NISKANEN CENTER

Public Interest Comment

Comments submitted to the National Telecommunications and Information Administration in the Matter of:

Promoting Stakeholder Action Against Botnets and Other Automated Threats

Ryan Hagemann
Director of Technology Policy
The Niskanen Center

Submitted: July 28, 2017
Docket No. 170602536-7536-01

Executive Summary

In response to the National Telecommunications and Information Administration's call for comments on addressing the threat posed by botnets and online automated threats, the Niskanen Center responds to a number of policy questions that present challenges to the security of the emerging Internet of Things. In addition, we make a number of general recommendations for consideration: (1) defending intermediary liability protections for online service providers and content delivery networks; (2) continuing to embrace the *Framework for Global Electronic Commerce*; (3) promoting cybersecurity insurance; (4) extending public-private information sharing regimes; and (5) codifying the process by which the government shares zero-day exploits with firms.

Introduction

An increasing number of everyday objects are connecting to the Internet. New industries of "smart" devices are coming to populate American kitchens and livingrooms, as well as public spaces where WiFi networks are increasingly ubiquitous. These devices—collectively referred to as the Internet of Things (IoT)—are poised to disrupt the consumer market, while providing even bigger benefits to manufacturing productivity and logistics efficiencies. Unfortunately, cybersecurity concerns are a considerable roadblock to greater adoption. For the IoT to make good on its potential benefits, consumers will need to start trusting these systems more than they currently do.

Traditional computing devices like laptops and smartphones are relatively easy to update, with alerts that remind users that an upgrade is available and preference settings that give consumers considerable control over their device. Unfortunately, this PC-era security model does not work for IoT devices, which are more vulnerable to attacks due to individual consumers' inability or unwillingness to update devices, manufacturers' disincentives from embracing security-by-design standards, and more pronounced network effects in which one insecure device can have a ripple effect throughout the IoT ecosystem. As a result, we need to rethink cybersecurity approaches in an age of ubiquitous interconnectivity in which everything from our toasters to our cars are linked to the Internet.

In response to these concerns, the Niskanen Center will answer four of the National Telecommunications and Information Administration's (NTIA) questions (1, 3, 4, and 5) in its recent call for comments.[1]

Response to Questions

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?

Over half of all companies in the United States are ill-prepared to deal with a cybersecurity attack.[2] However, a majority of firms recognize the need to better-equip themselves against potential cybersecurity attacks. One approach that is gaining popularity among firms is the use of cybersecurity insurance.

Cybersecurity insurance reduces financial risks associated with data breaches, network damage, distributed denial of service (DDoS) attacks, and other related cyber incidents. A growing number of companies are making use of cyber security insurance. According to PricewaterhouseCoopers, cybersecurity insurance annual gross written premiums are set to grow from around $2.5 billion today

[1] "Promoting Stakeholder Action Against Botnets and Other Automated Threats," National Telecommunications and Information Administration, U.S. Department of Commerce, Docket No. 170602536-7536-01, https://www.ntia.doc.gov/files/ntia/publications/fr_ntia_cyber_eo_rfc_-_rin_0660-xc035.pdf.
[2] "The Hiscox Cyber Readiness Report 2017," Hiscox, 2017, http://www.hiscox.com/cyber-readiness-report/.

to $7.5 billion by 2020.[3] That growth, however, is likely to face a number of challenges for actuaries attempting to underwrite cybersecurity policies.

Lack of actuarial data presents major challenges for insurance underwriters attempting to accurately quantify cyber risk, resulting in restricted coverage. The Department of Homeland Security National Protection and Programs Directorate is exploring the feasibility of creating a cyber incident data repository "that creates a trusted environment for enterprise risk owners to anonymously share sensitive cyber incident data." A cyber incident data repository could enable insurers to more accurately assess the risks from online security threats and provide better coverage for the potential damages related to cyber incidents. Encouraging firms to purchase cybersecurity insurance can help lead to the adoption of better security practices and cybersecurity response plans tailored to the risks incurred by a variety of business models.

The threat of cybersecurity attacks has also resulted in an emerging collection of cybersecurity products aimed at automating the detection of compromised IoT devices and providing secure pathways to issue security patches at scale. Cloudflare Orbit, for example, is a product that provides IoT vendors and users with the capability to push updates and patches at the network level, defraying the need to rely on updates to the physical devices themselves. Devices using Cloudflare Orbit will first pass through Cloudflare before connecting to the Internet, filtering out malicious activity.[4] Essentially, Orbit operates as a "fog" between the physical device and the networked "Cloud." The fog can filter out suspicious code and activity that would otherwise trickle down to user devices, all without necessitating additional security protocols that are hardcoded into the actual IoT device. Emerging technologies like this can act as additional layers of security for IoT devices, and could help remedy concerns associated with relying on updates on the user-level.

Of course, there are other solutions to protecting against online threats that have require less substantive investments than embracing new technologies. The value of encryption in protecting users, for example, cannot be overstated. New developments in enterprise encryption could also help mitigate more focused attacks, with companies like IBM investing in user-friendly systems that encrypt massive troves of data at multiple levels within a network.[5] Encrypting sensitive data is an important part of ensuring the proliferation of trust in the online ecosystem—which in turn has promoted the growth of the digital economy—and can have a similar effect on the emerging IoT economy.[6]

Additionally, there are a number of ongoing proceedings, industry-based standards and frameworks, and technical analysis efforts aimed at establishing best practices for curtailing the threats posed by

[3] "Insurance 2020 & Beyond: Reaping the Dividends of Cyber Resilience," PricewaterhouseCoopers, 2015, https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf.
[4] Dani Grant, "Introducing Cloudflare Orbit: A Private Network for IoT Devices," Cloudflare Blog, April 27, 2017, https://blog.cloudflare.com/orbit/.
[5] Lily Hay Newman, "IBM's Plan to Encrypt Unthinkable Amounts of Data," *Wired*, July 17, 2017, https://www.wired.com/story/ibm-z-mainframe-encryption/.
[6] Ryan Hagemann and Joshua Hampson, "Encryption, Trust, and the Online Economy: An Assessment of the Economic Benefits Associated with Encryption," Niskanen Center, November 9, 2015, https://niskanencenter.org/wp-content/uploads/2015/11/RESEARCH-PAPER_EncryptionEconomicBenefits.pdf.

botnets, as well as promoting a wide range of technical recommendations that can help better inform policymakers' perspectives on these issues.[7]

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?

In the near-term, technologies like Cloudflare's Orbit service could be used to help reduce the risks associated with automated botnets, cybersecurity insurance could help incentivize firms to prioritize cybersecurity best practices, and encryption can help users secure their most sensitive data at both network endpoints and in-transit. With specific regards to content delivery networks (CDN) like Cloudflare, government policies should reinforce deference to the intermediary liability protections promoted by the Digital Millennium Copyright Act (DMCA). In order for CDNs to continue offering new and innovative products that can promote online security, policymakers must push back against mistaken assertions that claim they do not qualify for intermediary liability protections under the DMCA.[8]

Promoting greater information-sharing between the public and private sector can also help address the problems of online hackers and malicious third parties. In particular, sharing information about "zero-day" exploits and funding bug bounty programs can help secure the digital landscape by promoting greater collaboration and trust among individuals in government, the intelligence community, and private firms. To that end, a good first step would be codifying the vulnerabilities equities process (VEP) in law.[9]

Currently, the VEP is simply an administrative policy. Unbacked by the force of statute, its information-sharing provisions can be withdrawn at any time. Sens. Ron Johnson (R-WI) and Brian Schatz (D-HI), however, have recently proposed the PATCH Act, which would move the VEP into more certain legal territory by enshrining it in law.[10] Efforts like these are important steps in creating a security landscape that further stimulates cooperation in the fight against the proliferation of software vulnerabilities and botnets.

---

[7] In particular, we would direct NTIA's attention to this recently-released technical white paper written in response to the Trump Administration's Executive Order 13800: Industry Technical White Paper, Communications Sector Coordinating Council, July 17, 2017, https://docs.wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf.

[8] Ryan Hagemann, *Comments submitted to the United States Trade Representative in the Matter of: A Rebuttal to "A Request for Comment on the 2016 Special 301 Out-of-Cycle Review of Notorious Markets,"* Niskanen Center, Docket No. USTR-2016-2013, submitted October 20, 2016, https://niskanencenter.org/wp-content/uploads/2016/10/NiskanenCenter_USTRCommentsNotoriousMarketsRebuttal.pdf.

[9] Ryan Hagemann, "Balancing Cybersecurity and National Security," Niskanen Center, July 28, 2016, https://niskanencenter.org/blog/balancing-cybersecurity-national-security/.

[10] Ryan Hagemann, "How to Cure What Ails American Cybersecurity," *RealClearPolicy*, May 18, 2017, http://www.realclearpolicy.com/articles/2017/05/18/how_to_cure_what_ails_american_cybersecurity.html.

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?

Multistakeholder processes and soft law governance mechanisms have proved a vital source of regulatory flexibility for the IoT and other emerging technology industries. Recently, the Department of Commerce reaffirmed its commitment to the Clinton Administration's *Framework for Global Electronic Commerce*—the statement of principles that helped the early commercial Internet grow into the major driver of economic growth that it is today.[11] Those principles should continue guiding the Department's treatment of this industry, as the Niskanen Center noted in its supporting comments of the Department's Green Paper on the IoT.[12]

In particular, the Niskanen Center suggests a continuation of the multistakeholder model of emerging technology regulatory governance. This inclusive approach, buttressed by openness and transparency, can help ensure individuals and organizations from the private sector, civil society, and government all have a seat at the table to voice concerns and offer solutions to the many issues confronting the future of the IoT. An approach that respects the tenets of the *Framework for Global Electronic Commerce* while embracing the multistakeholder process would track closely along the following lines:

> *Governance of new, untried and untested technologies should begin with industry issuing standards and best practices. A multistakeholder review process—facilitated but not dictated by the appropriate federal agency—should follow, with clear process guidelines and objective goals and deliverables. This process should in no way be predicated on a presumption of regulatory action, but merely serve as a forum for discussion. Public comments should be sought throughout the process. During this time, firms should be granted a default approval to continue operating. Regulators should observe-and-respond to ongoing developments, proposing new rules only if a risk-based assessment warrants further action.*[13]

---

[11] The Department of Commerce, Internet Policy Task Force and Digital Economy Leadership Team, "Fostering the Advancement of the Internet of Things," January 12, 2017, p. 11, https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf. ("Dating back at least to the 1997 Framework for Global Electronic Commerce, the U.S. Government has been operating under the principle that the private sector should lead in digital technology advancement. Even where collective action is necessary, the U.S. Government has encouraged multistakeholder approaches and private sector coordination and leadership where possible. When governmental involvement is needed, it should support and enforce a predictable, minimalist, consistent, and simple legal environment for commerce.")

[12] Ryan Hagemann, *Comments submitted to the National Telecommunications and Information Administration in the Matter of: Green Paper: Fostering the Advancement of the Internet of Things*, Niskanen Center, Docket No. 170105023-7023-01, submitted February 8, 2017, https://www.ntia.doc.gov/files/ntia/publications/niskanencenter_commentsiotgreenpaperntia.pdf.

[13] Ryan Hagemann, "New Rules for New Frontiers: A Regulatory Manifesto for Emerging Technologies," Niskanen Center, January 30, 2017, https://niskanencenter.org/blog/new-rules-new-frontiers-regulatory-manifesto-emerging-technologies/.

In short, collaboration on governing standards should remain an open, inclusive, and iterative process that permits a wide array of stakeholders to have a voice in the process.

5. Policy and the role of government: What specific roles should the federal government play? What incentives or other public policies can drive change?

NTIA is currently in the process of hosting ongoing multistakeholder engagements discussing the environment surrounding upgrading and patching devices in the IoT ecosystem.[14] Those proceedings have thus far been extremely productive, and have even resulted in positive engagement with the Federal Trade Commission on the need for appropriately communicating how manufacturers will safeguard consumers' IoT devices.[15] NTIA and the Department of Commerce should continue playing the role of a convener of these types of multistakeholder meetings while ensuring they remain open and transparent processes in which all interested parties can engage.

General Recommendations

Whether aiming to increase endpoint security for IoT devices or disrupting malicious network activity conducted through automated botnets and DDoS attacks, the government can play a positive role in promoting information sharing and incentivizing the adoption of new technological solutions. What it cannot do, however, is impose security through top-down dictates. With that in mind, the Niskanen Center would recommend NTIA and the Department of Commerce consider alternatives to a more heavy-handed regulatory regime. We recommend:

1. Defending intermediary liability protections for CDNs and other online service providers;
2. Continuing to embrace the *Framework for Global Electronic Commerce* as the guiding principles governing the Department's perspective on IoT regulatory approaches;
3. Leading on embracing cybersecurity insurance by implementing federal cybersecurity insurance requirements for contractors, examining the feasibility of providing tax breaks for insurers, and permitting data sharing to help develop actuarial assessments of the cybersecurity threat landscape;
4. Promoting information-sharing initiatives between the public and private sectors; and
5. Codifying the VEP in law to ensure appropriately-vetted zero-day exploits can be quickly and effectively disseminated for patching.

---

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

[15] Federal Trade Commission Public Comment on "Communicating IoT Device Security Update Capability to Improve Transparency for Consumers," Communicating Upgradability and Improving Transparency Working Group, Multistakeholder Process on Internet of Things Security Upgradability and Patching, National Telecommunications and Information Administration, https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-comment-national-telecommunications-information-administration-communicating-iot-device-security/170619ntiaiotcomment.pdf.

Conclusion

Cybersecurity is a growing concern throughout the world. Although there are certainly risk-mitigation strategies that can promote better standards and practices in cybersecurity hygiene, risk assessment reports like those that dominate Executive Order 13800 amount to little more than kicking the can further down the road.[16] While no system can ever be one hundred percent secure, there are a number of positive steps the government can take to be an effective steward of ensuring the stability and security of the online landscape. By embracing ongoing multistakeholder efforts at NTIA, forbearing from onerous regulatory actions and one-size-fits-all security standards, defending intermediary liability protections for online service providers and CNDs, and promoting information-sharing regimes like the VEP, the government can do far more to help catalyze the growth and security of the IoT.

We would like to thank NTIA for the opportunity to comment on this issue and look forward to remaining engaged with the Agency on this matter.

[16] Brandon Valeriano and Ryan Hagemann, "Managing the Risk of Cyber Security: The Trump Administration's Executive Order," Niskanen Center, May 16, 2017, https://niskanencenter.org/blog/managing-risk-cyber-security-trump-administrations-executive-order/.