, distributed threats
4.2	The federal government should promote international adoption of best practices and relevant tools through bilateral and multilateral international engagement efforts.

V. Conclusion

CCIA appreciates the opportunity to submit these comments and participate in the efforts of the Departments of Commerce and Homeland Security to address botnets and other automated, distributed threats to the digital ecosystem. CCIA encourages the Departments to maintain their focus on setting out concrete, achievable technical goals, promoting government and industry collaboration to develop voluntary standards and best practices, and ensuring that the Internet remains a welcoming place for communication and commerce.

February 12, 2018

Respectfully submitted,

Bijan Madhani
Senior Policy Counsel
Computer & Communications Industry
Association
655 15th Street NW, Suite 410
Washington, D.C. 20006
(202) 783-0070