Before the
National Telecommunications and Information Administration
Washington, D.C.

In the Matter of	)	Docket No. 170602536-7536-01
	)	
The Request for Comments	)	82 Fed. Reg. 112
On the Resilience Against	)	
Botnets	)	

COMMENTS OF THE R STREET INSTITUTE

July 28, 2017

Prepared by:
Anne Hobson
Associate Fellow
R Street Institute
1050 17th St. NW #1150, Washington DC, 20036
202-525-5717
ahobson@rstreet.org

James Czerniawski
Research Assistant
R Street Institute
1050 17th St. NW #1150, Washington DC, 20036
202-525-5717
jczerniawski@rstreet.org

Introduction

On behalf of the R Street Institute, we respectfully submit these comments in response to the National Telecommunications and Information Administration's (NTIA) request for comments on actions that could be taken—as part of the activity directed by the president in Executive Order 13800, ‘‘Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure’’[1]—to address automated and distributed threats to the digital ecosystem. The R Street Institute is a free-market think tank with a pragmatic approach to public policy challenges.

[1] Department of Commerce, National Telecommunications and Information Administration, “The Resilience Against Botnets,” Request for Public Comment, Federal Register, Vol. 82, No. 112, June 13, 2017. https://www.ntia.doc.gov/files/ntia/publications/fr-ntia-cyber-eo-rfc-06132017.pdf.

We thank NTIA for the opportunity to submit further comments concerning the best approaches to ensure resilience against botnets. The severity of device vulnerabilities within the ecosystem of internet-enabled devices is exacerbated by inconsistent cyber-hygiene practices and a lack of adoption of cybersecurity standards among internet-of-things devices. Malicious actors can take advantage of these widespread vulnerabilities by mobilizing networks of infected computers into botnets. These distributed networks of hijacked machines perform automated tasks – such as spreading spam or malware, generating fraudulent clicks or denial-of-service attacks that flood a website to render it inaccessible. While there are serious policy questions that arise from the threat of botnet-enabled cyberattacks, it is also important to recognize that distributed computing is an agnostic technological application that can have many positive use cases. Additionally, cybersecurity in the internet of things and beyond is a complex global problem. It is important to avoid heavy-handed regulatory solutions that may appear to be a panacea but would, in reality, undermine beneficial uses, take away incentives for innovation or offer prescriptive design mandates. Instead, policymakers should focus on a multifaceted approach that would better align market incentives to promote cyber hygiene and encourage both manufacturers and customers to adopt cybersecurity best practices.

The Department's green paper sets the appropriate tone by framing NTIA's role as one of support and encouragement for emerging technology in the internet ecosystem.[2] What follows is an outline of the role of the federal government and Department of Commerce ["Department"] in particular, in advancing a light-touch regulatory approach to the internet of things and related issues, such as botnets. With this focus in mind, the sections that follow define the challenges posed by the botnets and automated threats, identify solutions to widespread device insecurity and outline the role of the federal government.

I. The Botnet Problem

Botnets rely on the innate characteristics of the connectivity, scope and scale of the "internet of things." Broadly, the "internet of things" is an array of connected objects with unique identifiers that have the ability to transfer data over a network.[3] A botnet is a collection of internet-enabled devices or "bots" using software designed to connect to a command-and-control server to perform automated tasks.[4] Botnets serve as the delivery system for cyberattacks. When the intent is malicious, botnets can be used to inflict serious damage through viruses, spam, distributed denial-of-service attacks and other forms of online fraud.

Broadly construed, botnets and automated activities using distributed computing are not inherently malicious. "Botnets," in this sense, have many beneficial applications. For example,

---

[2] Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, "Fostering the Advancement of the Internet of Things," January 2017. https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

[3] Anne Hobson, "Aligning Cybersecurity Incentives in an Interconnected World," R Street Institute Policy Study No. 86, February 2017. http://www.rstreet.org/policy-study/aligning-cybersecurity-incentives-in-an-interconnected-world/.

[4] Internet Society, "Policy Brief: Botnets," Internet Society, October 2015. https://www.internetsociety.org/policybriefs/botnets.

they can be used to allocate spare computing power to raise money for charities,[5] perform medical research to find cures for cancer[6] or help search for extraterrestrial life.[7] In fact, when acting together, distributed computer networks can mobilize more processing power than supercomputers.[8] Because not all automated network-driven activity is malicious, it is important to avoid policy approaches that might lead to banning or restricting broad categories of internet activity – since it may not always be possible for service providers to tell them apart.

For example, the BOTS Act of 2016 bans the use of bots and botnets in the context of the online secondary market for tickets, an approach with deleterious consequences for legitimate ticket brokerage services and for the fans who are reliant on them.[9] As lawmakers and regulators pursue policy solutions, it is important to remember that it is the user's intent and action that makes botnets criminal, not the underlying technology.

While the scale, scope and interconnectivity of the internet of things can lead to economic growth and increases in human productivity and prosperity, these features also present unique challenges. Because it is a global ecosystem, one device's vulnerability can become a problem for the entire network. Malware can infect vulnerable internet-of-things devices, which it can then leverage to form a botnet and organize DDoS attacks using the inflected devices now on the net to bombard websites or service providers with traffic. Such attacks rely on sheer numbers to accomplish their nefarious ends and can result in costly internet outages. The average DDoS attack costs an afflicted firm $500,000, according to one estimate.[10]

Addressing issues related to cybersecurity and privacy will require efforts from industry, policymakers, consumers and third parties. The Department can play a role in improving security outcomes by supporting market solutions, convening stakeholders and adopting a light-touch regulatory approach to improve security on the ecosystem as a whole.

II. Cybersecurity Solutions

Distributed threats require distributed solutions from industry, government and civil society. Put another way, distributed attacks require distributed defenses informed by a multiplicity of perspectives and efforts. Question 4 in the RFC asks what stakeholders should be involved in addressing automated threats.[11] This section will demonstrate that a confluence of efforts by

---

[5] Stanford University, "Folding@Home," http://folding.stanford.edu/.
[6] Mark McAndrew, "Charity Genie," http://www.charityengine.com/about.
[7] U.C. Berkeley, "Seti@Home," https://setiathome.berkeley.edu/.
[8] Boon-Chong Seet, "*Mobile Peer-to-Peer Computing for Next Generation Distributed Environments: Advancing Conceptual and Algorithmic Applications*," Information Science Reference, (2009).
[9] BOTS Act of 2016, S. 3183, 114th Cong. (2016). https://www.congress.gov/bill/114th-congress/senate-bill/3183.
[10] Incapsula, "Survey: What DDoS Attacks Really Cost Businesses," pp. 1-9, 2014. https://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20 Impact%20Survey.pdf.
[11] 4. Governance and collaboration: What stakeholders should be involved in developing and executing policies, standards, practices, and technologies? What roles should they play? How can stakeholders collaborate across roles and sectors, and what should this collaboration look like, in practical terms?

stakeholders in the public and private sectors are necessary to create long-lasting resiliency to distributed cyberattacks. For example, entrepreneurs can invent after-market solutions that leverage artificial intelligence. Consumers can purchase smart firewalls or routers and provide feedback on online platforms about cybersecurity performance of internet-of-things devices. Efforts to determine security best practices or risk-analysis tools benefit from input from device manufacturers, insurers, civil society organizations, government agencies and standards bodies. The federal government can convene these stakeholders to advance critical discussions about solutions. For instance, the NTIA's multistakeholder process on upgradeability helps to advance the discussion on best practices, emphasize solutions and coordinate efforts.[12] The redundancy and scope of these efforts distributed across multiple actors is critical to produce a resilient internet of things ecosystem.

In the remainder of this section, we will address questions 1 and 3 of the RFC – specifically, what solutions work and how do solutions mitigate cyber risk.[13] The efforts detailed below are already working to increase device security and foster best practices.[14]

Voluntary Third-Party Certification Programs and Consumer Feedback

Third party accreditation organizations, standards organizations, online forums, and ratings bodies can and do provide information about the security of internet-of-things devices. By revealing a company's cybersecurity track record, these entities encourage a company to adopt better cybersecurity practices and help to hold companies accountable.

Public pressure has an effect. For example, after November 2016's DDoS attack in which the Mirai malware infected hundreds of thousands of devices, the Chinese company responsible for manufacturing webcams implicated in the attack voluntarily recalled millions of insecure devices to avoid the scorn of the public and other entities.[15] As a result of that attack, popular sites like

---

[12] National Telecommunications and Information Administration, "Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching." https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

[13] 1. What works: What approaches (e.g., laws, policies, standards, practices, technologies) work well for dealing with automated and distributed threats today? What mechanisms for cooperation with other organizations, either before or during an event, are already occurring?
3. Addressing the problem: What laws, policies, standards, practices, technologies, and other investments will have a tangible impact on reducing risks and harms of botnets? What tangible steps to reduce risks and harms of botnets can be taken in the near term? What emerging or long term approaches may be promising with more attention, research, and investment? What are the public policy implications of the various approaches? How might these be managed, balanced, or minimized?

[14] Anne Hobson, "Aligning Cybersecurity Incentives in an Interconnected World," R Street Institute Policy Study No. 86, February 2017. http://www.rstreet.org/policy-study/aligning-cybersecurity-incentives-in-an-interconnected-world/.

[15] Michael Mimoso, "Chinese Manufacturers Recalls IoT Gear Following Dyn DDoS," Threat Post, Oct. 24, 2016. https://threatpost.com/chinese-manufacturer-recalls-iotgear-following-dyn-ddos/121496/.

PayPal, Amazon, Twitter and Spotify all were brought down for the duration.[16] It was projected that more than $100 million in revenue was lost.

Negative press, as well as negative consumer reviews on Amazon and Yelp, can help penalize vendors who neglect security. The Online Trust Alliance, a multistakeholder initiative affiliated with the Internet Society, released its 2017 "IoT Trust Framework" that details devices' design requirements and security processes, serving as a checklist for a future internet-of-things device-certification program. The Consumer Technology Association (CTA), an industry association, produced guidelines establishing security practices for residential internet-of-things devices.

The Institute of Electrical and Electronics Engineers is a technical professional organization that drives the development of technical standards to ensure interoperability and security in the internet-of-things ecosystem.[17] Their successful efforts include Wi-Fi and Ethernet. There also is a role for open-source initiatives to produce standards. For example, AllSeen Alliance's AllJoyn project lets compatible "smart things" recognize each other and share information resources across brands, networks and operating systems.[18]

Industry Best Practices and Guidelines

Industry best practices encourage basic beneficial security behavior, such as avoiding hard-coded or default passwords, incorporating encryption or applying authentication protocols.[19] Insurers reward better cybersecurity practices with lower insurance rates and can encourage the adoption of best practices based on the National Institute of Standards and Technology (NIST) framework.[20] In fact, some insurers already use the NIST framework as a basis for risk assessments.[21] However, there is still room to apply the NIST framework to specific industry subsets or applications, such as autonomous vehicles. For example, the Automotive Information Sharing and Analysis Center formalized cybersecurity best practices for connected cars.[22] The Consumer Technology Association produced guidelines for home internet-of-things applications.[23]

---

[16] Rich Umbach, "Mirai Botnet Costs Companies Hundreds of Millions," Oct. 26, 2016. http://effortlessoffice.com/mirai-botnet-attack-costs-companies-hundreds-of-millions/.
[17] IEEE, "IEEE-SA IoT Ecosystem Study," 2015. http://standards.ieee.org/innovate/iot/.
[18] AllSeen Alliance, "AllJoyn Framework," 2017. https://allseenalliance.org/framework.
[19] Keith Moore, Richard Barnes, and Hannes Tschofenig, "Best Current Practices for Securing Internet of Things (IoT) Devices," July 3, 2017. https://tools.ietf.org/id/draft-moore-iot-security-bcp-01.html.
[20] Anne Hobson, "The Request for Comments on the 2017 draft Framework for Improving Critical Infrastructure Cybersecurity Version 1.1," April 10, 2017. https://www.nist.gov/sites/default/files/documents/2017/04/19/2017-04-10_-_r_street_institute.pdf.
[21] Judy Greenwald, "Cybersecurity framework marches forward," July 3, 2017. http://www.businessinsurance.com/article/20170703/NEWS06/912314233/Cyber-security-framework-President-Donald-Trump-executive-order.
[22] "Automotive Cybersecurity Best Practices," Automotive Information Sharing and Analysis Center, July 2016. https://www.automotiveisac.com/best-practices/.
[23] Consumer Technology Association, "Welcome to the Connected Home Security Checklist Tool," 2017. https://www.cta.tech/Membership/Member-Groups/TechHome-Division/Device-Security-Checklist.aspx.

The Broadband Internet Technical Advisory Group's 2016 report detailed the best current software practices for internet-of-things devices, which included shipping devices with current software; designing a mechanism for secure, automated software updates; employing strong authentication by default; using cryptography best practices; and testing and hardening internet-of-things device configurations.[24] Incorporation of these practices on a wide scale will make the internet-of-things ecosystem more resilient to automated attacks.

Clearer Rules for Security Research

The efforts of security researchers to identify and investigate vulnerabilities are crucial to improve baseline cybersecurity in consumer products. They help manufacturers discover vulnerabilities and patch them, thereby making the entire ecosystem more secure. Many internet companies—such as Google, Mozilla, Microsoft and Facebook—provide incentives through bug bounties to discover and report vulnerabilities. For instance, Google alone has paid out more than $9 million over the course of its Vulnerability Rewards Program.[25] However, many companies do not welcome scrutiny of their security practices and may have significant legal recourse under current law. In order to reverse engineer devices or circumvent controls without fear of reprisal, security researchers acting in good faith need strong exemptions from laws such as the Digital Millennium Copyright Act's (DMCA) anti-circumvention provision and the Computer Fraud and Abuse Act (CFAA).[26] To address this problematic gray area and reverse the chilling effect, the federal government should consider expanding and codifying exemptions to the DMCA and clarifying critical ambiguities in the CFAA[27].

Mechanisms to Improve Consumer Confidence

Individual consumers and small businesses don't always know how to tell when a given internet-enabled device is secure. Even if consumers have a strong preference for security and privacy, information asymmetries may get in the way. Uncertainty and dishonest practices can erode trust between buyers and sellers, reducing incentives for manufacturers to invest in security technologies and providing opportunities for malicious botnets to thrive. Guarantees and warranties can build consumer confidence by signaling that companies have invested in the security of their products and stand behind them in the event of a breach or failure.

---

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

[25] Hatmaker, Taylor. 2017. "Google's Bug Bounty Program Pays Out $3 Million, Mostly For Android And Chrome Exploits," *Techcrunch*. Accessed July 27 2017. https://techcrunch.com/2017/01/31/googles-bug-bounty-2016/.

[26] Jen Ellis, "New DCMA Exemption is a Positive Step for Security Researchers," *Rapid7 Community*, October 28, 2015. https://community.rapid7.com/community/infosec/blog/2015/10/28/new-dmca-exemption-is-a-positive-step-for-security-researchers.

[27] "'The Cyber:' Hard Questions In The World Of Cybersecurity". 2017. Cdt.Org. Accessed July 27 2017. https://cdt.org/insight/the-cyber-hard-questions-in-the-world-of-cybersecurity-research/.

Warranties can promote accountability, as companies commit to guarantee satisfaction, performance or quality. For example, a warranty could promise that a device is free from certain security vulnerabilities. In the event of a breach or malicious botnet activity, the seller would commit to update, refund, repair or replace the device. For example, SentinelOne provides a $500,000 insurance-backed warranty for damages their clients incur from ransomware attacks.[28] Another cybersecurity company, Armor, also offers a $100,000 warranty in the case of an attack.[29] Cymmetria, another provider of cybersecurity, boasts a $1 million insurance-backed warranty in the event their software does not detect an advanced persistent threat (APT) attack.[30] On the margin, wider use of guarantees can provide incentives for companies to compete on cybersecurity, which is especially important for certain highly sensitive internet-of-things devices like webcams or baby monitors. While this may encourage the purchase of more secure devices, this is not a panacea. It's not always clear to a consumer when an internet-of-things device is infected or when private information is stolen.

Threat Information-Sharing Efforts and Risk Measurement

Information about cyberattacks and threats can help industry and government prepare and mount a defense. For insurers, correct information about risk can enable them to offer more accurately priced products, thus expanding coverage to more small and medium-sized businesses. Understanding risk can help companies and government prioritize where to allocate resources. It is challenging to coordinate the exchange of detailed and correct information about threats, though both the public and private sectors are trying. The NIST framework, a multistakeholder effort, developed a common language and best practices to help organizations manage, understand and communicate cyber risks.[31] In 2016, Congress passed the Cybersecurity Information Sharing Act, which sought to promote communication between companies and federal agencies.[32] Programs like Facebook's ThreatExchange,[33] IBM's X-Force Exchange[34] and DHS's US-Cert programs also help to fill the information gap.

Automated Defenses & After-Market Cybersecurity Solutions

---

[28] SentinelOne, "Defense Against Every Threat at Every Stage." https://sentinelone.com/why-sentinelone/.
[29] Armor, "Armor Cyber Warranty," 2017. https://explore.armor.com/100k-guarantee/.
[30] Gadi Evron, "Cymmetria now offering a $1 million USD warranty for APT attacks," Nov. 28, 2016. http://blog.cymmetria.com/cymmetria-now-offering-a-1-million-usd-warranty-for-apt-attacks.
[31] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Jan. 10, 2017. https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf.
[32] Cybersecurity Information Sharing Act of 2015, S. 754, 114th Congress (2016). https://www.congress.gov/bill/114th-congress/senate-bill/754.
[33] Facebook for Developers, "ThreatExchange," 2016. https://developers.facebook. com/products/threat-exchange; see also Department of Homeland Security, "Cyber Information Sharing and Collaboration Program," May 4, 2016. https://www.dhs.gov/ciscp.
[34] IBM, "IBM X-Force Malware Exchange," 2017.https://exchange.xforce.ibmcloud.com/.

Automated defenses can leverage artificial intelligence or "cognitive security," such as IBM's program that applies their Watson system to identify and analyze threats.[35] On the consumer end, smart routers and firewalls can monitor traffic patterns and metadata to detect when a home's connected devices are compromised.[36] These devices can aid in both attack mitigation and endpoint prevention. Question 7 in the RFC asks "what can be done to educate and empower users and decision-makers?"[37] Smart firewalls empower consumers to recognize insecure devices and take action. ISPs also have an important role to play, given their unique ability to analyze large networks and traffic flows, and even detect unpatched vulnerabilities. Measures such as the Federal Communications Commission's (FCC) Communications Security, Reliability and Interoperability Council's (CSRIC) Anti-Bot Code of Conduct provide a basic framework to detect botnet activity, notify customers and help provide remediation options. While there certainly is potential for ISPs to do more, this must be balanced against a variety of concerns, including burdening private entities with the cost of global security, compelling engagement that is potentially invasive to privacy and blocking or restricting legitimate activity that comes up as a false positive. The question of the role of ISPs, particularly where they intersect with national security considerations, is worthy of further consideration and review.

Cyber Insurance Adoption

Cyber insurance aligns the incentives of insurers with the insured. Insurers perform risk assessments both in the underwriting stage, when deciding whether to take on a particular risk, and in the rate-setting stage, when they must ensure that the premium will cover the risk. Companies that demonstrate preparedness are rewarded with lower premiums. In this way, wide adoption of cyber insurance helps companies understand risk and internalize the cost of device insecurity. It also encourages a culture of preparedness.

Nevertheless, challenges to adoption remain. Clients misunderstand or underestimate their risk exposure and the nature of the cyber-insurance policies available.[38] A limited amount of historical data on cyberattacks, combined with quickly evolving threat vectors, suppresses insurers' ability to price risk accurately. Expensive premiums remain a challenge for small and medium-sized businesses. The upward trend in adoption[39] will increase the data available and the quantity of products available at lower prices.

---

[35] IBM, "IBM Cognitive SOC, Powered By Watson," 2017. https://www.ibm.com/security/cognitive/.
[36] CNET, ""Cujo safeguards your entire home against online threats," Jan. 5, 2017. https://www.cnet.com/products/cujo-smart-firewall/preview/.
[37] 7. Users: What can be done to educate and empower users and decision-makers, including enterprises and end consumers?
[38] Sam Friedman and Adam Thomas, "Demystifying cyber insurance coverage," Deloitte University Press, Feb. 23, 2017. https://dupress.deloitte.com/dup-us-en/industry/financial-services/demystifying-cybersecurity-insurance.html .
[39] Allie Sanchez, " Lloyd's predicts surge in cyber insurance uptake in 2017," Insurance Business, Jan. 4, 2017. http://www.insurancebusinessmag.com/us/news/cyber/lloyds-predicts-surge-in-cyber-insurance-uptake-in-2017-42244.aspx.

Regulatory efforts that rely on market-based incentives, such as cyber insurance, can have better, longer-lasting results than other legislative approaches. Inconsistent takeup in the manufacturing industry, compared to the health and financial services sectors, presents an opportunity for insurers and policymakers to encourage adoption.[40]

NTIA should seek out ways to encourage firms to share threat information; promote cyber-insurance adoption; foster ethical cyber research; encourage private efforts to recognize security-conscious products with certifications; develop and adopt best practices voluntarily; and reward innovative after-market cybersecurity products. Raising baseline cybersecurity through a combination of efforts by stakeholders will help to increase immunity among internet-enabled devices. There is no simple or low-cost regulatory fix. Instead, policymakers will have to encourage an environment where these cybersecurity solutions can emerge. NTIA should continue to play the role of convening stakeholders and encouraging discussion around cybersecurity.

III. The Role of Government

This section will address question 5 of the RFC, namely "what is the role of government?"[41] The complex nature of the problem and the diverse stakeholders involved in advancing solutions suggest that a heavy-handed regulatory approach easily could prove more damaging than beneficial. In the same way as people's compromised internet-of-things devices abroad can result in a DDoS attack that renders websites inaccessible in the United States, a policy developed in the United States could hamstring foreign manufacturers seeking to sell in the global market. Thus, as question 6. suggests,[42] the inherent global nature of the problem makes identifying a solution more difficult. Instead, it is important to focus on creating the policy environment such that a wide set of solutions can evolve.

A Light-Touch Regulatory Approach

The government's policy approach to the internet is a good historical test case that demonstrates the value of a light-touch policy environment. The federal government and federal agencies should continue to follow the approach detailed in the 1997 Framework for Global Electronic Commerce.[43] This framework reinforces the importance of industry-led policies and defines government's role as fostering that development. As incidents continue to emerge, the Department should pursue a light-touch regulatory approach to botnets. Furthermore, they should encourage state and local governments to do the same. Because devices are diverse in

[40] Council of Insurance Agents and Brokers, "Cyber Insurance Market Watch Survey," October 2016. https://www.ciab.com/uploadedFiles/Resources/Cyber_Survey/102016CyberSurvey_Final.pdf.
[41] 5. Policy and the role of government: What specific roles should the Federal government play? What incentives or other public policies can drive change?
[42] International: How does the inherently global nature of the Internet and the digital supply chain affect how we should approach this problem? How can solutions explicitly address the international aspects of this issue?
[43] The Framework for Global Electronic Commerce (July 1997), https://clinton4.nara.gov/WH/New/Commerce/.

functionality and nature, one-size-fits-all regulation is bound to have unintended consequences that result in larger net harm than net benefit. For example, the California State Senate released a bill targeting internet-of-things devices that required an "indicator light" for "any device, sensor, or other physical object that is capable of connecting to the internet, directly or indirectly, or to another connected device."[44] An indicator light is infeasible in some cases and not salient in others. Applying design requirements to a broad category of consumer devices can reduce cybersecurity by misallocating resources to compliance tasks.

When defining regulations to encourage cybersecurity, policymakers should favor performance standards that specify the desired outcome over design standards that specify the means of achieving security. In contrast to design standards, which can easily become empty compliance tasks, performance standards allow companies the flexibility to find methods to achieve security that work for their given product and its range of use cases. Regulations would be difficult to change over time once they are applied. Moreover, compliance costs of regulations could deter innovation in software improvements that could defend against botnets. Lastly, such requirements would crowd out private efforts to improve cybersecurity and privacy at the industry and firm level.

In its recent green paper, NTIA recognizes the danger of inconsistent or unpredictable regulation, while acknowledging the importance of industry experimentation and allowing for market solutions to emerge to address the constantly changing cyber-threat landscape.[45] Achieving resiliency will require a flexible policy environment that allows for the development of a variety of different solutions. Beyond using its convening power to encourage stakeholders to work together to overcome barriers to the exchange of information about threats or cybersecurity products, the Department also can play a role in encouraging market mechanisms mentioned in the prior section. These include voluntary industry guidelines and best practices, information-sharing efforts and private certification programs.

The federal government is also uniquely situated to promote cyber-insurance adoption.[46] The government is a large buyer of internet-enabled devices. The government could use this purchasing power to award contracts to internet-of-things contractors that emphasize cybersecurity. It can also urge other federal entities to do the same. The federal government should introduce a financial-responsibility requirement in its contracts with internet-of-things device vendors to transfer the financial and operational risks of cyberattacks.[47] This would help companies recover and prevent high vendor turnover due to a cyberattack. It will promote cyber-insurance adoption more broadly, helping to immunize the entire internet-of-things ecosystem

---

[44] Anne Hobson, "The Teddy Bear and Toaster Act is Device Regulation Gone Wrong," Techdirt, April 4, 2017. https://www.techdirt.com/articles/20170418/12443837180/teddy-bear-toaster-act-is-device-regulation-done-wrong.shtml.

[45] Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, "Fostering the Advancement of the Internet of Things," January 2017, p. 14. https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

[46] https://www.ntia.doc.gov/files/ntia/publications/ntia_comments_iot_rstreet.pdf.

[47] Anne Hobson, "Aligning Cybersecurity Incentives in an Interconnected World," R Street Institute Policy Study No. 86, February 2017. http://www.rstreet.org/wp-content/uploads/2017/02/86.pdf.

from cyberattacks. Moreover, it will encourage market growth for risk-based products and increase the availability and affordability of insurance products.

Conclusion

The internet of things is a complex, global network with numerous stakeholders operating across different legal frameworks. It cannot be underscored enough that there's no single panacea to address the security vulnerabilities that enable botnet attacks. Heavy-handed approaches and prescriptive remedies, while perhaps well-intentioned, are likely to produce counterproductive results. Instead, industry, governments, consumers and civil-society stakeholders will have to work together on a variety of efforts to mitigate cyber risk and align incentives to improve the ecosystem as a whole. Policymakers should aim to create a policy environment that encourages market-based solutions – such as cybersecurity guarantees, certifications and ratings; cyber-insurance adoption; freedom for cybersecurity research; facilitation of information-sharing efforts; and the adoption of industry best practices. We are encouraged by NTIA's efforts to understand the internet of things, engage stakeholders and develop a constructive policy approach that lets private stakeholders, rather than government, do the heavy lifting. We look forward to continuing to engage with the Department on this topic and welcome its engagement and critical role in convening stakeholders to promote commonsense solutions.

Respectfully submitted,

Anne Hobson
Associate Fellow
R Street Institute

James Czerniawski
Research Assistant
R Street Institute