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

)
)
Promoting Stakeholder Action Against)
Botnets and Other Automated Threats) Docket No. 170602536–7536–01
)
)
)

COMMENTS OF THE
NCTA – THE INTERNET AND TELEVISION ASSOCIATION

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

Matthew J. Tooley
Vice President, Broadband Technology
Science & 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

July 28, 2017

Table of Contents

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

	)	
	)	
Promoting Stakeholder Action Against	)	Docket No. 170602536–7536–01
Botnets and Other Automated Threats	)	
	)	

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/] issued by the Department of Commerce on ways to reduce threats perpetuated by automated distributed attacks, such as botnets, and what role the U.S. government should play in this area.

INTRODUCTION AND SUMMARY

NCTA appreciates the opportunity to provide input on ways to strengthen protections against botnets and Distributed Denial of Service (DDoS) attacks. While botnets are not a new phenomenon, their global scale and the exponential growth in attack entry points and command and control devices for bot masters brought about by the growth of the Internet of Things (IoT) makes them a particularly potent and resilient threat to the entire Internet ecosystem. Meeting this threat effectively and successfully will require participation by and contributions from all portions of that ecosystem.

[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. 170602536–7536–01, 82 Fed. Reg. 27042 (June 13, 2017) ("RFC").

NCTA's member companies have been at the forefront of developing and implementing a broad range of practices and protocols for identifying and addressing cybersecurity risks and vulnerabilities. As the nation's largest providers of broadband Internet access service, cable companies work continuously to detect, prevent, and mitigate cyber threats in order to minimize their impact on broadband networks and consumers. NCTA's members have made significant investments designed to enhance network security, participated extensively in collaborative industry-based and public-private initiatives to bolster anti-botnet efforts, incorporated a range of recognized measures and protocols to protect against botnets and DDoS attacks, and developed innovative services that empower consumers facing cyber threats.

But cable broadband providers and other Internet service providers (ISPs) are only one part of an Internet ecosystem that includes 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. The rapid growth of the IoT, which is expected to increase the number of Internet-connected devices from 15 billion in 2015 to 50 billion by 2020,[3/] greatly expands the range of potential devices through which to launch and amplify cyber attacks. Business and enterprise networks continue to be highly attractive targets for botnets seeking to harvest or exploit valuable commercial data. And the relative lack of awareness and understanding of botnet threats among retail consumers can make them vulnerable to infections and unwitting enablers of cyber attacks. The problems associated with botnets and DDoS attacks are ecosystem-wide. While ISPs are able to stop a large number of attacks on their networks every day, neutralizing the full scope of botnet threats and DDoS attacks prevalent today requires collective action and holistic solutions.

[3/] *See infra* at n. 27.

The threats and challenges posed by botnets are exacerbated by gaps in existing efforts to combat them. The overwhelming majority of botnet attacks are launched from outside the United States,[4/] meaning that effective action to reduce such threats requires government leadership to foster globally-scaled solutions and international cooperation. In addition, cyber criminals are technologically sophisticated, extremely agile, and highly innovative. Anti-botnet efforts must keep pace with rapid changes in technology, threat vectors and strategies, and attack surfaces. Outmoded approaches to combatting botnet threats and DDoS attacks must be updated or discarded. Meanwhile, the quantum growth in IoT devices has introduced a whole new spate of gaps and vulnerabilities. Many such devices use outdated or insecure operating system software, lack the capability to receive software upgrades or vulnerability patches, and fail to take rudimentary steps to ensure secure connections with cloud servers and host platforms.

Finally, the "human element" continues to persist as a key gap in the effort to help secure network endpoints against cyber risks. End users that fail to change default passwords, update device software, or recognize spear phishing schemes and other forms of malware attack may inadvertently contribute to the spread and amplification of a botnet or DDoS attack. And this gap has widened with the proliferation of IoT devices that may operate for long periods of time without any user interaction or oversight.

There are, however, measures and initiatives to help address these gaps, and NTIA can play a significant role in promoting these efforts. First, NTIA should promote awareness and adoption of network defense measures that have proven to be demonstrably effective against the

[4/] *See e.g., Global DDoS Threat Landscape Q1 2017*, INCAPSULA.COM (Spring 2017), https://www.incapsula.com/ddos-report/ddos-report-q1-2017.html; *Akamai's State of the Internet Security Q4 2016 Report* (2017), https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf; *The 10 Worst Botnet Countries*, SPAMHAUS, https://www.spamhaus.org/statistics/botnet-cc/ (last visited July 26, 2017). *See also infra* at n. 42.

latest iteration of botnet threats and DDoS attacks, including those that seek to mask command and control infrastructure by employing techniques such as fast flux DNS or peer-to-peer (P2P) architecture. Such measures include IoT devices making use of network filtering and network isolation techniques, fast flux mitigation techniques, application of machine learning to botnet detection, distributed hosting of content (*e.g.*, content delivery networks, AnyCast), taking advantage of software-defined network capabilities, and adoption of Mutually Agreed Norms for Routing Security (MANRS).

Second, NTIA should convene a multi-stakeholder process to improve IoT device security. This process could build on the work of NTIA's IoT Security Upgradability and Patching multi-stakeholder process, as well as the recommendations on IoT device security from the Broadband Internet Technical Advisory Group (BITAG). This multi-stakeholder process could identify key security issues that arise over the entire life-cycle of IoT products and offer voluntary guidance to device makers on security capabilities that should be designed into their products.

Third, NTIA should enhance the security of network endpoints by launching an education and outreach campaign aimed at fostering greater awareness among end users of botnet risks and key preventative measures. Such an effort would be designed to address the human element, focusing especially on education and training for enterprise customers, since their networks are frequently targeted by malicious actors.

Fourth, NTIA should encourage continued examination of the extent to which uncertainty and liability concerns may hamper anti-botnet strategies and countermeasures. And, finally, the Federal government should take the lead on bolstering international efforts to combat botnets.

NCTA supports initiatives to encourage and enhance cooperation and information sharing between all relevant parties from both the public and private sectors that have a stake in the fight against botnets. With tens of millions of customers utilizing their networks every day, cable broadband providers have strong incentives to employ the most effective and practicable measures, tools, and protocols to protect their networks and their customers against botnet threats and DDoS attacks. Providing the private sector with continued flexibility to adapt to the ever-changing threat landscape continues to be an important guidepost for government policy. But it is equally important to employ a holistic, ecosystem-wide approach that reflects the interdependent nature of the problems associated with botnet threats and DDoS attacks.

I. THE CABLE INDUSTRY IS ENGAGED IN A WIDE RANGE OF ACTIVITIES TO COMBAT BOTNET THREATS

Preventing, detecting, and mitigating the barrage of botnet threats is a key business driver for cable broadband providers in serving their high-speed Internet customers. Increasing awareness and attention to botnets and DDOS attacks has led to considerable progress in detecting and defending against them. The fall-out from typical DDoS attacks can usually be contained today so that they do not totally impair the provision of critical services or the entire Internet ecosystem. While such attacks are now far less likely to completely disable critical infrastructure or the Internet as a whole, they can still cause significant harm to their targets, damage the devices of infected end users, and disrupt network-based services for consumers. As discussed below, the progress that has been made to date is the result of significant investment in state-of-the-art technologies and applications, industry collaboration, and providing customers with security offerings to foster a safe and secure network environment.

A. Cable Operators Are Employing Key Measures and Leading-Edge Tools for Combatting Botnets

The cable industry is committed to investing in and using all available tools to combat the continuing threat posed by botnets. Those tools, as described below, include the NIST Cybersecurity Framework, filtering and DDOS scrubbing techniques, system design and operations measures, and an array of customer tools and programs.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework. Cable companies continue to employ the NIST Cybersecurity Framework[5/] as a key resource in connection with their management of cybersecurity and assessment of their cyber defense protocols and practices. The voluntary and flexible nature of the Framework has been instrumental to its adoption and use by the cable industry, providing companies with flexibility to tailor the procedures and tools contained within the Framework to best comport with their particular network assets, business operations, and corporate structure. The Framework's five functions – identify, detect, protect, respond, and recover – offer a useful template for organizing risk management activities aimed at safeguarding networks against botnet threats.

Many of the key risk management processes and cyber defense measures referenced in the Framework were already incorporated into the existing business practices of many NCTA members even before adoption of the Framework. For smaller companies, the Framework – in conjunction with guidance on its use released in 2015 by the Federal Communications Commission's Communications Security and Interoperability Council (CSRIC)[6/] – has served as an important tool for organizing and strengthening cybersecurity practices and processes. More

[5/] FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, VERSION 1.0, NATIONAL INSTITUTE FOR STANDARDS AND TECHNOLOGY (2014).

[6/] 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 ("*CSRIC IV Working Group 4 Report*").

broadly, the Framework has provided a common taxonomy on cybersecurity matters that facilitates communication on these issues within individual companies and the communications sector, between the sector and government, and across various sectors of the economy.

Filtering and DDoS Scrubbing. Cable companies increasingly are employing a variety of filtering techniques to directly protect their network infrastructure. As noted by BITAG, network service providers[7/] seek to block inbound malicious traffic at its ingress points, such as at the network interconnection links to other ISPs, to prevent sources outside a company's network from sending traffic on these ports to the company's users.[8/] Cable providers also leverage the filtering capabilities built into the cable modems used by their customers to filter malicious traffic that may be originating from their customers' enterprise or home networks. Network service providers utilize a variety of filtering techniques to safeguard their routers, servers and other network infrastructure from botnet attacks.[9/] Bot masters routinely spoof the source IP address in their attack packets, particularly in network reflection incursions. As a result, most network service providers now engage in network filtering for spoofed IP addresses as a common best practice.[10/] Effective network filtering is not limited to ISP networks, it should be pushed all the way to the edge of the network with end-points supporting network filtering capabilities.

[7/] When used in this submission, "network service provider" or "network operator" refers not just to ISPs, but to any enterprise or organization that is operating a network with an assigned autonomous system number (ASN).

[8/] PORT BLOCKING, BROADBAND INTERNET TECHNICAL ADVISORY GROUP, at 13-14 (2013), http://bitag.org/documents/Port-Blocking.pdf. BITAG is a multi-stakeholder organization focused on bringing together engineers and technologists to develop consensus on broadband network management practices and related technical issues.

[9/] *Industry Technical White Paper*, COMMUNICATIONS SECTOR COORDINATING COUNCIL, at 16 (July 17, 2017) ("CSCC Technical White Paper").

[10/] For example, Comcast's implementation of network filtering for spoofed IP addresses is described in more detail here: *FAQs on Preventing Network Spoofing*, COMCAST (Mar. 13, 2014), http://networkmanagement.xfinity.com/#38.

Other techniques for filtering botnet traffic employed by cable broadband providers include Access Control Lists (ACLs), traffic policing, black holing, and sink holing. These measures are commonly used to neutralize the command and control traffic for client-server botnets. They are, however, less effective against more advanced botnets taking advantage of P2P architecture, encryption, and/or techniques like fast flux DNS to further shield their command and control origins from detection. Fast flux is used by bot masters to disguise the servers being employed to launch attacks by utilizing a continuously-changing rotation of compromised hosts acting as proxies.[11/]

Cable broadband providers also have invested in DDoS scrubbing systems which can be activated to filter out attack traffic from good traffic. Botnet victim traffic is diverted through scrubbers "on-demand" and then placed back onto the provider's network for transmission to its intended destination. Network service providers will use a combination of in-house scrubbing systems, third party scrubbing systems, and on-demand scrubbing capacity through contracts with third-party DDoS mitigation providers.[12/] The availability of incremental scrubbing capacity on the open market is critical because network service providers will not always have sufficient capacity to scrub all compromised traffic associated with high-volume attacks. Some cable broadband providers also may take advantage of the Flowspec[13/] capabilities of the Border Gateway Protocol (BGP) to dynamically filter readily identifiable compromised traffic flowing through network routers. Through Flowspec, BGP updates can be submitted and withdrawn expeditiously, thereby enabling faster mitigation and minimizing diversion of network traffic.

[11/] CSCC Technical White Paper at 16.

[12/] *Id.* at 16-17.

[13/] *Id.* at 17; Leonardo Serodio, *Traffic Diversion Techniques for DDoS Mitigation using BGP Flowspec* (May 2013), https://nanog.org/sites/default/files/wed.general.trafficdiversion.serodio.10.pdf.

System Design and Operation. Cable broadband providers employ numerous system design techniques to enable their systems to withstand attacks from, and damage caused by, malware, viruses, bots, and other cyber threats. For instance, they design their infrastructure to have spare capacity, redundant links, and redundant servers in order to have the ability to re-route traffic away from infrastructure that might be subject to a DDoS attack or under control of a botnet. Cable broadband providers have invested in network sensors, threat intelligence-gathering capabilities, and internal cybersecurity forensics, facilitating pattern-based detection and other threat-monitoring measures. These capabilities help repel sophisticated cyber incursions, including volumetric DDoS attacks.

Some cable broadband providers have deployed advanced inline security features that protect Internet-connected devices on the home network from online threats.[14/] Network architecture advancements made possible by Software Defined Network (SDN) capabilities and the use of automated machine-to-machine (M2M) sharing of cyber threat indicators could make it technically viable for network operators to automate the coordination of their botnet mitigations and reduce the response time to when a malicious bot is detected on a network or a botnet is initiating an attack.

For malicious traffic emanating from customer endpoints, cable broadband networks are designed to effectuate the key recommendations in the voluntary Anti-Bot Code of Conduct for Internet Service Providers (ABC for ISPs).[15/] These include identifying and detecting botnet activity in the ISP's network to determine potential bot infections on end-user devices; notifying end-users of suspected bot infections; providing remediation information to end-users to address and resolve bot infections; and collaborating with other ISPs regarding the source and methods

[14/] *See e.g.*, ARRIS SURFboard, http://www.arris.com/surfboard/mcafee/ (last visited July 28, 2017).

[15/] *ABCs For ISPs*, M^{3}AAWG, https://www.m3aawg.org/abcs-for-ISP-code (last visited July 28, 2017).

of attack and key mitigation and remediation tools. In addition, cable operators push automated, secure updates to company-provided customer premises equipment (CPE, *e.g.*, cable modems and home gateways) using the DOCSIS 3.1 Security Standard,[16/] which helps guarantee that CPE receives timely updates from trusted sources.

Cable operators and other ISPs also are exploring ways to leverage the features of SDNs to help mitigate attacks from botnets. SDNs provide the capability to dynamically create overlay networks.[17/] In tandem with other network partitioning techniques, SDNs offer the capability to dynamically create virtual lanes for different IP-based services. Under this approach, network service providers and IoT device makers can work together to develop end-to-end virtual lanes from the IoT device through the network to the cloud-based IoT service platform. These virtual lanes provide the capability to prevent an IoT device from becoming compromised by restricting its ability to communicate with unauthorized endpoints, thereby reducing its capacity to be employed as a client in a DDoS or botnet attack.[18/]

Cable operators are working with the Messaging, Malware and Mobile Anti-Abuse Working Group (M^3AAWG) to develop an application program interface (API), data storage, and open source reference implementation to enable network service providers to share DDoS threat indicators for the purpose of identifying sources of DDoS attack traffic. The M^3AAWG approach allows network service providers to share the source IP addresses for the inbound IP flows that their DDoS detection systems identify in an anonymous fashion with the network on which the DDoS attack originated, allowing network operators to clean up the sources of DDoS

[16/] *DOCSIS 3.1 Security Specification*, CABLELABS, https://apps.cablelabs.com/specification/CM-SP-SECv3.1 (last visited July 28, 2017).

[17/] *See* CSCC Technical White Paper at 19.

[18/] *See id.* at 19-20.

attack traffic.[19/] Cable operators also are supporting the Internet Engineering Task Force's (IETF) DDoS Open Threat Signaling (DOTS)[20/] working group that is a developing a protocol for DDoS mitigation platforms to exchange data.

Customer Tools and Programs. NCTA's members offer their customers – both residential and enterprise – services and resources that deter botnet threats, alert customers to botnet attacks that occur, provide notifications to customers with infected devices, and offer assistance with remediation. For instance, Comcast provides the Norton Security Suite at no charge to Xfinity internet service customers;[21/] Charter offers its Internet customers a free Security Suite[22/] and AntiBot Scanner;[23/] Cox provides McAfee at no charge as part of the Cox Security Suite Plus available to all Cox High Speed Internet customers;[24/] and Altice USA provides its broadband service customers with McAfee or Panda Antivirus offerings at no additional charge.[25/] In addition, Comcast has recently launched a service – the Xfinity xFi system – that enables users to create a base station in the home to connect and control users' iPads, smart appliances, and other IoT devices, as well as defend against phishing and malware.[26/] Cable operators also conduct consumer awareness and outreach, providing

[19/] *See id.* at 20-21.

[20/] *DDoS Open Threat Signaling (dots)*, IETF, https://datatracker.ietf.org/wg/dots/about/ (last visited July 28, 2017).

[21/] *Norton Security Suite for PC*, CONSTANT GUARD, http://constantguard.xfinity.com/products-and-services/norton-security-suite/(last visited July 28, 2017).

[22/] *Security Suite: Information and Support*, SPECTRUM, http://www.spectrum.net/support/internet/security-suite-information-and-support/ (last visited July 28, 2017).

[23/] *Security Suite: AntiBot Scanner*, SPECTRUM, http://www.spectrum.net/support/internet/antibot-scanner/ (last visited July 28, 2017).

[24/] *Cox Security Suite Plus powered by McAfee®*, COX, https://www.cox.com/residential/support/internet/cox-security-suite-plus.html (last visited July 28, 2017).

[25/] *About Internet protection powered by McAfee®*, OPTIMUM, http://optimum.custhelp.com/app/answers/detail/a_id/3720/kw/anti-virus/related/1/session/L2F2LzEvdGltZS8xNDk5ODA0MTExL3NpZC80UVJRT2xubg%3D%3D (last visited July 28, 2017); *Panda Antivirus*, SUDDENLINK, http://help.suddenlink.com/internet/Pages/PandaAntivirus.aspx (last visited July 28, 2017).

[26/] Dong Ngo, *Comcast launches Xfinity xFi, turning gateways into Wi-Fi systems*, CNET (May 7, 2017), https://www.cnet.com/news/comcast-launches-xfinity-xfi/ (last visited July 28, 2017).

customers with online security and safety resources via email, engaging in community events, and reaching out to blogs and newspapers with tips and information.

While the Internet of Things promises to add billions of connected devices to the Internet,[27/] the immense benefits of this transformation could be undermined by security concerns. NCTA members are developing new products to leverage ubiquitous computing and low power sensors. Many cable operators offer Internet-powered security and home monitoring systems to their customers.[28/] Cable operators also have created customer support programs to educate consumers about cyber threats, including botnets. Comcast has a dedicated Customer Security Assurance group to answer questions from customers about cybersecurity, consisting of nearly 100 trained professionals who offer support at no additional cost to Xfinity Internet customers. This group averages approximately 100,000 inbound/outbound calls every month.

B. Cable ISPs Are at the Forefront of Various Industry Organizations to Address Botnet Threats

Industry-led, multi-stakeholder organizations are critical in the ongoing battle to mitigate botnet attacks and strengthen the cybersecurity of critical infrastructure. Cable ISPs participate in a variety of organizations that engage in cybersecurity work, including CSRIC, M^{3}AAWG, IETF, and the BITAG. These industry-driven forums foster collaboration and initiatives among Internet stakeholders on a wide array of leading-edge cybersecurity best practices, including improving detection, mitigation and remediation of botnet attacks, domain name security, and Internet routing protection.

[27/] *Internet of Things will Deliver $1.9 Trillion Boost To Supply Chain and Logistics Operations,* CISCO.COM, (Apr. 15, 2015), at http://newsroom.cisco.com/release/1621819/Internet-Of-Things-Will-Deliver-1-9-Trillion-Boost-To-Supply-Chain-And-Logistics-Operations (estimating that more than 50 billion devices will be connected to the Internet by 2020 compared to 15 billion in 2015).

[28/] *See, e.g. Xfinity Home,* COMCAST, http://www.xfinity.com/home-security (last visited July 28, 2017).; *Cox Homelife,* COX, http://www.cox.com/residential/homelife.cox (last visited July 28, 2017).

NCTA member companies played a key role in compiling M^{3}AAWG's report on *Common Best Practices for Mitigating Large Scale Bot Infections in Residential Networks*,[29/] which is utilized across the communications industry as a common platform for building a network malware management strategy. M^{3}AAWG has been particularly active in developing voluntary practices that serve as a framework for botnet remediation, drawing from technical experts, researchers, and policy specialists from a broad base of ISPs, software companies, network equipment vendors and other key technology providers, academia and stakeholder organizations.[30/]

ISPs have long worked together to mitigate the impact of malware and botnets on the Internet ecosystem. Through the FCC's CSRIC III Working Group (WG) 7, cable ISPs helped develop and implement an Anti-Bot Code of Conduct, a voluntary, industry-driven effort to reduce malware activity.[31/] Cable industry engineers in network operations and management also have worked on botnet-related initiatives with the Quality and Reliability Committee of the Institute for Electrical and Electronics Engineers (IEEE), and the IETF. Cable industry technical personnel developed a seminal memorandum for IETF addressing bot remediation issues for ISPs.[32/] IETF contributed to the development of DNS authentication technologies like DNSSec and the BGP secure routing protocols. More recently, IETF released a paper summarizing a

[29/] Nirmal Mody, Michael O'Reirdan, Sam Masiello, and Jason Zebek, *Common Best Practices for Mitigating Large Scale Bot Infections in Residential Networks*, MESSAGING MALWARE MOBILE ANTI-ABUSE WORKING GROUP (July 2009) (*"Best Practices Report"*).

[30/] *See, e.g. Best Practices Report*; M^{3}AAWG Comments on "Cybersecurity, Innovation and the Internet Economy June 2011," (July 2011), http://www.maawg.org/sites/maawg/files/news/MAAWG_DoC_Internet_Task_Force-2011-08.pdf; *see also MAAWG Published Documents*, M^{3}AAWG, http://www.maawg.org/published-documents (last visited Sept. 26, 2014).

[31/] *See* CSRIC III Working Group 7 Final Report, *U.S. Anti-Bot Code of Conduct for Internet Service Providers (ISPs)* (March 2012), http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf.

[32/] Jason Livingood, Nirmal Mody, and Mike O'Reirdan, *Recommendations for the Remediation of Bots in ISP Networks* (March 2012), https://tools.ietf.org/html/rfc6561.

workshop on attack response, which included a discussion on effectively and safely scaling responses to botnet and DDoS attacks.[33/]

The cable industry also participated in the development of the BITAG recommendations on the security of IoT devices.[34/] The BITAG report provides guidelines to improve the security and privacy of IoT devices and minimize the costs associated with the collateral damage that would otherwise affect end users and ISPs. The report found that cybersecurity increasingly depends upon providing continuous security and automated software updates to Internet-connected devices, including IoT devices.

The cable industry's research and development consortium, CableLabs, is devoting substantial resources to cybersecurity research and innovation to support the continued growth in broadband services and products. It has a long history of securing devices within and beyond the cable industry, using a public key infrastructure (PKI).[35/] Leveraging this expertise, CableLabs is working to enhance IoT security through standards bodies and industry working groups including the Open Connectivity Foundation in such areas as device identity, authentication, authorization, delivery of software updates, and managing the complexities of device life cycles.

[33/] K. Moriarty and M. Ford, *Coordinating Attack Response at Internet Scale (CARIS) Workshop Report* (March 2017), https://tools.ietf.org/html/rfc8073.

[34/] *Internet of Things (IOT) Security and Privacy Recommendations*, Broadband Internet Technical Advisory Group (November 2016), https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf ("BITAG Report").

[35/] Since 1999, CableLabs has managed the specifications that require embedding digital certificates into cable devices, including cable modems, VoIP terminals, CableCARDs, and Uni-Directional Cable Products (UDCPs), at the time of manufacture. The certificates provide the basis for data confidentiality, content integrity, and hardware authentication. In addition, CableLabs, through its subsidiary – "Kyrio" – manages the PKI that issues the embedded digital certificates to cable device manufacturers. *See Security Services*, KYRIO, http://www.kyrio.com/security-services/ (last visited July 28, 2017). Through Kyrio, CableLabs also provides electric utilities with a managed PKI service that ensures device security for "smart grid" and specifically, automated demand response. *See OpenADR and Cyber Security*, OpenADR, http://www.openadr.org/cyber-security (last visited July 28, 2017). Kyrio provides a similar managed PKI service to the Wi-Fi Alliance to secure "Passpoint" certified hotspots. *See Certificate Authority Vendors*, Wi-Fi Alliance, http://www.wi-fi.org/certification/certificate-authority-vendors (last visited July 28, 2017). To date, Kyrio has issued over 400 million device certificates off of the CableLabs PKI. *See Security Services*, KYRIO, http://www.kyrio.com/security-services/ (last visited July 28).

Building on the cable industry's experience and the work of BITAG and other industry and government stakeholders, CableLabs developed and recently released a white paper, entitled "A Vision for Secure IoT." [36/] NCTA's Cybersecurity Working Group, which provides a forum for cable operators to discuss cybersecurity issues and share information and best practices, recently created a subgroup to focus solely on IoT security. Cable operators also participate in other groups addressing IoT security issues, including the Society of Cable Telecommunications Engineers (SCTE), IEEE, and the Alliance for Telecommunications Industry Solutions (ATIS).[37/]

Industry-led initiatives are underway to improve automated cyber threat information sharing. NCTA and its members were heavily involved in the development of the CSRIC V WG5 report that provided a series of recommendations to foster greater cybersecurity information sharing among communications sector companies.[38/] Those recommendations were informed by several information sharing use cases, including the Qakbot botnet. The report also highlighted some of the continuing challenges associated with ensuring that information sharing practices and protocols provide real-time, value-added benefits to companies combatting cyber threats such as botnets, particularly when it comes to integrating shared information into the operation of security tools and active defense measures:

> Quality of data and relevance to use cases also can be an impediment to fruitful information sharing. . . . The timeliness, scale or capacity, and integration of the information into various security tools also create technical challenges. Production of

[36/] *A Vision for Secure IoT*, CABLELABS (Summer 2017), http://www.cablelabs.com/vision-secure-iot/. This paper details the technical goals of an industry-led approach to IoT device security, as well as the governance goals of the development organization. The paper recommends that such an undertaking address such key issues as: (i) device identity; (ii) authentication, authorization, and accountability (onboarding); (iii) confidentiality; (iv) integrity; (v) availability; (vi) lifecycle management; and (vii) future (upgradable) security.

[37/] Since 2011, Comcast and the University of Connecticut have teamed up on a number of special projects centered on hardware security and the need for a more holistic approach to addressing the evolving challenges of cybersecurity, including the problems associated with botnets and DDoS attacks. In 2014, Comcast expanded its relationship with the University of Connecticut by establishing the Comcast Center of Excellence for Security Innovation, a dedicated security innovation laboratory aimed at provide training and education for the next generation of cyber professionals and developing cutting-edge security technologies, practices, and processes.

[38/] WORKING GROUP 5: CYBER SECURITY INFORMATION SHARING, COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL (March 2017).

> refined intelligence can take time and may not enable real time protection. On the other end of the spectrum, quickly produced intelligence can be fraught with peril leading to false positives and other negative outcomes. Also there are scaling challenges as information is integrated into security tools. At scale, a firewall can be overwhelmed with rules to block literally thousands of IP addresses. Meanwhile the collective set of botnets has millions of IP addresses they cycle through daily. Finally integrating the data into an intrusion detection system or firewall can create additional challenges and further development work.[39/]

NCTA members continue to work to improve collaboration and coordination to reduce the response time to cyber threats and to ensure that shared threat information is both timely and targeted. The Cybersecurity Information Sharing Act (CISA), enacted in 2015, and the rollout of the DHS Automated Information Sharing (AIS) are helping to facilitate machine-to machine (M2M) initiatives. DHS' AIS platform also provides an opportunity to improve and enhance the timely and tailored sharing of cyber threat indicators to meet the needs of the recipient.[40/]

NTIA should continue to promote and support these types of public-private partnerships and inter-industry groups working on anti-botnet initiatives, incorporating input from all segments of the broadband ecosystem.

II. ANTI-BOTNET EFFORTS SHOULD ACCOUNT FOR EXISTING GAPS AND STEER RESOURCES AND EFFORTS AWAY FROM APPROACHES THAT HAVE BECOME OUTDATED OR INEFFECTIVE

While the measures, practices, and collaboration initiatives discussed in Section I reflect a diverse array of Internet technologies and architectures, broader collaboration among stakeholders is needed, as cyber attacks have been observed and mapped to every layer of Internet protocols and against every category of participants in the ecosystem.[41/] The threat landscape is constantly changing, and there are gaps in the existing approaches. For example,

[39/] *Id.* at 16.

[40/] *Automated Indicator Sharing (AIS)*, DEPARTMENT OF HOMELAND SECURITY (June 21, 2016), https://www.dhs.gov/ais.

[41/] *CSRIC IV Working Group 4 Report* at 26; *see also id.*, Section 9.7, Cyber Ecosystem and Dependencies subgroup report at 321.

while botnets and DDoS attacks used to employ attack vectors that relied primarily upon ISP networks, malicious actors increasingly are targeting cloud storage providers and hosting services, because these entities may have more available bandwidth and CPU to exploit and therefore make a better platform for launching attacks. The government's anti-botnet efforts should account for existing gaps and technical and operational challenges, and should move away from approaches that have proven to be outdated or no longer effective. Some key gaps and archaic practices are highlighted below.

First, the overwhelming majority of malicious botnet traffic aimed at targets in the United States originates outside our borders, making filtering close to the source impossible for U.S. companies to achieve alone.[42/] Effective filtering instead requires resource intensive cooperation and collaboration between governments and with international network operators and edge providers, cloud and hosting platforms, and other entities operating autonomous networks (enterprises, educational institutions, governments, organizations, etc.). Botnet takedowns similarly require careful coordination between many stakeholders across international borders. Moreover, due to the international nature of the threat, protecting against botnets requires that Internet-connected devices adhere to security standards at a global level, and not just on a country-by-country basis. Because botnets operate on a global scale and generally are launched from outside the United States, an international strategy and close coordination with foreign governments is essential.

Second, malicious cyber actors are continually adapting to changes in technology and developing new strategies and attack vectors to evade detection and circumvent defensive

[42/] *See supra* at n. 4. *See also The Impact of IP Access Control Lists on Firewalls & Routers – A business case for nextgen perimeter security*, TECHGUARD SECURITY (2012), https://bandurasystems.com/assets/files/Impact-of-ACLs-on-Routers_Firewalls_PoliWall_Whitepaper1.pdf.

measures. Their seemingly boundless capacity for innovation and adaptation presents a number of technical challenges. For example, botnets are now using P2P architectures to operate, making it harder to block the command and control traffic. Rather than conform to a conventional structure of a centralized control server and distributed client bots across the Internet, P2P bots can serve as both a command distribution server and a client which receives commands. Anti-botnet strategies and tools need to account for the multiplicity of command centers – and their ability to be disguised as clients – that P2P technology offers bot masters.

Third, there is diminished value in simply relying upon shared blacklists of suspect IP addresses or URLs as a mechanism for combatting botnets. The increased use of techniques such as fast flux DNS discussed earlier has emerged as a key method by which malicious actors and bot masters camouflage their architecture. By effectively hiding the devices and services executing malicious attacks from detection, fast flux makes severing a bot's contact with the command and control servers difficult or impossible to accomplish by IP address filtering alone.

In 2008, the Internet Corporation for Assigned Names and Numbers (ICANN) Security and Stability Advisory Committee (SSAC) released a security advisory setting forth mitigation recommendations that help neutralize fast flux DNS techniques.[43/] Included in the SSAC findings was a recommendation encouraging ICANN, registries, and registrars to consider the fast flux mitigation practices in the advisory. Since then, advancements in machine learning have been applied to detecting botnets using fast flux-like techniques to obfuscate their infrastructure, thereby facilitating automation and integration into botnet detection systems.[44/]

However, fast flux DNS exposes just one of the flaws associated with over-reliance on blacklists. Botnets often do not have a static IP address, and most ISPs use dynamic IP

[43/] *See* CSCC Technical White Paper at 24; *SAC 025 SSAC Advisory on Fast Flux Hosting and DNS*, SSAC (March 2008), https://www.icann.org/en/system/files/files/sac-025-en.pdf.

[44/] *See* CSCC Technical White Paper at 25.

addresses. Further, bot masters often deploy command and control servers from a server platform with a single IP address shared by multiple hosts. In other words, the command and control server may live on a server alongside hundreds or thousands of legitimate domains, and it may even be a legitimate domain that has been compromised. In addition, the command and control servers may have a pool of IP addresses or shared hosts that they rotate through. These techniques can limit the value of malicious IP address information shared with ISPs if such information is provided without an accompanying time stamp. Botnets may also employ anonymizing proxy servers that mask the true source of the attack, making it difficult to identify the best place to mitigate the malicious traffic.

Given the above, blocking command and control traffic based upon IP addresses identified as the source of botnet activity is no longer a reliable or robust method of combatting botnets. Moreover, this problem is exacerbated by potential risks and liability associated with implementing block requests that may have inaccurate IP address information, lack a time stamp for dynamic addresses, or otherwise be unreliable or unverified. Neutralizing botnet attacks may require swift deployment of countermeasures, but uncertainty about the implications of taking certain actions can lead to delay in situations in which a rapid response is critical.[45/]

Fourth, the massive proliferation of Internet-connected devices in recent years significantly expands the potential sources of incursion by botnets. Recent events have demonstrated that large networks of IoT devices compromised by bots when connected to high-speed Internet connections can cause damage. For example, in Fall 2016 the Mirai botnet exploited weak security in many IoT devices to cause a massive and disruptive DDoS attack against DNS provider Dyn. The Mirai botnet proliferated by seizing control of insecure IoT

[45/] *See infra* at Section III.D.

devices to propagate large volumes of traffic to Dyn domains, thereby degrading service for Dyn's customers, including Amazon, Twitter, Netflix and Spotify.[46/]

Insecure IoT devices are offering new points of entry and a new source of command and control infrastructure for bot masters. Some IoT devices ship with software that either is outdated or becomes outdated over time. Other IoT devices may ship with more current software, but vulnerabilities may be discovered later. Vulnerabilities that are discovered throughout a device's lifespan may make a device less secure over time unless it has a mechanism to update its software. Thus, software patching capability is critical, but manufacturers of connected devices often lack effective update and upgrade paths for installed products. The BITAG Report offers a plethora of useful recommendations for bolstering IoT device security, including the following:

- IoT devices should ship with reasonably current software free of severe, known vulnerabilities. IoT device makers or service providers should design processes to ensure automatic updating of IoT device software, without any type of user action or user opt-in.

- IoT devices should be secured by default and not use easily guessable user names and passwords. Authentication for remote access should be secured.

- Manufacturers should test the security of each device with a range of possible configurations and interfaces and should prevent users from configuring the device in a way that makes it less secure.

- All communication for device management should take place over an authenticated and secured channel. Any sensitive or confidential data should reside in encrypted storage.

- Each device should have unique credentials and support a secure mechanism by which credentials can be updated.

- Device manufacturers should close unnecessary ports, such as telnet, and should use libraries and frameworks that are actively supported and maintained whenever possible.

[46/] *See e.g., Mirai: what you need to know about the botnet behind recent major DDoS attacks*, SYMANTEC OFFICIAL BLOG (Oct. 26, 2016), https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks; *Major DDoS attack on Dyn disrupts AWS, Twitter, Spotify and more*, Datacenter Dynamics (Oct. 21, 2016), http://www.datacenterdynamics.com/content-tracks/security-risk/major-ddos-attack-on-dyn-disrupts-aws-twitter-spotify-and-more/97176.fullarticle.

- IoT devices that have implications for user safety should continue to function if Internet connectivity – or connectivity to the back-end – is disrupted. IoT devices/services that depend on or use a cloud back-end should continue to function, even if in a degraded or partially functional state, when connectivity to the cloud back-end is interrupted or the service itself fails.

- IoT devices should support best practices for IP addressing and the use of the Domain Name System.[47/]

The strength and utility of these recommendations, however, are only as robust and effective as the degree to which they are adopted by device makers and stakeholders across the Internet. NTIA is already engaged in important work aimed at addressing some of these issues through its IoT Security Upgradability and Patching multi-stakeholder process,[48/] but there is more to be done to deter proliferation and amplification of botnet threats and DDoS attacks via IoT devices.

Fifth, services and solutions aimed at protecting end users from botnet infections are insufficiently geared toward prevention. Traditional anti-virus products function by detecting and quarantining or removing malicious files. Some of these products are becoming obsolete due to new botnet strategies that employ fileless malware – *i.e.*, malware that does not drop files into the local host system, but rather resides in a device's Random Access Memory and propagates by co-opting the device's legitimate operating system resources. More importantly, the market's orientation toward post-infection product offerings leaves a gap in terms of preventive measures and tools, failing to grapple with the "human element" that is critical to the amplification of botnets. The rapid spread of the Mirai botnet was linked to vulnerabilities in Linux devices, which were exacerbated by device users that never changed default passwords or

[47/] *See BITAG* Report at iv – vii; *id.* at 18-23.

[48/] *Multi-stakeholder Process; Internet of Things (IoT) Security Upgradability and Patching*, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (July 18, 2017), https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

updated firmware.[49] Symantec Corporation reports that "[m]alicious emails were the weapon of choice for a wide range of cyber attacks" during 2016, in part because email "doesn't rely on vulnerabilities, but instead uses simple deception to lure victims into opening attachments, following links, or disclosing their credentials."[50]

There is clearly a gap in end user education and awareness that cannot completely be addressed by the marketplace alone, but which is absolutely critical to endpoint protection. That gap encompasses both enterprise customers and residential users. Indeed, while enterprise customers may, in many respects, be more sophisticated purchasers of communications and IT services, they often forego elementary security tools that could lower their exposure to cyber risks. For example, end user transit customers often do not have provisions in place with their transit provider for the transit provider to filter out the bad traffic. Network operators of all sizes (ISPs, enterprises, governments, academic institutions, etc.) should ensure they have provisions in place with their Internet transit providers and peering networks to provide for upstream filtering and scrubbing of malicious traffic.

The gaps highlighted above underscore the challenges to anti-botnet efforts arising from a combination of near continuous changes in technology, highly sophisticated and innovative cyber criminals, an ever-broadening attack surface ushered in the by the IoT, and a deficit in end user awareness and understanding of the nature of the threat and how to protect themselves. The measures and initiatives suggested below in Section III are designed to help address these gaps.

[49] *RSA 2017: SophosLabs sees spike in Linux-IoT malware*, NAKED SECURITY (Febr. 13, 2017), https://nakedsecurity.sophos.com/2017/02/13/rsa-2017-sophoslabs-sees-spike-in-linux-iot-malware/; *Linux Malware on the Rise: A Look at Recent Threats*, LINUX.COM (July 7, 2017), https://www.linux.com/news/2017/7/linux-malware-rise-look-recent-threats.

[50] SYMANTEC CORPORATION, INTERNET SECURITY THREAT REPORT (2017) ("*Internet Security Threat Report*") at 8.

III. NTIA SHOULD PROMOTE A HOLISTIC APPROACH TO DEALING WITH BOTNET THREATS AND SPUR MEASURES AND INITIATIVES TO BOLSTER EXISTING EFFORTS AND ADDRESS KEY GAPS

The gaps and limitations flagged in Section II demonstrate the need for NTIA to embrace a holistic approach to combatting botnet threats. No single segment of the Internet ecosystem, including ISPs, can combat botnet threats on its own. The technical measures, public-private partnership efforts, and policy initiatives discussed below are aimed at strengthening the nation's overall defenses against botnets and DDoS attacks, boosting awareness and education regarding these threats, and promoting effective policies and initiatives for combatting them.

A. NTIA Should Highlight Technical Measures That Can Help Address the Latest Iterations of Botnet Threats

NTIA should promote awareness of technical measures that make full use of the latest advances in technologies and reflect contemporary strategies and methods of attack by malicious actors. These include:

Application of Machine Learning and Big Data to Detect Botnets. The Internet ecosystem should move away from manually reverse engineering botnet domain generation algorithms and begin applying big data frameworks and machine learning (*i.e.*, artificial intelligence) to automate the real-time detection of botnets using fast flux, encryption, and other techniques to mask their infrastructure.[51/]

Adoption of Mutually Agreed Norms for Routing Security (MANRS). MANRS[52/] constitutes an industry-led initiative to memorialize a consensus group of shared values for network operators into a set of definitions and ideal behaviors. MANRS endorses implementation of anti-spoofing filtering to prevent packets with incorrect source IP addresses

[51/] *See* CSCC Technical White Paper at 30.

[52/] *Mutually Agreed Norms for Routing Security (MANRS)* (Sept. 08, 2016), http://www.routingmanifesto.org/manrs/.

from entering or leaving the network. Over 45 network operators currently participate in MANRS.[53/]

Adoption of the Fast Flux Mitigation Techniques in SAC 025 SSAC Advisory on Fast Flux Hosting and DNS. ICANN, registries and registrars should consider and adopt the fast flux mitigation techniques in the SSAC advisory.[54/]

Use of Network Filtering and Network Isolation Techniques. IoT device manufacturers and IoT service providers should ensure that their devices use – and interoperate with – network isolation and/or network based filtering to prevent infected devices from inflicting harm on others in the Internet ecosystem.[55/]

Distributed Hosting. Techniques such as Anycast or content delivery networks/content distribution networks can mitigate DDoS attacks by geographically distributing hosts. Due to geographic distribution, the magnitude of the DDoS attack needs to be significantly larger to succeed at disrupting the site or service.[56/]

Use of Software Defined Network Capabilities. As discussed in Section I.B, SDN capabilities potentially can be used to dynamically create virtual end-to-end networks on demand for services, ensuring that a compromised IoT device cannot communicate with unauthorized endpoints.[57/]

Incorporation of Automated Software Updates and Patches for Devices. Ensuring that all end-points are all running up-to-date software with the latest security patches and updates will help reduce the number of infected and compromised end-points on the Internet.[58/]

[53/] *See* CSCC Technical White Paper at 27.

[54/] *See id.* at 30.

[55/] *See supra* at 7-8; CSCC Technical White Paper at 31.

[56/] *See* CSCC Technical White Paper at 17.

[57/] *See supra* at 9-10; CSCC Technical White Paper at 27.

[58/] *See* CSCC Technical White Paper at 30-31.

Completion of the Migration to IPv6. Completing the migration to IPv6 will reduce the dependency on Network Address Translation and will allow devices to have a unique address, making it easier to identify end-points sending malicious traffic.[59/]

Development of Information Sharing Platforms Capable of Providing Targeted, Reliable and Actionable Data Regarding Compromised Network Endpoints. Information sharing platforms that share cyber threat indicators should be tailored to meet the needs of the recipient. Cyber threat information needs to be timely and targeted to be effective.[60/] Network service providers need a single, highly reliable, near term indication that an IP address has generated malicious traffic or has been scanned to show exposed vulnerable services and the compromised hosts.

B. NTIA Should Convene a Multi-Stakeholder Effort to Develop Guidance for IoT Security

As discussed in Section II, insecure IoT devices are offering new points of entry and a new source of command and control infrastructure for bot masters. IoT devices on the market today may be subject to a number of vulnerabilities, including shipping with out of date software containing known vulnerabilities and lacking the capability for an automated software update; protection only by factory default or hardcoded user names and passwords; unauthenticated communications; unencrypted communications; and lack of mutual authentication and authorization. The BITAG Report has a number of actionable recommendations that could address these and other flaws in IoT devices.[61/] But due to the global scale of botnet threats, the efficacy of these recommendations depends upon their widespread adoption across the ecosystem.

[59/] *See id.*at 29.

[60/] *See id.*; *see supra* at 15-16, 18-19.

[61/] *See supra* at 20-21.

To this end, NTIA should convene a multi-stakeholder effort to provide voluntary guidance on security for IoT products. Building on the current NTIA initiative around IoT security upgradability and patching, this effort could address security issues as they arise over the entire life-cycle of IoT products – including product development, security by design, deployment, upgrades and maturity, and obsolescence. The objective would be to provide guidance to device makers, so that they are apprised of the range of security measures and capabilities that should be designed into IoT products. The initiative also would provide IoT vendors greater clarity with regard to the security outcomes and level of security performance that should be reflected in products they develop and acquire for the market.

An NTIA-led multi-stakeholder initiative on IoT device security also could focus on ways to encourage incorporation of the most up-to-date and advanced measures and protocols for enhancing IoT security.[62/] For example, the IETF's Manufacturers Usage Description (MUD) protocol relies upon network isolation capabilities and gateway-stored behavioral profiles that define and limit the functions and communications paths of devices located behind home routers.[63/] Home-based IoT devices would only be able to communicate with white-listed destinations, thereby limiting device vulnerabilities. In addition, the multi-stakeholder process could explore ways in which cloud-based platforms can be better designed to mitigate security vulnerabilities in the IoT devices they communicate with. Amazon has indicated that it is providing an API for its cloud that is specific for IoT devices and aimed at securing the link between the device client and the cloud host.[64/] The NTIA process could examine whether cloud

[62/] *See id.;* CSCC Technical White Paper at 30-31.

[63/] *See e.g.*, *Scaling Security for The Internet of Things with MUD*, THE SECURITY LEDGER (Oct. 14, 2016), https://securityledger.com/2016/10/mud-scaling-security-for-the-internet-of-things/; E. Lear, Cisco Systems, R. Droms, D. Romascanu, *Manufacturer Usage Description Specification draft-ietf-opsaw-mud*-05 (Mar. 8, 2017), https://tools.ietf.org/html/draft-ietf-opsawg-mud-05.

[64/] *See How AWS IoT Works*, AMAZON WEB SERVICES http://docs.aws.amazon.com/iot/latest/developerguide/aws-iot-how-it-works.html (last visited July 28, 2017); *AWS* storage providers and hosting platforms can do more to integrate security into their links and connections with IoT devices, both to reduce device vulnerability and to harden the cloud/host server against ingesting malware from infected client devices.

NTIA is well-suited to guide a multi-stakeholder initiative on IoT device security, particularly given its experience with the security upgradability and patching group. The Department of Commerce has recognized that "an industry-led, bottom-up, consensus-based approach to standards development is necessary to realize the benefits of the" Internet of Things.[65/] Achieving consensus on the best means of fostering integration and interoperability of IoT devices, network and data systems, cloud-based data storage and service hosting platforms, business processes, and personnel managing product and service provision will be important to realizing the promise of the IoT. Today, the technical specifications of IoT devices differ significantly – from processing capacity, memory, and size to functional sophistication. Integrating big data analytics algorithms and capabilities with IoT devices will be critical to transforming raw data into useful, actionable intelligence to serve consumers. In short, there is a considerable range of interdependencies involved in addressing and solving the issues of IoT device security that cannot be bifurcated into severable industry or sector segments. The effort to boost IoT device security requires collective action and a well-organized response across the entire Internet ecosystem, and NTIA's subject matter expertise and experience with convening a multi-stakeholder proceeding make it well-positioned to steer such an undertaking.

IoT Documentation, AMAZON WEB SERVICES, https://aws.amazon.com/documentation/iot/ (last visited July 28, 2017).

[65/] FOSTERING THE ADVANCEMENT OF THE INTERNET OF THINGS, DEPARTMENT OF COMMERCE, INTERNET POLICY TASK FORCE & DIGITAL ECONOMY LEADERSHIP TEAM, at 47 (Jan. 2017), https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf ("Green Paper"). As discussed in its comments on NTIA's IoT Green Paper, NCTA members support the efforts of the Department of Commerce to bring private sector experts together with policymakers to define security principles and encourage the implementation of best practices. Green Paper at 2, 41.

C. NTIA Should Lead a Campaign Aimed at Securing Network Endpoints through Greater Awareness and Education about Steps to Reduce the Risks of Botnets and DDOS Threats

While the malicious actors launching botnets and DDoS attacks possess technical sophistication, the breadth and impact of successful attacks are almost invariably amplified by human error and preventable mistakes. The most damaging attacks frequently rely upon a combination of psychology and technology, as cyber criminals exploit human habits and biases. For instance, social engineering attacks – *i.e.*, attacks that use manipulation, influence, or deception to get a person to take action that benefits the attacker – can be carried out by email and can have huge impacts. These attacks may appeal to human motivations such as ego, empathy, financial need, curiosity, and job duties, "with the goal of getting the target to either click on a link that redirects the target to a malicious website or open an attachment that contains malware."[66/] Moreover, email malware rates are increasing – up from 1 in 220 emails sent in 2015 to 1 in 131 emails sent in 2016.[67/] And social engineering attacks are increasingly tailored to a recipient individual or company, "appear[ing] to come from . . . a source they would trust, or contain[ing] information that would be relevant to the target's professional role."[68/] The FBI reports that business financial scams perpetrated over email, often using spear-phishing, have resulted in over $3 billion in losses since January 2015.[69/] According to Symantec Corporation, over 400 businesses are targeted by such scams every day.[70/]

[66/] Lillian Ablon, *Social Engineering Explained: The Human Element in Cyberattacks*, THE RAND BLOG (Oct. 20, 2015), https://www.rand.org/blog/2015/10/social-engineering-explained-the-human-element-in-cyberattacks.html ("*Social Engineering Explained*").

[67/] *Internet Security Threat Report* at 24.

[68/] Solange Deschatres, *Social Engineering: Attacking the Weakest Link in the Security Chain*, SYMANTEC (Jul. 8, 2014) https://www.symantec.com/connect/blogs/social-engineering-attacking-weakest-link-security-chain ("*Social Engineering: Attacking the Weakest Link in the Security Chain*").

[69/] *See Business E-Mail Compromise*, FBI (Feb. 27, 2017) https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise.

[70/] *See Internet Security Threat Report* at 26.

Cyber criminals have also begun to incorporate offline tactics into their attacks, using phone calls to acquire information by, for instance, posing as tech support personnel.[71/] Not all attacks require an individual to actively click on a link or open a document. In fact, some depend on individuals failing to take action – for instance, neglecting to update software. Others may take advantage of an unsuspecting individual's unintentional data disclosure – perhaps the result of sending a sensitive email over an unsecured network or keeping a list of difficult to remember passwords next to one's computer.[72/] In short, the human element is a key contributing factor that can often open the door to serious harm from botnets and others forms of cybercrime.

Education is key to combatting attacks that exploit human behavior.[73/] It may only take one error – a single employee clicking on a link in a malicious email – for an attacker to gain access to a large enterprise's internal network.[74/] While the marketplace is working to provide tools, products, and services that help network providers, enterprises, and consumers deal with the fall-out, there is still considerable work to be done in terms of boosting awareness of botnet risks and front-loading preventative steps. Further, the exponential growth of IoT devices has widened the awareness deficit regarding botnets and DDoS attacks, as consumers and enterprises employ devices they do not routinely interact with but which are still susceptible to infection.[75/]

[71/] *See Social Engineering: Attacking the Weakest Link in the Security Chain*.

[72/] *See* Steve Durbin, *Insiders are today's biggest security threat,* RECODE (May 24, 2016) https://www.recode.net/2016/5/24/11756584/cyber-attack-data-breach-insider-threat-steve-durbin ("*Insiders*").

[73/] *See, e.g., Social Engineering Explained*; Mav Turner, *The Human Element of Cybersecurity,* SECURITY MAGAZINE (May 26, 2015), http://www.securitymagazine.com/articles/86387-the-human-element-of-cybersecurity ("*The Human Element of Cybersecurity*").

[74/] *See* Ian Barker, *Threat hunting and why combating cyber attacks needs a human element [Q&A],* BETANEWS (Feb. 2017), https://betanews.com/2017/02/03/threat-hunting-qa/.

[75/] *The Botnet That Broke The Internet Isn't Going Away*, WIRED (Dec. 9, 2016), https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/ ("One reason Mirai is so difficult to contain is that it lurks on devices, and generally doesn't noticeably affect their performance. There's no reason the average user would ever think that their webcam—or more likely, a small business's— is potentially part of an active botnet. And even if it were, there's not much they could do about it, having no direct way to interface with the infected product").

NTIA and DHS should take the lead in organizing education and awareness campaigns aimed at enlisting end users to help secure Internet endpoints against botnet threats and DDoS attacks via preventative measures that promote good cyber hygiene. NTIA and DHS should also help organize initiatives to promote an enterprise culture that emphasizes employee awareness and training aimed at preventing botnet attacks, as well as appropriate response protocols.

Education and outreach toward enterprise customers would be especially worthwhile, since their networks are of particular value to malicious actors. Enterprises should be encouraged to address network security and cyber hygiene in a manner similar to how they approach workplace safety – through training, awareness programs, and built-in job functions. In addition to benefiting from greater education and training on anti-botnet prevention measures that their employees could follow, many enterprises also would benefit from greater awareness of and exposure to resources and tools available to them in the market to combat DDoS attacks and botnet threats. As noted above, many ISPs and other third parties offer DDoS mitigation tools and services to enterprise customers. Large end-users also should ensure they have provisions in place with their Internet transit providers and peering networks to provide for upstream filtering and scrubbing of malicious traffic. Many enterprises have been slow to implement proven defensive measures such as BCP-38, and may be unaware of the value of taking such a step. There are new information sharing resources, such as the DDoS online threat signaling protocol (DOTS) being developed by IETF, that are geared toward promoting information exchange between service providers and enterprise users regarding DDoS attacks.

By increasing the collective knowledge and vigilance of all end users, an NTIA/DHS-led education and outreach campaign aimed at fostering greater awareness of botnet risks and key preventative measures, with a special focus on enterprise customers, would augment the security of network endpoints. Such a campaign could be undertaken in tandem with other government initiatives to harden defenses against botnets, such as increased support for research and development on botnet prevention, detection, and remediation tools and technologies.

D. NTIA Should Promote Efforts to Strengthen Collaboration with Law Enforcement

While network service providers recognize that effective anti-botnet and DDoS mitigation strategies may require blocking, quarantining, or sink-holing traffic to and from suspect IP addresses, such action implicates a range of security, operational, customer impact, and legal considerations. ISPs have worked with the FBI-National Cybersecurity Industry Joint Task Force (NCI-JTF) and InfraGuard, which are involved in botnet takedowns, repelling DDoS attacks, and addressing other cyber threats – and expect to continue to do so in the future where appropriate.[76/] Federal law enforcement officials have some leeway to conduct or direct botnet takedown activities under the protection of judicial orders, though even that authority is limited to instances in which botnets are used to commit violations of fraud or wiretapping statutes.[77/] Often, however, the government will only undertake such action in response to a specific request, but concerns about potential consequences from vulnerability disclosure may affect the initiation or timing of such requests. The development of clearer procedures and protocols for expediting law enforcement assistance with botnet takedowns is an area worthy of further exploration.[78/]

For private sector entities, the potential for litigation can be impediments to utilization of counter-measures and threat mitigation practices that may have effects that go beyond the entity's network or that impact devices of innocent third parties – notwithstanding the need for,

[76/] *See* CSRIC V WG 5 Report, at 13.

[77/] Statement of Leslie R. Caldwell, Assistant Attorney General, Criminal Division, Department of Justice, "Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks," Senate Judiciary Committee, Subcommittee on Crime and Terrorism, at 10-11 (July 15, 2014).

[78/] *See* CSCC Technical White Paper at 30.

and efficacy of, such measures to counter an attack. While enactment of the Cybersecurity Information Sharing Act (CISA) has helped to clear away some of the legal underbrush that inhibited cyber threat information sharing, the statute only authorizes – but does not offer liability protection for – operation of defensive measures,[79/] which leaves companies employing such measures open to potential liability on various legal grounds, including tort and common law causes of action. Further, CISA's authorization to conduct defensive measures excludes activities that cause harm to third-party networks (or information thereon) that do not consent to the operation of such measures on their networks.[80/] Thus, while swift decision-making and rapid deployment of countermeasures may be critical to containment of a botnet or DDoS attack, the need to assess liability exposure associated with taking certain actions can cause delay and uncertainty in situations where time is of the essence.[81/]

The breadth and depth of most private sector-conducted anti-botnet activities and defensive measures undertaken have emerged without any express guarantee of liability protection. Both government and industry should continue to examine ways in which the legal landscape may be affecting anti-botnet efforts.

E. The Federal Government Should Take the Lead on Strengthening International Efforts to Combat Botnets

The Federal government should take the lead on bolstering international efforts to combat botnets. As discussed previously, the overwhelming majority of botnet traffic originates outside the U.S.[82/] And private actors are not the only entities engaging in cyber-attacks. State actors

[79/] *Compare* 6 U.S.C. § 1503 and 6 U.S.C. § 1505.

[80/] 6 U.S.C. § 1501(7).

[81/] *Cf.* Josephine Wolf, *When Companies Get Hacked, Should They Be Allowed to Hack Back?*, THE ATLANTIC (July 14, 2017), https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679/.

[82/] *See supra* at n. 4.

such as China, Russia, and North Korea have also recently engaged in cyber-attacks on various U.S. public and private entities.[83/]

Given that most botnet traffic is from outside the United States, international cooperation is essential. For instance, filtering close to the source requires cooperation and collaboration between governments and international network operators. And the Federal government can help bolster U.S. perimeter defense by supporting and incentivizing efforts to augment capabilities to filter and block compromised traffic at border crossing ingress points, thereby reducing the risk and severity of damage from malware and botnet attacks originating overseas**.**

Increased harmonization and coordination of cybercrime enforcement internationally also would be beneficial. Botnets are best countered by close international cooperation between governments and technically-oriented and legislative institutions. The United States should demonstrate international leadership by promoting international norms and methods to bring cyber criminals to justice. As the Justice Department has acknowledged, "just as sophisticated cybercriminals take advantage of weaknesses in computer security, technology can allow them to take advantage of international borders and differences in legal systems, hoping that investigators from the victim's country will not be able to obtain evidence from abroad, if it is even available. As a result, international partnerships are a critical tool in the fight against cybercrime."[84/]

[83/] *A New Great Game: Russia, China, North Korea heighten Cyber Risk*, THE SECURITY LEDGER(June 13, 2017), https://securityledger.com/2017/06/a-new-great-game-russia-china-north-korea-heighten-cyber-risk/; *Changing cybersecurity landscape creates global threat, warns Accenture*, THE STACK (July 27, 2017), https://thestack.com/security/2017/07/27/changes-to-cybersecurity-landscape-create-global-threat-warns-accenture/; *The War You Can't See: U.S. cyber warriors protects us from daily attacks*, DAYTON DAILY NEWS (Apr. 10, 2017), http://www.daytondailynews.com/news/local/the-war-you-can-see-cyber-warriors-protect-from-daily-attacks/2kYpgKyutTmXvPg1QUhLPP/.

[84/] *Assistant Attorney General Leslie R. Caldwell Speaks at the CCIPS-CSIS Cybercrime Symposium 2016: Cooperation and Electronic Evidence Gathering Across Borders*, DEPARTMENT OF JUSTICE (June 6, 2016) https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-speaks-ccips-csis-cybercrime-symposium-2016 ("*Caldwell Speech*").

Accordingly, the United States should promote and encourage more countries to sign the Convention on Cybercrime, also known as the Budapest Convention.[85/] Described by the Justice Department as the "'gold standard' agreement addressing cybercrime, cyber investigations and evidence sharing,"[86/] the Budapest Convention requires signatory nations to formally criminalize certain basic malicious cyber activity and sets extradition standards, thereby helping to ensure that cyber criminals cannot escape prosecution based on location. To assist with cybercrime investigations and prosecutions, it further requires signatories to adopt procedures – specifically concerning preservation and disclosure of stored data and traffic data, production orders, search and seizure of computer data, real-time collection of traffic data, and interception of content data – aimed at improving transnational law enforcement cooperation and evidence sharing.

Insecure devices must also be addressed at the global level – addressing the issue on a national basis will help, but it will not be sufficient. Fragmented standards could result in some device manufacturers failing to incorporate sufficient security features into their products, and could allow cybercriminals to take advantage of weaknesses in IoT devices. Having international standards in place would help ensure that device manufacturers incorporate basic levels of security in device design, and will aid in consistently identifying and treating data coming from IoT devices.

In addition, the Federal government should work with ICANN and its Internet Assigned Numbers Authority department and with regional internet registries and registrars to enforce best practices for handling abuse involving domain names sponsored by the registrars. As noted above, fast flux enables botnets to rotate through thousands of IP addresses using a single domain or group of domains, circumventing IP blacklists. Combatting abuse at the domain name

[85/] Convention on Cybercrime, T.I.A.S. 13174, https://www.state.gov/s/l/treaty/tias/2001/131597.htm.

[86/] *Caldwell Speech.*

level is therefore vital, and the United States should encourage adoption of domain name anti-abuse best practices globally.

CONCLUSION

NCTA's members have made substantial investments in technologies, tools, protocols, and collaboration initiatives aimed at addressing and deterring botnet threats – and they will continue to do so going forward. Strengthening the nation's efforts to detect, deter, contain, and, where necessary, recover from botnets and DDoS attacks requires the involvement of all participants in an inter-dependent Internet ecosystem. NTIA should promote technical measures, multi-stakeholder efforts, education and awareness campaigns, and policy initiatives aimed at bolstering collective action against these threats.

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, Science & Technology
and Chief Technology Officer

Matthew J. Tooley
Vice President, Broadband Technology
Science & Technology

July 28, 2017